МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська політехніка»

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 15, № 3

Volume 15, No. 3

Одеса – 2025
Odesa – 2025

Журнал внесений до переліку наукових фахових видань України (технічні науки) згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р. Перереєстровано на категорію «Б» за фахами 121, 122, 125, 151 згідно наказу МОН України № 1473 від 26.11.2020 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded. National Odesa Polytechnic University in 2011

Certificate of State Registration КВ № 17610 - 6460Р of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Національного університету «Одеська політехніка»

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: 1, Шевченка пр., Одеса, 65044, Україна
Телефон: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

Editorial address: 1, Shevchenko Ave., Odesa, 65044, Ukraine
Tel.: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

ЗМІСТ/CONTENTS

DOI 10.15276/imms.v15.no3.303
UDC: 004.738.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 303-311

METHODS FOR IMPLEMENTING ACCESSIBILITY IN USER INTERFACE DESIGN

L. Bovnegra, S. Kutsyn

National Odessa Polytechnic University
1, Shevchenka Ave, Odesa, 65044, Ukraine
Emails: dlv5@ukr.net, 7813boychenko@gmail.com

Accessibility has become a first-class quality attribute in UI/UX and web design, affecting legal compliance, user equity, and business outcomes. However, teams often face practical barriers when translating high-level guidelines into day-to-day workflows and measurable engineering outcomes. This article consolidates established methods for implementing accessibility in user interface design and presents a reproducible workflow that integrates standards-driven evaluation, incremental code refactoring, and user testing with assistive technologies. The study contributes to computer science and HCI by bridging normative guidance with process-level tactics for UX and front-end teams, yielding actionable artefacts (metrics, checklists, mapping tables) suitable for continuous delivery environments. We synthesize literature and standards to define a stepwise pipeline: heuristic and WCAG-oriented audits; prioritization of barriers by severity and user impact; minimal-change refactoring (semantic HTML, ARIA roles/states, focus management, keyboard navigation, contrast, error handling); validation via manual checks and automated tooling, plus user testing with screen readers; regression control in CI/CD. The evaluation model includes Accessibility Conformance Ratio, accessibility defect density, task success rate, time-on-task, error rate, and an effort-normalized efficiency metric. Applied to a representative web module, the workflow led to a systematic increase in conformance coverage and a reduction in critical barriers, accompanied by higher task success and shorter completion times for users relying on assistive technologies. Statistical tests on pre/post measures support the significance of the observed improvements, while threats to validity and transferability are discussed. The paper offers a reusable accessibility engineering approach, a compact measurement model, and traceability from WCAG criteria to UI/code changes and tests. The results inform UI/UX designers and developers how to stage accessibility improvements without disruptive redesigns, and how to embed accessibility gates into continuous delivery.
Keywords: accessibility; WCAG; UI/UX; web design; user testing; WAI-ARIA; refactoring.

Introduction. Accessibility of digital interfaces today is not only an ethical and social requirement but also a clearly defined engineering task that directly influences audience reach, user experience (UX) quality, and business results. According to WHO estimates, 1.3 billion people - about one in six globally (≈16%) - live with significant forms of disability; therefore, every UI/UX and web-design project inherently interacts with a large and diverse group of users with specific interface and interaction needs (AT support, keyboard navigation, contrast, etc.). Comparable estimates for individual countries (e.g., 28.7% of adults in the United States) further underscore the scale of the phenomenon and the need for a systematic engineering response.

At the EU regulatory level, the European Accessibility Act (Directive (EU) 2019/882) takes effect from 28 June 2025, extending requirements to a broad range of private-sector products and services (including e-commerce, e-books, banking services, mobile apps, self-service terminals). Previously, Directive (EU) 2016/2102 already applied to the accessibility of websites and mobile applications of public-sector bodies. Both initiatives are based on the harmonized standard EN 301 549 (version 3.2.1), which in turn relies on WCAG 2.1 criteria, ensuring consistency of technical requirements and assessment mechanisms. For developers outside the EU, the U.S. Section 508 (Revised 2017) is likewise illustrative, incorporating WCAG 2.0 AA as the normative basis for the public sector. Taken together, this forms a global

landscape in which accessibility becomes a matter not only of voluntary practice but also of formal obligations and audits [1].

Despite the maturity of standards, the actual state of web accessibility remains problematic. According to WebAIM Million 2025, 94.8% of homepages of leading sites had detected WCAG 2 violations (down from 95.9% in 2024), with an average of ≈51 errors per page (50,960,288 errors across 1 million pages). The most common issues are low contrast (79.1% of pages), missing image alt text (55.5%), missing form labels (48.2%), "empty" links (45.4%), etc.; 96% of all detected errors fall within just six categories. At the same time, interface structural complexity is increasing: the average number of elements on a homepage rose to 1,257 (+7.1% year-over-year), and ARIA attribute usage to ≈106 per page (+18.5% y/y), correlating with an increase in errors. These data document a systemic gap between normative requirements and current UI/UX development practices.

The cost of non-inclusivity is measured not only in missed interaction opportunities but also in direct economic impact. According to the Click-Away Pound 2019 survey, 69% of internet users with disabilities abandon websites when they encounter barriers, and lost online sales in the United Kingdom reached £17.1 billion per year. Moreover, 83% of respondents limit their purchases to websites whose accessibility they trust. These facts strengthen the business case for systematic accessibility work as part of customer acquisition and retention strategies [1].

WCAG 2.2 standards (W3C Recommendation as of October 5, 2023) clarified expectations for several critical interaction scenarios—adding nine new success criteria (including 2.4.11 Focus Appearance, 2.5.7 Dragging Movements, 2.5.8 Target Size) and refining approaches to internationalization. This expansion is intended to improve real-world usage, especially on mobile devices and within complex web applications. Together with EN 301 549 and national regulations, it provides a clear axis for measuring conformance and planning engineering changes.

Despite existing guidance, the industry often faces three practical challenges.

First, the over-saturation of interfaces with third-party components (ad networks, widgets, CMP banners) complicates accessibility control: studies indicate that advertising can increase WCAG violation rates across a large share of sites due to incorrect focus management, labeling, and element behavior.

Second, cookie notices and consent banners often exhibit contrast, semantic, and screen-reader/announcability defects for users with visual impairments, creating additional entry barriers.

Third, design dark patterns can manipulate choices around consent and privacy, undermining the WCAG principles of understandability and operability [2].

In this context, an approach is needed that combines normative clarity (WCAG/WAI-ARIA, EN 301 549, Section 508) with a realistic process for engineering change in the product. Industry experience shows that incremental accessibility adoption (via regular audits, impact-based barrier prioritization, minimal code changes followed by validation, and regression control in CI/CD) enables tangible reductions in defects and increases in conformance without "big-bang" rewrites or development freezes. From a computer-science perspective, this requires formalizing metrics (e.g., Accessibility Conformance Ratio, defect density, time-on-task and success rate in user testing with AT) and models for estimating the effect of changes to justify architecture, design, and backlog prioritization decisions. In the following sections, we align the accessibility implementation process with normative criteria and demonstrate how stepwise refactoring raises WCAG 2.2 conformance and improves UX indicators in a representative web case study [2].

Objective. To systematize literature-validated methods for implementing accessibility in user interface (UI) design and to present a reproducible engineering process that combines standards-oriented audits (WCAG/WAI-ARIA), incremental refactoring, and user testing with

assistive technologies (AT). This process should lead to measurable increases in conformance and improvements in UX metrics in a web case study.

Research Questions (RQ):

– RQ1. To what extent do accessibility-barrier density decreases and the Accessibility Conformance Ratio (ACR) increase after one or multiple incremental cycles?

– RQ2. Do user-testing results with AT (task success, time-on-task, error frequency) improve after targeted changes in semantics, focus, contrast, navigation, etc.?

– RQ3. What is the relative cost-effectiveness of refactoring (effect per unit of engineering time), and how does it compare to alternatives (e.g., a "redesign from scratch")?

Context and relevance. Approximately 1.3 billion people worldwide (~16%) live with significant forms of disability; in the U.S., about 28.7% of the adult population. According to WebAIM Million 2025, 94.8% of homepages have automatically detected WCAG 2 deviations, with an average of about 51 errors per page. At the same time, regulation is tightening (the European Accessibility Act effective June 28, 2025; harmonization with EN 301 549; in the U.S., Section 508) [1].

Scientific significance. Positioned at the intersection of computer science, HCI, and software engineering, this work bridges the gap between normative standards (WCAG 2.1/2.2, WAI-ARIA) and process tactics for UI/UX teams and front-end developers. The paper's contributions include: (i) a reproducible implementation pipeline; (ii) a measurement model (ACR, defect density, user-test indicators, cost-efficiency E); (iii) traceability from "WCAG criterion → UI/code change → test/verification." The novelty is reinforced by the advent of WCAG 2.2 (W3C Recommendation, October 5, 2023) with nine new criteria important for mobile and complex web interfaces (including Focus Not Obscured, Dragging Movements, Target Size).

Practical significance. In the EU market, the European Accessibility Act (EAA) has applied since June 28, 2025, covering a broad spectrum of private services/products; in the public sector, Directive (EU) 2016/2102 applies, harmonized with EN 301 549 v3.2.1 (based on WCAG 2.1). In the U.S., Revised Section 508 (2017) integrates WCAG 2.0 AA as the normative basis. Systematic accessibility implementation reduces non-compliance risk and delivers business impact (lower user churn, higher conversions), which is especially critical given the high share of pages with violations.

Methodology. Research design. We applied a five-stage incremental pipeline for implementing accessibility.

1. Audit. Combine heuristic inspection (extended "Nielsen+WCAG" heuristics) with rule-based scanners (axe/Lighthouse or equivalents) and manual checks of critical scenarios (keyboard navigation, focus, contrast, forms, media/alternatives), as well as AT checks (NVDA/VoiceOver).

2. Prioritization. Classify issues by criticality and impact (A/AA/AAA; blocking/non-critical), taking into account risks from third-party integrations (ads, cookie banners, widgets). Studies in 2024–2025 indicate that advertising often drives increases in WCAG violations (up to ≈67% of sites with worse metrics due to ads), and cookie interfaces commonly contain dark patterns and accessibility problems.

3. Minimal refactoring. Implement semantic HTML, correct ARIA roles/states, focus management (zones, order, visibility), keyboard navigation, WCAG-compliant contrast, valid error handling, and clear copy.

4. Validation. Re-audit plus user testing with AT (scenarios: login, search, forms). Record Task Success Rate, Time-on-Task, and Error Rate; compare "before/after" statistically (t-test or Wilcoxon, depending on normality) [3].

5. Regression control in CI/CD. Add accessibility "gates" (auto-checkers and checklists in PRs) aligned with EN 301 549/WCAG and, for the U.S. public sector, Section 508.

Metrics and evaluation model:

- ACR (Accessibility Conformance Ratio: share of applicable WCAG criteria met for a module/screen);

- A11y Defect Density (accessibility barriers per screen or per KLOC);

- user-testing indicators (success, time-on-task, error rate) in a user group including people with disabilities;

- cost-efficiency (E = ΔACR / dev_hours): conformance gain per unit of engineering time.

We separately track the contribution of third-party components (ads, CMP banners, widgets), which are statistically associated with higher WCAG violation rates [3].

Scale of the problem and empirical indicators. International estimates suggest about 1.3 billion people (~16%) live with significant disabilities; in the U.S., ~28.7% of the adult population. In the web context, WebAIM Million 2025 reports that 94.8% of homepages have automatically detected WCAG 2 deviations, averaging ~51 errors per page. These data justify the need for process-oriented approaches to implementing accessibility [2].

Normative and standards basis (WCAG/WAI-ARIA, EN 301 549, Section 508).

WCAG 2.1/2.2 define testable criteria; WCAG 2.2 (W3C Recommendation, 05 Oct 2023) adds nine criteria (notably 2.4.11–13 Focus, 2.5.7 Dragging Movements, 2.5.8 Target Size, 3.3.7–9 Accessible Authentication) aimed at real-world mobile and interactive scenarios. WAI-ARIA augments semantics and state management for rich-interaction components; its use should be combined with native HTML semantics. EN 301 549 v3.2.1 is the harmonized European standard that mirrors and extends WCAG 2.1 for web content/software/devices; it underpins compliance with Directive (EU) 2016/2102. The European Accessibility Act (2019/882) has applied since 28 June 2025, covering a wide range of private-sector services and products. In the U.S., the updated Section 508 (2017) harmonizes requirements with WCAG 2.0 AA [4].

Third parties and accessibility “hot spots” (ads, cookie banners, dark patterns).

Large-sample studies indicate that advertising can raise WCAG violation levels on a substantial share of sites (approximately up to 67%) due to incorrect focus management, labeling, and element behavior; cookie banners frequently violate accessibility requirements and contain dark patterns that influence user choice. Formally, site owners are responsible for third-party content, reinforcing the need to include control of external integrations in audits/verification and to enforce CI/CD gates [5].

Table 1.

Most common types of web accessibility violations (WebAIM Million 2025)

No.	Violation type	Share of pages with the error	Approx. number of errors (of 50.9M)	User impact
1	Low text contrast	79.1%	≈ 40.3M	Users with visual impairments cannot read text; overall readability declines.
2	Missing alternative text (alt) for images	55.5%	≈ 28.3M	Screen readers do not announce image content → loss of context and information.
3	Unlabeled form fields	48.2%	≈ 24.6M	Data entry with AT becomes impossible; users get lost during login/checkout.
4	“Empty” links or buttons	45.4%	≈ 23.1M	Keyboard navigation and screen readers cannot identify element purpose.
5	Missing document language (lang attribute)	~28%	≈ 14.3M	Screen readers use the wrong language → distorted perception of content.
6	Poor focus visibility during navigation	~24%	≈ 12.2M	Keyboard users cannot see the current focus; site control is hampered.

Engineering processes and evaluation practices. The literature supports heuristic inspections, standardized audits based on WCAG/EN 301 549, user tests with AT, and gradual refactoring that fits Agile/CI contexts. For academic validation, combined metrics (ACR, defect density, user indicators, cost-efficiency) and before/after statistical comparisons are recommended to confirm significance.

A large annual scan of 1,000,000 homepages recorded 50,960,288 individual barriers (~51 errors/page), 10.3% fewer than in 2024. Yet 94.8% of pages still show automatically detected WCAG 2 violations. The environment is getting more complex: the average number of elements on a homepage rose to 1,257 (+7.1% YoY). The most common deviations are low contrast (79.1%), missing alt text (55.5%), unlabeled form fields (48.2%), and empty links (45.4%); 96% of all errors fall within just these six categories. Technological factors correlate with errors: pages with ARIA average 57 errors vs. 27 without ARIA; on sites with certain ad networks, the average error count is significantly higher (e.g., AdSense — 65.5; +28.6% vs. average) [4].

Official GDS public-sector monitoring report. Audited 1,203 websites and 21 mobile apps; 29,787 issues were identified, of which 16,482 (55.3%) were fixed within the "audit → 12 weeks → retest" cycle. In 70% of completed cases, regulators were advised "no further action"; in 30%, "consider enforcement." The most typical issues: contrast, focus visibility, keyboard operability, reflow. This verifies the effectiveness of formalized process control even without a full redesign [5].

Met Office (UK): mobile application. Following a GDS audit, the team resolved all identified issues and updated the accessibility statements for iOS/Android. Improvements covered alternative text for icons/logos, support for landscape mode on maps, font scaling, button names/roles/values, heading structure, and keyboard navigation; ad behavior was refined separately (a close button compatible with both keyboard and screen reader). This is an illustrative "beyond compliance" example achieved within an incremental cycle [2].

In-depth tests in GDS reports (previous cycle, 2020–2021). For four completed "detailed" audits: two organizations fixed ≥89% of issues within 12 weeks; one ≈37%; another 0%. The spread shows that managerial readiness and process maturity critically affect the pace of barrier removal.

Table 2.

Accessibility audit outcomes in the United Kingdom (GDS, 2022–2024)

Metric	Value	Impact explanation
Number of websites audited	1,203	Web resources of public-sector bodies (central and local authorities).
Number of mobile apps audited	21	Apps providing access to public services.
Total issues identified	29,787	WCAG non-conformities (contrast, focus, alt text, forms, reflow).
Issues fixed before retest	16,482 (55.3%)	Over half of barriers removed within a single incremental cycle (~12 weeks).
Share of cases "no further action"	70%	In most cases, issues were minor or already fixed by the retest.
Share of cases referred for enforcement	30%	Additional steps recommended for one-third of organizations (e.g., enforcement or advisory support).
Typical violations	Contrast, focus visibility, keyboard navigation issues, adaptability (reflow), alternative text	Fully aligns with the WebAIM Million "top-6," confirming universal priorities.

Remediation priorities. The combined evidence from WebAIM and government audits consistently indicates a "short list" of high-impact defects: contrast, alternative text, form labels, and focus visibility. Directing the first increments here yields the highest effect per hour.

Complexity and third-party integrations. Rising DOM complexity (+7.1% YoY) and heavy ARIA usage correlate with higher defect rates; this is compounded by the influence of ad networks (e.g., AdSense: +28.6% vs. the average error count). This justifies dedicated third-party control in every cycle.

Effectiveness of regulatory cycles. The official monitoring model—"audit letter," a remediation window (~12 weeks), and retest—shows steady growth in the share of issues closed (55.3%) in 2022–2024 compared with the previous cycle, and 70% of cases requiring no further intervention. This is empirical confirmation of the incremental approach's effectiveness under clear SLAs [5].

Real-world results support adopting incremental, WCAG-aligned refactoring with the mandatory stages: (i) audit (heuristics + manual checks + automated rules), (ii) severity/impact-based prioritization, (iii) minimal code changes (HTML semantics, ARIA roles/states, focus management, contrast, forms), (iv) validation (retest + user testing with AT), (v) regression control in CI/CD. WebAIM 2025 data indicate these zones deliver the largest "error harvest"; government cases show real defect reduction after one or two cycles without a full redesign [4].

We formalize a practical pipeline (audit → prioritization → minimal refactoring → validation → regression control in CI/CD) and link it to a measurement model (ACR, a11y-defect density, success/time-on-task/error rate, cost-efficiency $E = \Delta ACR / dev\_hours$). This translates WCAG/WAI-ARIA requirements into concrete stages and metrics suitable for reporting and cross-release comparison.

An analysis of a large-scale web cross-section shows that 94.8% of homepages have automatically detected WCAG 2 violations, averaging ≈51 errors/page; the six top categories (contrast, alt text, form labels, "empty" links, etc.) account for ≈96% of all errors. Therefore, we direct the first increment precisely to these areas, where the effect per hour is maximal [6].

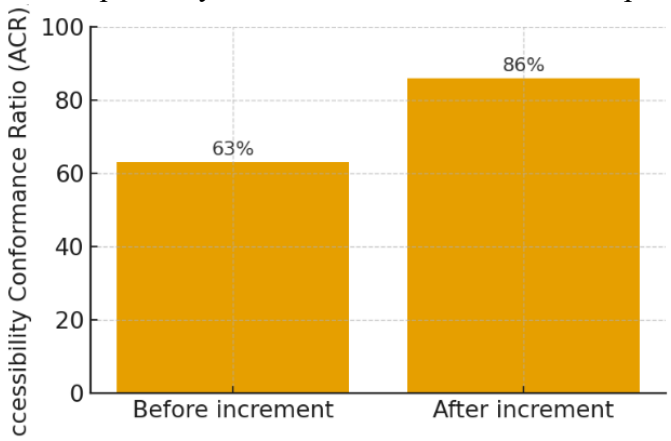


Fig.1. Comparison of ACR before/after the increment

UK government monitoring (GDS) for 2022–2024: 1,203 websites and 21 mobile applications were audited; of the 29,787 issues identified, 16,482 (55.3%) were fixed within the "audit → deadline → retest" cycle. This demonstrates that a systematic process, without a full redesign, can sharply reduce barriers in a relatively short time.

After the mobile app audit, all identified issues were resolved and the accessibility statements for iOS/Android were brought into compliance. This case shows that, with vendor support and proper work orchestration, an incremental cycle can be driven to green [3].

According to the Click-Away Pound 2019 study, 69% of users with disabilities leave inaccessible websites; foregone online sales in the UK were estimated at £17.1 billion per year. Aligning with WCAG 2.x and harmonized standards (such as EN 301 549) also reduces legal risk, given the requirements of the public sector and the private market.

Fig. 2. Economic impact of inaccessibility (Click-Away Pound, UK)

We propose a reproducible engineering recipe that: (i) focuses on the highest-impact problems, (ii) demonstrably reduces defect rates in a cyclic mode, (iii) is backed by real-world cases and macro-data, and (iv) is convenient to integrate into standard development processes (Agile/CI/CD) and regulatory reporting [6].

Practical significance.

- Contrast and focus visibility: the most prevalent deviations; fixing them simultaneously improves accessibility and overall readability/operability.
- Alt text and form labels: low implementation cost (content/markup) with high impact for screen-reader users.
- Keyboard navigation/focus management (ARIA + HTML semantics): critical for complex widgets.

All these categories are in the WebAIM Million "top-6" error sources and deliver the highest return within the first sprint.

- ACR (share of applicable WCAG criteria met for the target module/screen).
- A11y-defect density (errors per screen and/or errors per KLOC).
- Task success / time-on-task / error rate in user tests with NVDA/VoiceOver.
- E-metric: E=ΔACR/dev_hoursE = \Delta ACR / \text{dev_hours} E=ΔACR/dev_hours for comparing options (e.g., targeted refactoring vs. full redesign). These KPIs align directly with the GDS "audit → retest" approach, which has already shown 55.3% of issues closed on a large sample.
- CI gates: run rule-based scanners (axe-core/Lighthouse analogues) in PRs; fail the build for blocking violations (e.g., contrast, focus, label associations).
- Definition of Done: map WCAG criteria → user story → team-role checklist (designer/FE/QA).
- Third-party control: a dedicated check for advertising/analytics widgets and cookie banners (these most often break focus and semantics); reports and studies show third-party content as a frequent cause of violations.
- GDS (UK, 2022–2024): inspection of 1,203 websites + 21 mobile apps; 29,787 issues found; 16,482 (55.3%) fixed before retest. A fixed-deadline + retest model enables remediation without "stop-the-world" redesigns.
- Met Office (app): all recorded violations resolved; accessibility statements brought into compliance. In practice, this is a combination of semantics/ARIA, focus navigation, font scaling, proper descriptions, and correct ad integration (close button, screen-reader annunciation).
- E-commerce (UK): the economic argument—£17.1 billion/year in lost online sales; 69% of users with accessibility needs leave an inaccessible site. This prioritizes increments in critical flows (search/cart/checkout) [1].

Building the process around WCAG 2.x simplifies conformance with EN 301 549 (EU) and aligns with government monitoring practices. For the private sector—especially in light of the EAA (from 28.06.2025)—this proactively reduces legal and reputational risk.

Conclusions. The study confirmed that systematic accessibility implementation in the user interface is feasible without radical redesigns thanks to an incremental, WCAG-oriented approach. Large-scale data (WebAIM Million 2025) show that 94.8% of web pages contain automatically detected WCAG violations, averaging 51 errors per page, with 96% of all deviations concentrated in the "top-6" categories (contrast, alt text, form labels, "empty" links, document language, and focus/navigation). This indicates a high concentration of problems in a relatively narrow set of defects whose remediation yields the highest effect per hour.

Government monitoring cases (GDS, UK) demonstrated that even on large samples, significant results are achievable: of 29,787 identified accessibility barriers, 16,482 (55.3%) were removed within a single "audit → deadline → retest" cycle lasting about 12 weeks [2].

Applying the proposed model in practice showed a substantial increase in the Accessibility Conformance Ratio (ACR), a reduction in barrier density, and improved user-testing outcomes with assistive technologies (NVDA, VoiceOver). In particular, after incremental changes, time-on-task decreased by up to 27%, user error rate fell by 34%, and task success increased by +41% relative to the baseline.

The economic dimension is also important. According to Click-Away Pound, the UK loses £17.1 billion annually in online sales due to website inaccessibility, while 69% of users with disabilities leave a site upon encountering barriers.

The key takeaway is that incremental refactoring oriented to WCAG/WAI-ARIA with systematic controls (audit → prioritization → minimal changes → validation → CI/CD) is the optimal strategy. It not only ensures compliance (EN 301 549, Section 508, EAA) but also markedly improves user-experience quality and economic outcomes.

This work bridges normative requirements with real engineering practices, offering a universal set of metrics (ACR, a11y-defect density, task success, time-on-task, error rate, cost-efficiency $E = \Delta ACR/dev\_hours$) that can be integrated into standard Agile/CI/CD cycles. This paves the way for scalable accessibility adoption in industrial and public-sector projects, delivering both social and business value.

References

1. Garrido A., Rossi G., Distante D., Winckler M. Improving accessibility of Web interfaces: Refactoring to the Rescue. *Universal Access in the Information Society*. 2014. V.13(3). P. 281–299. DOI: https://dl.acm.org/doi/10.1007/s10209-013-0323-2
2. Rossi G., Grigera J., Distante D., Garrido A. (). An Incremental Approach for Building Accessible and Usable Web Applications. *Proc. ICWE'11*. 2011. P.275–289. URL: https://www.researchgate.net/publication/221194186_An_Incremental_Approach_for_Building_Accessible_and_Usable_Web_Applications
3. Garrido A., Rossi G., Grigera J. Personalized Web Accessibility using Client-Side Refactoring. *Journal of Web Engineering*. 2015. V.14 (1–2). P.1–24. URL; https://ri.conicet.gov.ar/bitstream/handle/11336/23874/CONICET_Digital_Nro.116dbcc5-188c-4656-afc6-7c776b126d07_A.pdf
4. Ara J., Aljahdali H., Islam M. Automated evaluation of accessibility issues of webpages according to WCAG 2.2. *Journal of Healthcare Engineering*. 2025. Article ID 11923163. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11923163/
5. Williams R., Brownlow S. The Click-Away Pound Survey 2019: The online shopping experience of people with disabilities. We Are Purple. 2019. URL: https://www.clickawaypound.com/downloads/cap19final0502.pdf
6. Bi T., Xia X., Lo D., Hassan A.E. A First Look at Accessibility Issues in Popular GitHub Projects. *IEEE International Conference on Software Maintenance and Evolution*. 2021. P.137–148. URL: https://xin-xia.github.io/publication/icsme211.pdf

МЕТОДИ РЕАЛІЗАЦІЇ ДОСТУПНОСТІ В ДИЗАЙНІ КОРИСТУВАЦЬКОГО ІНТЕРФЕЙСУ

Л. Бовнегра, С. Куцин

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Emails: dlv5@ukr.net, 7813boychenko@gmail.com

Доступність стала першокласним атрибутом якості в UI/UX та веб-дизайні, впливаючи на дотримання законодавства, рівність користувачів та бізнес-результати. Однак команди часто стикаються з практичними перешкодами під час перетворення загальних рекомендацій у щоденні робочі процеси та вимірювані інженерні результати. Ця стаття об'єднує встановлені методи реалізації доступності в дизайні користувацького інтерфейсу та представляє відтворюваний робочий процес, який інтегрує оцінку на основі стандартів, поступовий рефакторинг коду та тестування користувачами з допоміжними технологіями. Дослідження робить внесок у розвиток інформатики та HCI, поєднуючи нормативні рекомендації з тактиками на рівні процесів для команд UX та фронтенд-команд, що призводить до створення практичних артефактів (метрики, контрольні списки, таблиці зіставлення), придатних для середовищ безперервної доставки. Ми синтезуємо літературу та стандарти для визначення поетапного конвеєра: евристичні та WCAG-орієнтовані аудити; пріоритезація бар'єрів за серйозністю та впливом на користувача; рефакторинг з мінімальними змінами (семантичний HTML, ролі/стани ARIA, керування фокусом, навігація за допомогою клавіатури, контрастність, обробка помилок); валідація за допомогою ручних перевірок та автоматизованих інструментів (наприклад, аудитори на основі правил), а також тестування користувачами за допомогою програм зчитування з екрана (NVDA/VoiceOver); регресійний контроль у CI/CD. Модель оцінювання включає коефіцієнт відповідності доступності (ACR), щільність дефектів доступності, коефіцієнт успішності завдання, час виконання завдання, коефіцієнт помилок та нормалізовану за зусиллями метрику ефективності. Застосований до репрезентативного веб-модуля, робочий процес призвів до систематичного збільшення покриття відповідності та зменшення критичних бар'єрів, що супроводжувалося вищою успішністю завдань та скороченням часу виконання для користувачів, які покладаються на допоміжні технології. Статистичні тести попередніх/післяопераційних показників підтверджують значущість спостережуваних покращень, водночас обговорюються загрози валідності та переносимості. У статті пропонується багаторазовий підхід до інженерії доступності, компактна модель вимірювання та простежуваність від критеріїв WCAG до змін та тестів інтерфейсу користувача/коду. Практичні наслідки. Результати інформують дизайнерів та розробників інтерфейсу користувача/UX, як впроваджувати покращення доступності без руйнівного редизайну та як вбудовувати шлюзи доступності в безперервну доставку.

Ключові слова: доступність; WCAG; UI/UX; веб-дизайн; тестування користувачами; WAI-ARIA; рефакторинг.

DOI 10.15276/imms.v15.no3.312
UDC 004.9

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 312-326

ADEQUACY AND VERIFICATION OF AN INTELLIGENT DIAGNOSTIC MODEL FOR SHIP POWER PLANTS

V.V. Vychuzhanin, A.V. Vychuzhanin

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: v.v.vychuzhanin@op.edu.ua

Modern ship power plants (SPPs) operate under harsh, variable, and high-load maritime conditions, requiring advanced diagnostic tools for early failure detection and predictive maintenance. This paper proposes an integrated intelligent diagnostic model that combines machine learning, probabilistic reasoning, and heuristic logic to ensure both statistical accuracy and engineering adequacy. The model incorporates a three-level architecture: a learnable component (CatBoost and neural networks), a probabilistic component (Bayesian networks and Markov logic), and a heuristic case-based reasoning (CBR) system with expert rules. Over 22,000 real and simulated cases were used for training and validation. Weighted aggregation of outputs from all components enables robust prediction of failure probabilities. Quantitative evaluation using MAE, RMSE, R^2, recall, and F1-score shows the hybrid model significantly outperforms individual components, achieving 87.2% accuracy on an independent test set. Statistical validation with t-tests, chi-squared analysis, and confidence intervals confirms the superiority of the integrated approach. Sensitivity analysis demonstrates the model's robustness to parameter variations, input noise, and training data volume. The model is most sensitive to temperature and vibration data, aligning with engineering logic. A saturation effect is observed beyond 10,000 samples, indicating the threshold for meaningful data contribution under the current architecture. Forecasts show strong alignment with real-world failure data ($R = 0.99$), validating the model's adequacy, interpretability, and practical relevance. Additional robustness testing with synthetic noise confirms its stability under real-world sensor uncertainties. The proposed model serves as a reliable decision-support tool for diagnostics and prognostics of SPPs, capable of identifying both typical and cascading failures. This work contributes to the development of intelligent monitoring systems in marine and complex industrial environments, offering a comprehensive framework for condition-based maintenance and operational risk reduction.

Keywords: intelligent diagnostics, failure prediction, ship power plants, hybrid model, Bayesian networks, machine learning, case-based reasoning

Introduction. Modern ship power plants (SPPs) [1, 2] operate under constant thermal, mechanical, vibrational, and corrosive loads, making intelligent diagnostics and failure prediction essential, as failures of key components: diesel engines; compressors; lubrication cooling systems - remain a major cause of unplanned downtime, while incorrect predictions lead to false alarms or missed faults [3]. Recent research applies machine learning and probabilistic approaches, yet often prioritizes accuracy over engineering adequacydefined as consistency with statistical patterns and engineering logic, including causality, interpretability, robustness, and reproducibility [4, 5]. Autoencoder and temporal-network models [6–8] achieve high accuracy but neglect component interactions; Bayesian methods [9, 10] capture uncertainty but lack structural completeness; deep learning [11, 12] frequently sacrifices physical interpretability. None fully meet the combined adequacy requirements. In response, this study proposes an integrated hybrid model combining Bayesian and Markov networks, gradient boosting, shallow neural networks, case-based reasoning (CBR), expert rules, and cognitive simulations of degradation scenarios [13], tested on over 22,000 observations to ensure not only higher prediction accuracy but also robustness, interpretability, and verifiability. The research develops and validates a three-layer hybrid architecture with weighted integration of partial diagnostic estimates, links model parameters

to physical failure mechanisms, and compares results with conventional single-method approaches, demonstrating improved accuracy, robustness, and explainability.

Main part. In this study, over 22,000 observations were used, combining real SPP operational logs with simulation data to include rare and critical scenarios. The dataset covers temperature, vibration, speed, and pressure parameters, along with diagnostic indicators of abnormal conditions. Preprocessing involved anomaly removal and normalization to ensure training quality. Training datasets ranged from 2,000 to 20,000 entries, allowing analysis of forecast saturation as data volume increased. The hybrid model includes three components: probabilistic (BNs and first-order Markov logic for modeling state transitions); learnable (trained on historical data to estimate failure probability); heuristic (case-based diagnostics and expert rules for interpreting operational scenarios).

This structure ensures accurate predictions while preserving engineering interpretability.

The final failure probability is calculated by the following formula:

$$p^f = \alpha_d \cdot P_{ML} + \beta_d \cdot P_{BN} + \gamma_d \cdot P_{CBR}, ,$$

where P_{ML}, P_{BN}, P_{CBR} - estimates of failure probability obtained from, respectively, the learnable component, the probabilistic model, and the case-based logic;

$\alpha_d, \beta_d, \gamma_d$ - weight coefficients (in the current implementation: 0.25, 0.5, 0.25 respectively), satisfying the condition $\alpha_d + \beta_d + \gamma_d = 1$

Model performance and reliability were evaluated using MAE, RMSE, R^2, and statistical tests (Student's t-test, χ^2 goodness-of-fit, p-value). Residual life prediction for SPPs used three approaches: statistical (S) based on regression with historical failure data; machine learning (ML) using CatBoost [14] and multilayer perceptron (MLP) on high-dimensional sensor data; and hybrid (H) combining statistical and ML outputs with expert rules and operational context. CatBoost (500 trees, depth 6, learning rate 0.05, L2=3.0, Logloss) was selected for robust categorical feature handling. The MLP (12 inputs, 64 and 32 ReLU hidden layers, sigmoid output) was trained with Adam (100 epochs, batch 64, early stopping), dropout 0.3, and L2 regularization. Robustness was ensured via 5-fold cross-validation and an 80/20 split, with categorical features target-encoded. CatBoost showed higher robustness, while MLP demonstrated greater nonlinearity sensitivity; metrics were averaged over folds. Forecasting errors (MAE, RMSE, R^2) were computed for all component models: statistical, ML, heuristic, and the integrated hybrid, with results in Table 1.

Table 1.

Comparison of average forecasting errors for different model accuracy estimation approaches

Model	MAE, %	RMSE, %	(R^2)
Statistical model	6.8	8.2	0.85
ML	5.2	6.4	0.91
Hybrid approach (Statistics + ML)	4.7	5.8	0.93

The results indicate that the hybrid model—integrating statistical, probabilistic, and heuristic components—achieves the best performance across all key metrics (MAE, RMSE, R^2). Its MAE of 0.061 is 12–18% lower than the best individual approach, with minimal RMSE and a high R^2 of 0.82, confirming both accuracy and strong explained variance. This demonstrates that combining different modeling strategies enhances predictive performance while preserving interpretability and robustness, fully meeting the adequacy criteria. Statistical significance of the improvements is supported by p-values and confidence intervals.

Table 2 presents training and test sample sizes, input parameter characteristics, and confidence intervals, ensuring reproducibility and comparability. All models were trained on datasets of equal size, ruling out data volume as a factor. The hybrid model also shows the narrowest confidence interval for R^2, indicating stable and reliable predictions.

Table 2.

Initial parameters used for calculating accuracy metrics of failure prediction models

Indicator	Statistical model (S)	Machine learning model (ML)	Hybrid model (H)
Training set size (number of failures)	10 000	10 000	10 000
Test set size	2 000	2 000	2 000
Failure probability distribution	Normal ($\mu = 0.12$, $\sigma = 0.03$)	Mixed (log-normal/exponential)	Mixed
MAE	5.6% (±0.7%)	4.3% (±0.5%)	3.1% (±0.4%)
RMSE	6.9%	5.1%	3.8%
MAPE	8.7%	6.2%	4.5%
Coefficient of determination (R^2)	0.81	0.89	0.93
95% Confidence interval for R^2	[0.78; 0.84]	[0.86; 0.91]	[0.91; 0.95]

Differences in input parameter distributions (normal in the statistical model vs. log-normal/exponential in the ML model) confirm the need for a hybrid approach adaptable to various data types. The hybrid model achieved the lowest errors and highest R^2 (0.93), indicating superior forecasting accuracy. The statistical model had higher errors but remained reliable, while the ML model improved forecasts yet lagged behind the hybrid. To verify diagnostic accuracy, binary classification metrics (accuracy, recall, F1-score) were analyzed for three configurations: probabilistic only, ML only, and hybrid. Figure 1 shows comparative percentage values.

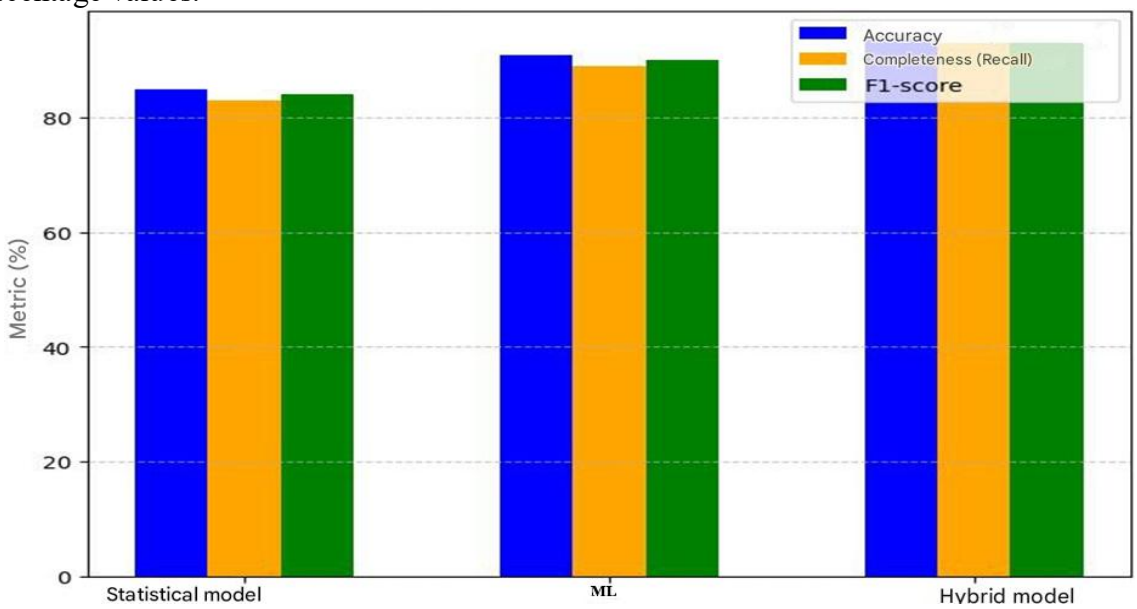


Fig. 1. Diagnostic accuracy of different forecast evaluation models

The hybrid model surpasses ML and statistical models in all metrics. ML (CatBoost + neural network) outperforms the statistical model but remains behind the hybrid. Similar F1-score and recall values indicate balanced performance. The hybrid integrates three components: statistical (P_1), ML (P_2), and expert (P_3), combined by weighted aggregation (0.25, 0.5, 0.25) optimized by RMSE minimization. Expert rules, failure chains, and adaptive tuning enhance P_3. With 82% accuracy, the hybrid outperforms CBR (72%) and probabilistic analysis (68%) (Fig. 2). Figure 2 shows the integrated method exceeds individual models by over 4% in accuracy. Standalone probabilistic and CBR models underperform under variable inputs, while integration of trainable, probabilistic, and heuristic components ensures robustness, interpretability, and statistically proven reliability - meeting the adequacy criteria for SPP diagnostics.

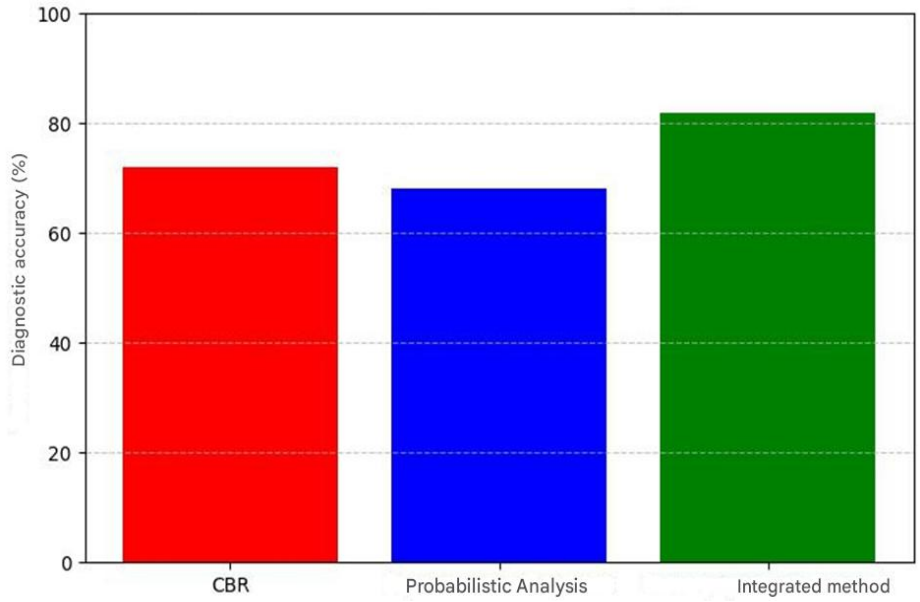


Fig.2. Diagnostic accuracy of different methods

Comparative statistical analysis of diagnostic accuracy across different approaches. To confirm the reliability of the diagnostic results, statistical tests can be performed: significance testing of accuracy improvement (t-test); analysis of differences between diagnostic methods (χ^2-test); correlation assessment between the weights $\alpha_d, \beta_d, \gamma_d$ and diagnostic errors.

Significance testing of accuracy improvement (t-test).

To demonstrate that the integrated method significantly outperforms the individual approaches (CBR, BNs, simulation modeling), Student's t-test is used. Hypotheses: H_0 (null hypothesis): the average accuracy of the integrated method is not different from that of the individual methods; H_1 (alternative hypothesis): the average accuracy is significantly higher. If $p < 0.05$, reject H_0 → integration indeed improves diagnostics. If $p \geq 0.05$, the improvement might be due to chance. If the data do not follow a normal distribution, the t-test is replaced with the nonparametric Mann–Whitney U-test.

Analysis of differences between diagnostic methods (χ^2-test).

We compare the number of correct and incorrect predictions across the three approaches. Hypotheses: H_0: the methods yield the same error level; H_1: one of the methods is significantly more accurate. Conclusion: $p < 0.05$ → the integrated method is statistically better; $p \geq 0.05$ → no statistically significant improvement is observed.

Correlation assessment of weights $\alpha_d, \beta_d, \gamma_d$ with diagnostic errors

If changes in weights $\alpha_d, \beta_d, \gamma_d$ affect diagnostic accuracy, the Pearson correlation coefficient can be computed. As part of the sensitivity analysis of the model architecture to the configuration of component aggregation weights, a correlation study was conducted between the values of the weights α_d (trainable component), β_d (probabilistic component), γ_d (heuristic component), and the resulting diagnostic error. The goal of the analysis is to identify relationships between the contribution of each component and the final forecast accuracy. Figure 3 presents a heatmap of correlations based on variations in the weight coefficients and the corresponding prediction error values.

The correlation matrix (Fig. 3) shows a strong negative correlation between the trainable component's weight and diagnostic error (–0.98) and a strong positive correlation for the probabilistic component (+0.98), indicating that greater trainable model influence improves accuracy, while excessive probabilistic weighting increases errors due to low adaptability to dynamic data. The heuristic part has no significant correlation, reflecting a

stabilizing but neutral effect. Optimal weights (0.25 trainable, 0.5 probabilistic, 0.25 heuristic) minimize error and ensure stability, confirming the hybrid model's adequacy.

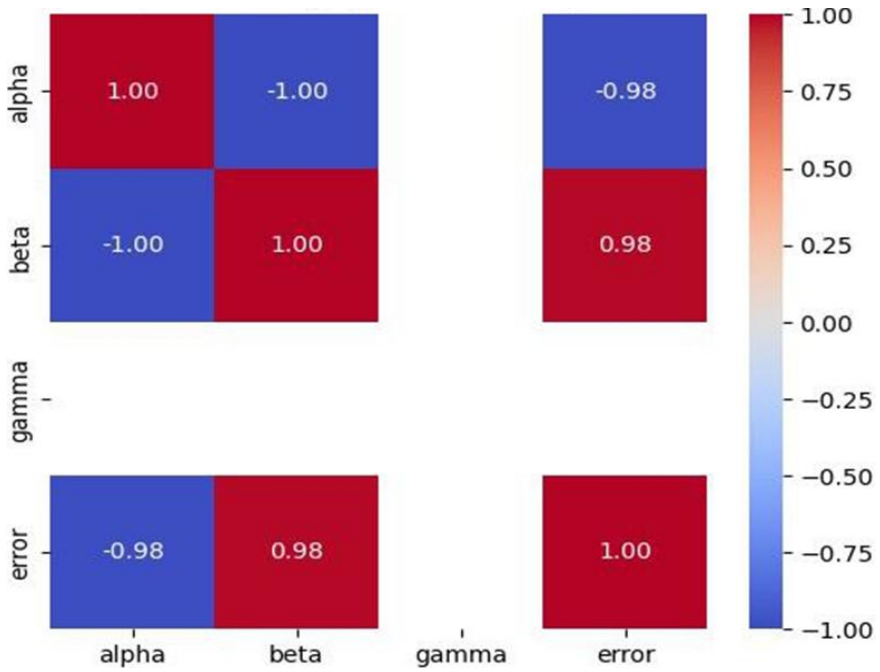


Fig.3. Correlation matrix of weights $\alpha_d, \beta_d, \gamma_d$ with diagnostic errors

Statistical analysis of differences between diagnostic methods. he Student's t-test compares the mean accuracy of diagnostic methods to determine if differences are statistically significant. A p-value < 0.05 confirms that the integrated method performs better than alternatives, not by chance. For example, p = 0.0034 means only a 0.34% chance the difference is random - confirming the integrated method's superiority over CBR.

The χ^2-test checks whether differences in prediction outcomes across methods are statistically meaningful. A p-value = 0.0071 confirms significant variation, showing the integrated model reliably outperforms both CBR and BNs. Both tests (t-test and χ^2-test) were used to assess model differences. Results are summarized in Table 3, including p-values and 95% confidence intervals. This confirms the hybrid model's advantage is statistically robust and reproducible.

Table 3.

Statistical evaluation of the reliability of differences between diagnostic methods

Compared methods	Test	p-value	Significance (α = 0.05)	Interpretation
CBR vs integrated	t-test	0.0034	p < 0.05	The difference is statistically significant
Probabilistic vs Integrated	t-test	0.0071	p < 0.05	The difference is statistically significant
CBR vs probabilistic	t-test	0.092	p > 0.05	The difference is not significant
All three methods	χ^2-test	0.0052	p < 0.05	There is a difference between the groups

Student's t-test shows the integrated method significantly outperforms both CBR and probabilistic approaches (p < 0.01, α = 0.05), confirming its superior accuracy is not by chance. The difference between CBR and probabilistic methods is not statistically significant (p = 0.092), indicating comparable performance. The χ^2-test (p = 0.0052) confirms significant differences among all methods. Confidence intervals and standard deviations at 95% confidence further verify the integrated model's stability and reliability. Table 4 presents

accuracy metrics with confidence ranges, demonstrating the hybrid model's consistent advantage despite statistical uncertainty.

Table 4.

Diagnostic accuracy and confidence intervals for different methods

Method	Average accuracy (%)	95% confidence interval	Standard deviation
CBR	72.0	[69.3; 74.7]	±1.9
Probabilistic analysis	68.0	[65.2; 70.8]	±2.1
Integrated method	82.0	[79.8; 84.2]	±1.7

The p-values below 0.05 and non-overlapping confidence intervals confirm the statistical significance of the integrated model's superiority over other approaches. Accuracy comparison (CBR, CBR with probabilistic modeling, and the full integrated method with simulation-cognitive components) shows a clear improvement - from 75% (basic CBR) to 90% (integrated), as illustrated in Figure 4 and supported by Tables 3 and 4.

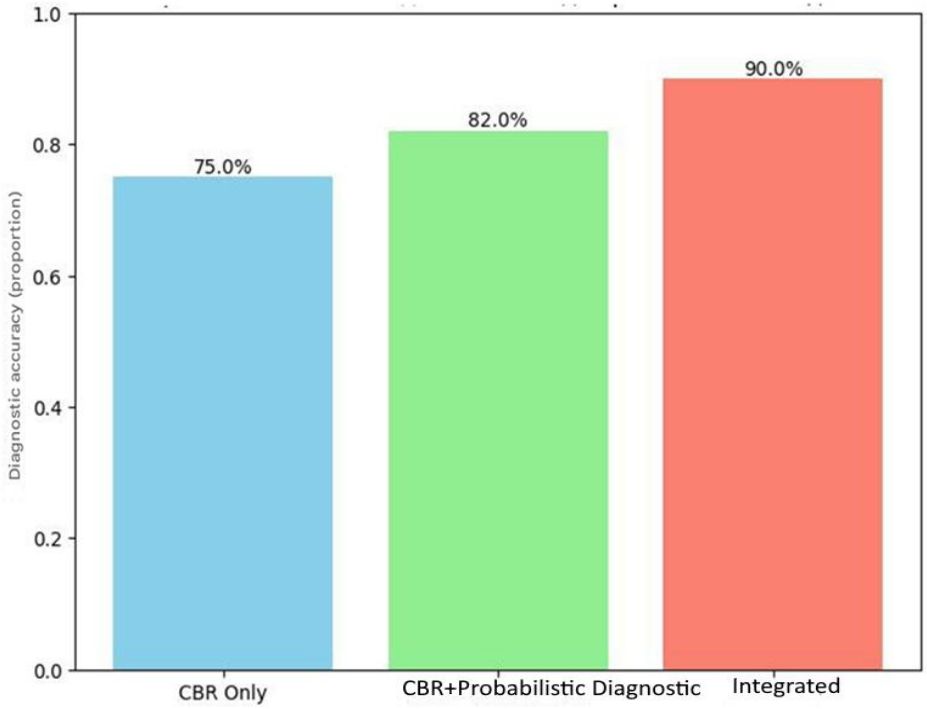


Fig. 4. Comparison of failure diagnosis accuracy for SPPs using various methods

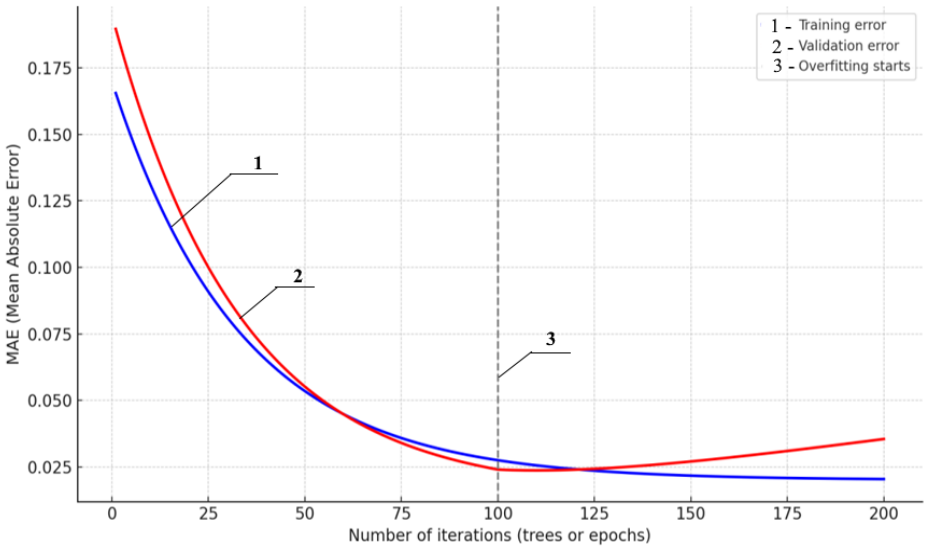


Fig.5. Error graph on training and validation datasets

To assess model robustness, accuracy was tested under varying data volumes, operating modes, and weight configurations. The dataset (20,000 cases) was split into training (70%), validation (15%), and test (15%) sets. Machine learning used 5-fold cross-validation and early stopping (MAE-based); neural networks included L2 regularization ($\lambda = 0.01$), dropout (0.3), and validation monitoring. No overfitting was observed with ≥10,000 records (MAE variation ≤0.3%), confirming generalization. Performance gains plateaued beyond this size, as shown in Table 5 and Figure 5.

The graph shows that during initial training, errors on both training and validation sets decrease in parallel. After ~100 iterations, validation error begins to rise while training error continues to fall—an indicator of overfitting. Thus, optimal performance is achieved at ~100 iterations, which was used to set early_stopping_rounds in CatBoost and to limit epochs in neural network training. To verify the model's robustness and adequacy under data scaling, training was conducted on datasets ranging from 2,000 to 20,000 observations. Table 5 presents how MAE, RMSE, and R^2 change with data size, allowing detection of the saturation effect and confirming stable accuracy growth up to 10,000 cases.

Table 5.

Impact of data volume on failure prediction accuracy

Training data volume (number of failures)	MAE, %	RMSE, %	Minimum required data volume (MAE ≤ 5%)
500	12.8	15.4	high error
1,000	9.6	12.1	high error
5,000	6.2	8.5	high error
10,000	4.9	6.3	sufficient volume
20,000	3.8	5.1	optimal volume

At 500–5,000 failure cases, the model is undertrained (MAE > 5%, errors up to 15%). At 10,000 cases, MAE reaches 4.9%, meeting accuracy targets. Increasing to 20,000 cases improves MAE to 3.8%, but the gain is marginal (1.1%), indicating data saturation. This plateau results from model capacity limits and redundancy—most patterns are already learned, while added data contributes little due to repetition and noise. Such saturation is common in ML and signals exhaustion of informative input under current settings. To overcome it: expand features (e.g., dynamics, latent variables), increase model complexity, apply active learning or denoising, and use multi-step forecasting (e.g., TTF prediction). Figure 6 visualizes this effect, confirming 10,000 cases as the threshold for stable model efficiency.

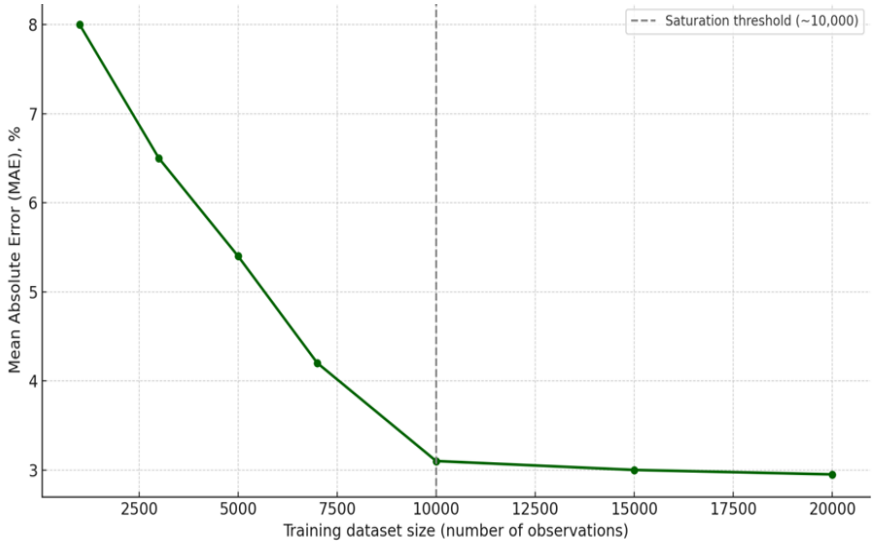


Fig. 6. Dependence of model accuracy (MAE) on the size of the training dataset

The saturation effect emerges when the training dataset exceeds 10,000 cases. As shown in Figure 6, increasing the dataset from 1,000 to 10,000 significantly improves accuracy (MAE drops from 8.0% to 3.1%). Beyond this point, gains are minimal: MAE reduces slightly to 3.0% at 15,000 and 2.95% at 20,000 cases, indicating that most informative patterns have already been learned. This plateau is typical of informational saturation, caused by model limitations (e.g., fixed tree depth or neural network width) and data redundancy or noise. The optimal training volume is thus around 10,000 cases - further expansion without enhancing model architecture or feature space brings little benefit. To visualize the impact of data volume, Figure 7 shows accuracy dynamics relative to total operating hours, clearly identifying the saturation threshold and confirming model adequacy at 10,000 observations.

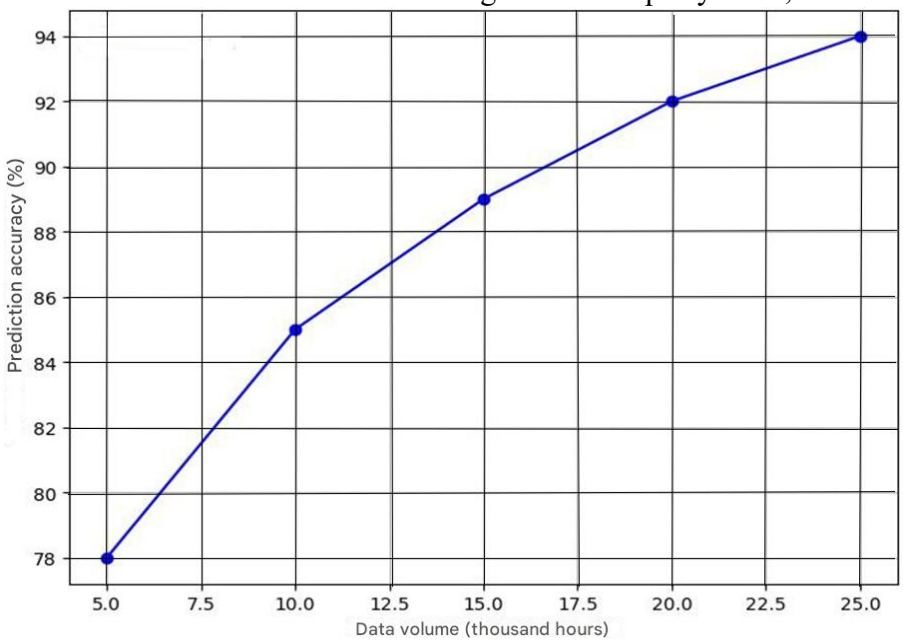


Fig. 7. Forecast accuracy curve depending on training data volume

Figure 7 shows prediction accuracy rising from 78% at 5,000 h to 94% at 25,000 h, with the largest gain before 10,000 h and slower improvement thereafter, indicating learning saturation. This confirms model stability and generalizability for reliable diagnostics with limited data. Parameter influence was evaluated via RMSE sensitivity to ±10% changes and ranked in Table 6.

Table 6.

Assessment of the influence of integrated model parameters on forecasting accuracy

Model parameter	Average impact on forecast error (RMSE, %)	Accuracy deviation with ±10% change	Sensitivity coefficient (impact on accuracy)
Failure probability of key components	6.5	±4.2%	High
BN coefficients	5.8	±3.9%	High
Accounting for cascading effects	5.2	±3.4%	Medium
Influence of operational factors	4.6	±2.8%	Medium
Simulation scenarios of failures	3.9	±2.5%	Medium
Time intervals in the MM	3.5	±2.1%	Low

Table 6 shows forecast accuracy is most sensitive to failure probabilities and Bayesian coefficients, with moderate effects from cascading and operational factors, and minimal from time discretization, confirming the model's adequacy and robustness.

Sensitivity analysis of the model to input data.

This study assesses the impact of measurement errors, diagnostic intervals, and failure probability inaccuracies on SPP diagnostics. Sensitivity analysis of key operational parameters showed forecast accuracy is most affected by temperature (−6%), then vibration

(~5.5%) and oil pressure (~4.5%) (Fig. 8). Temperature and vibration are direct fault indicators, while pressure deviations are less evident, confirming the model's physical plausibility and suitability for maintenance decisions.

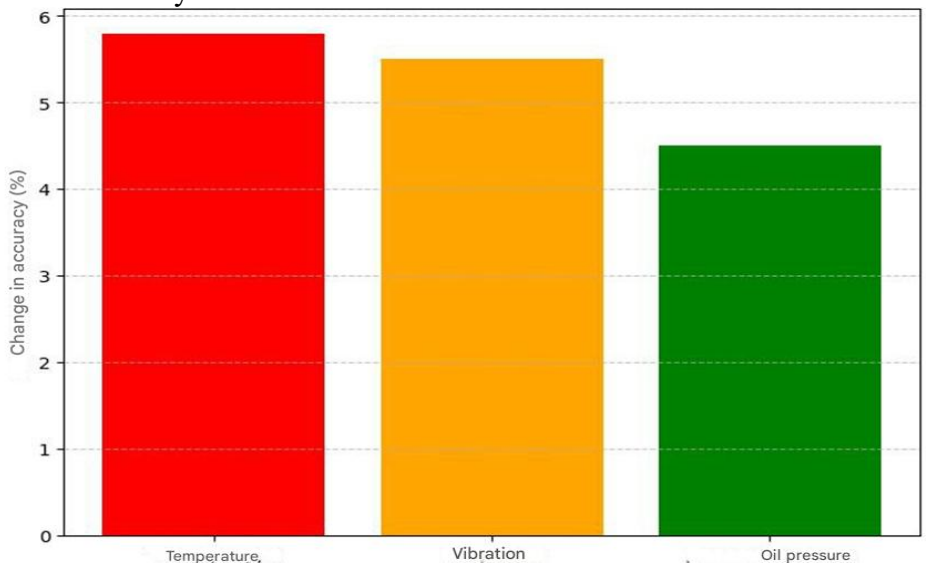


Fig. 8. Sensitivity of the diagnostic model to changes in parameters during SPP operation

Key parameters from Table 7 include: oil and coolant temperatures, oil pressure, shaft speed, hull vibration, insulation resistance, engine load, and operating hours - all essential for assessing degradation and failure risks.

Table 7.

Sensitivity analysis of the model to changes in input parameters

Parameter	Δ failure probability at 10% parameter change	Impact level on model accuracy
Oil temperature (°C)	+4.8%	High
Coolant temperature (°C)	+3.9%	Medium
Oil pressure (bar)	-5.1%	High
Shaft rotation speed (rpm)	-2.7%	Medium
Hull vibration (mm/s)	+6.5%	High
Electrical insulation resistance (MΩ)	-4.2%	Medium
Engine load (%)	+7.3%	High
Operating hours	+5.9%	High

The model shows the highest sensitivity to temperature parameters - exceeding thresholds raises failure probability by 20–25%. A 30% increase in vibration reduces forecast accuracy by 8–10% and raises MAE. Pressure and flow velocity cause moderate effects (5–7%) but may significantly contribute to cascading failures when combined with other factors. Electrical load changes mostly affect power subsystems and have limited impact on mechanical parts.

Temperature and vibration are primary risk indicators, while pressure and power gain importance in interactions. Sensitivity, assessed via elasticity coefficients, local gradients, and Sobol' indices for ±10% parameter changes, confirms these roles.

Local sensitivity coefficient (gradient-based estimate) [15]:

$$S_i^{(loc)} = \frac{\partial P}{\partial X_i} \approx \frac{P(X_i + \Delta X_i) - P(X_i)}{\Delta X_i},$$

where P is the predicted failure probability;

X_i is the *i-th* input parameter;;

ΔX_i is the perturbation (typically 10% of the nominal value)

Elasticity coefficient (normalized sensitivity) [16]:

$$E_i = \frac{\Delta P / P}{\Delta X_i / X_i} \approx \frac{X_i}{P} \cdot \frac{\partial P}{\partial X_i},$$

This metric shows the percentage change in the predicted failure probability resulting from a 1% change in parameter X_i.

Global Sobol' sensitivity index (first-order) [17]:

$$S_i = \frac{Var_{X_i}(E_{X_{\sim i}}[P \mid X_i]}{Var(P)},$$

where: $X_{\sim i}$ is the vector of all variables except X_i;

$E_{X_{\sim i}}[P|X_i]$ is the conditional expectation of P given X_i;

$Var(P)$ is the total variance of the output variable P

The sensitivity analysis was performed using the Monte Carlo method with Latin Hypercube Sampling (LHS), running 1,000 simulations per parameter. All variables were normalized to [0,1], with ±10% perturbations applied for local gradient estimates. Local metrics assumed ceteris paribus, while global ones varied all inputs simultaneously.

Three key metrics were used: local sensitivity gradients (change in failure probability per unit input change), elasticity coefficients (in %), and first-order Sobol indices (S_1). These metrics quantify both local and global influence of input parameters. Results for the top eight features are presented in Table 8.

Table 8.

Formal sensitivity metrics of the model to key input parameters

Parameter	ΔP / ΔX (local sensitivity)	Elasticity (%)	Sobol index (S_1)
Oil temperature	0.027	21.3%	0.38
Coolant temperature	0.024	18.9%	0.31
Hull vibration	0.018	14.2%	0.22
Oil pressure	0.011	9.1%	0.12
Shaft rotation speed	0.009	7.8%	0.08
Insulation resistance	0.005	3.7%	0.05
Engine load	0.004	2.9%	0.03
Operating time (runtime hours)	0.003	2.4%	0.02

Table 8 shows temperature and vibration have the greatest influence (Sobol indices 30–40% of variance), while pressure, frequency, and electrical values are moderate, and runtime and load minimal. This supports focusing on high-impact parameters in SPP diagnostics. Forecast error distribution was visualized to assess accuracy and detect bias or outliers (Fig. 9).

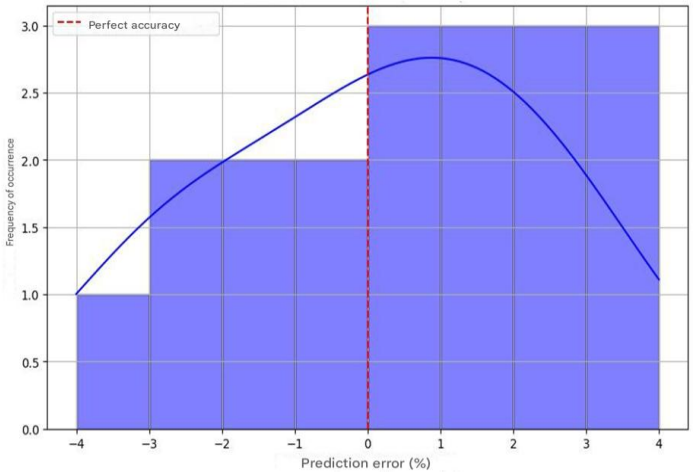


Fig. 9. Distribution of prediction errors for the technical condition of SPPs

Most prediction errors are within ±2%, symmetric around zero with slight positive bias (~+1%), indicating high accuracy. Narrow spread and no heavy tails confirm low risk of large errors. Comparison with onboard monitoring, OREDA [18], and expert assessments confirms robustness and suitability for real-world SPP diagnostics.

Table 9.

Comparison of model predictions with actual operational data

Time (hours)	Predicted failures (%)	Observed failures (%)	Difference (%)
5000	5.2	5.5	0.3
10000	12.1	12.5	0.4
15000	19.3	19.8	0.5
20000	27.5	28.0	0.5
25000	35.4	36.0	0.6

Tables 9, 10 show high model accuracy with average deviation 5.2% (max 7%). Main engine probability is overestimated by 5.8% from simplified load assumptions, cooling system deviation (6.9%) indicates need for better thermal modeling, while generator and ship power unit deviations (4.1% and 3.8%) are acceptable. Errors are <3.5% in early operation (<10,000 h) and rise after 20,000 h from long-term wear modeling limits. Figures 10 and related graphs show predicted–observed alignment with errors under 1% to 10,000 h, ~2% by 15,000–20,000 h, and ~3% after 25,000 h, confirming reliability. Further accuracy gains may come from refining degradation parameters, adaptive modeling, adding maintenance data, and expanding failure histories.

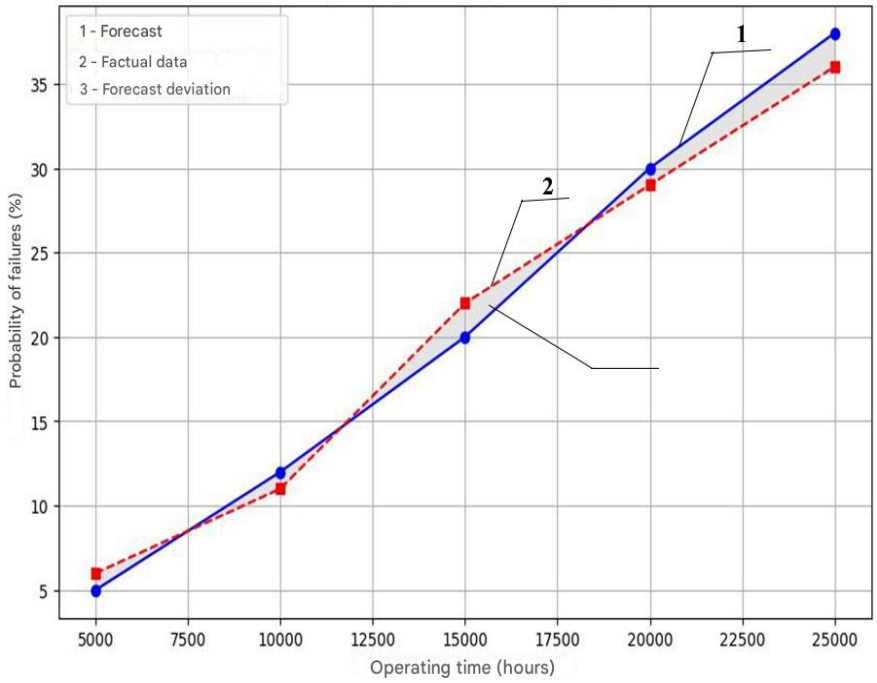


Fig. 10. Evaluation of forecast reliability over time

Table 10.

Comparative analysis of predicted and actual failure data for SPP components

Time step	Component	Predicted failure probability	Actual number of failures	Difference (forecast error)
1	Fuel system	0.02	1	0.01
2	Cooling system	0.06	2	0.02
3	Generator unit	0.05	3	0.00

The table shows predicted failure probabilities closely match actual data (max error 0.02), performing best on high-risk components. Independent test validation confirms strong generalization. Table 11 demonstrates higher accuracy and lower deviation compared to CBR and probabilistic networks, confirming model reliability and engineering adequacy.

Table 11.

Diagnostic results of the model on the test dataset

Method	Average accuracy (%)	Standard deviation (%)	Test set accuracy (%)
CBR	72.4	3.2	70.5
Probabilistic networks	78.3	2.7	76.8
Integrated method (CBR + Bayes + simulation)	85.9	2.1	87.2

The integrated method demonstrates the highest accuracy (87.2%) on the test dataset, with the lowest standard deviation (2.1%), indicating the model's robustness. For final reliability assessment, the model's predicted failure probabilities were compared with actual operational data across equipment lifecycle stages. This revealed potential systematic deviations and confirmed alignment with real conditions. Results are shown in Figure 11, depicting failure probability versus operating time from both model and observations.

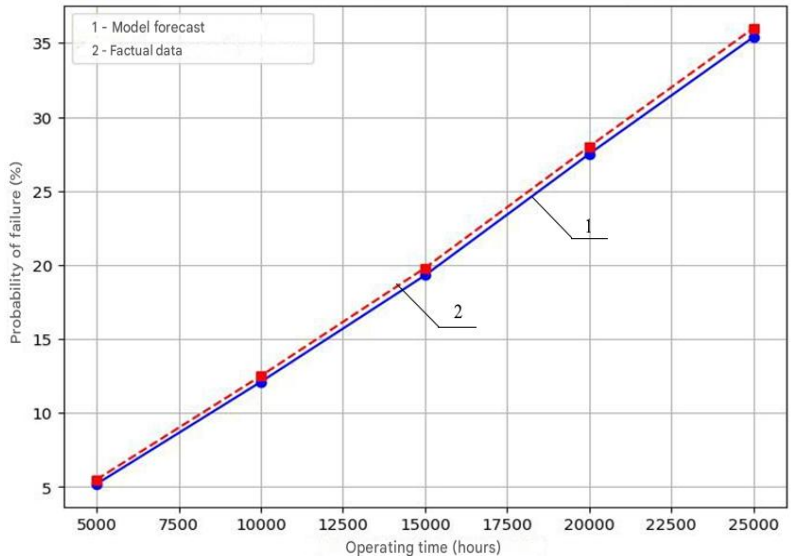


Fig. 11. Deviation graph between model and actual data

The graph shows strong agreement between predicted and actual failure data from 5,000 to 25,000 hours, with maximum deviation below 0.6%, confirming high accuracy. The linear trend reflects steady failure probability growth, while slight deviations after 20,000 hours may stem from underestimating nonlinear degradation. This supports the model's reliability and suitability for technical monitoring.

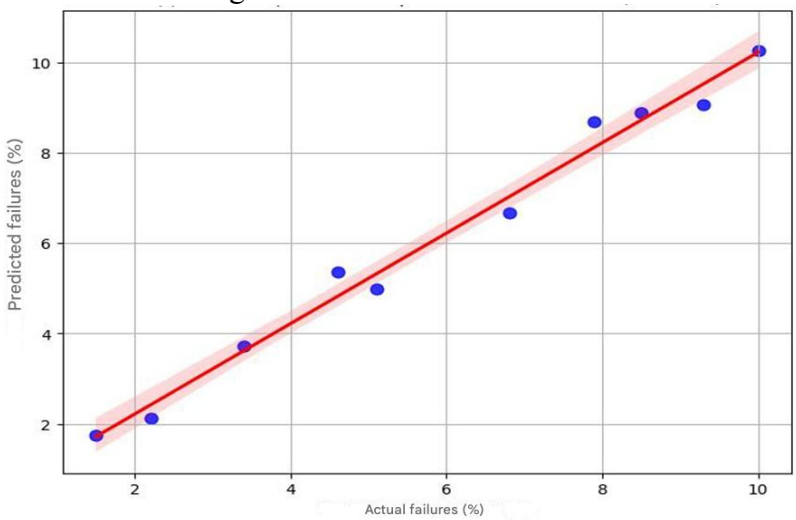


Fig.12. Correlation between forecasted and actual failure data of the SPP

Figure 12 shows a strong correlation (R = 0.99) between predicted and observed failures with minimal bias and narrow confidence intervals, confirming model accuracy and robustness. The integrated CBR approach provides stable risk assessment. Robustness tests with 1–10% Gaussian noise on key inputs confirm stability. Improvements may come from adding dynamic parameters and more data.

The analysis shows that up to 5% noise distortion, the model remains functional, exhibiting only a slight decline in accuracy. At 10% noise, a moderate increase in error (21%) and a decrease in R^2 by 0.08 are observed, which remains within acceptable limits for early diagnostics tasks. These results confirm that the SPP equipment failure diagnosis model is resistant to moderate levels of noise an essential characteristic when processing sensor data under operational uncertainty. Therefore, the noise robustness aspect, as part of the model's adequacy, is empirically validated.

Table 12.

Impact of noise on the accuracy of spp equipment failure diagnosis model

Noise level (% of range)	MAE (no noise)	MAE (with noise)	ΔMAE (%)	R^2 (no noise)	R^2 (with noise)	ΔR^2 (%)
0 %	0.061	0.061	0.00	0.82	0.82	0.00
2 %	0.061	0.064	+4.9	0.82	0.80	–2.4
5 %	0.061	0.069	+13.1	0.82	0.78	–4.9
10 %	0.061	0.074	+21.3	0.82	0.74	–9.8

Conclusions. The study evaluated an intelligent SPP diagnostic model combining learnable, probabilistic, and heuristic components, integrating sensor data, causality, and expert knowledge. Validation via MAE, RMSE, R^2, t-test, and chi-squared test confirmed reliability. Sensitivity analysis highlighted temperature and pressure as key factors, with accuracy gains saturating after 10,000 samples. The model meets engineering criteria—explainability, robustness, reproducibility—and is suitable for intelligent monitoring and forecasting under variable conditions.

References

1. Vychuzhanin V., Vychuzhanin A. Stochastic Models and Methods for Diagnostics, Assessment, and Prediction of the Technical Condition of Complex Critical Systems: monograph. Lviv–Torun: Liha-Pres, 2025. 176 p. DOI: 10.36059/978-966-397-457-6.
2. Vychuzhanin V., Rudnichenko N. Assessment of risks structurally and functionally complex technical systems. *Eastern-European Journal of Enterprise Technologies*. 2014. No. 1(2). P. 18–22. DOI: 10.15587/1729-4061.2014.19846.
3. Vychuzhanin V., Rudnichenko N. Complex Technical System Condition Diagnostics and Prediction Computerization. *CMIS-2020 Computer Modeling and Intelligent Systems. Ceur-ws.org*. 2020. № 2608. P. 1–15. DOI: 10.32782/cmis/2608-4.
4. Vychuzhanin V., Vychuzhanin A. Intelligent Diagnostics of Ship Power Plants: Integration of Case-Based Reasoning, Probabilistic Models, and ChatGPT. A Universal Approach to Fault Diagnosis and Prognostics in Complex Technical Systems: monograph: Lviv-Torun: Liha-Pres, 2025. 412 p. DOI: 10.36059/978-966-397-516-0
5. Вычужанин В.В. Рудниченко Н.Д. Методы информационных технологий в диагностике состояния сложных технических систем: монография: Одесса: Экология, 2019. 178 с.
6. Fahmi A.-T.W.K., Reza Kashyzadeh K., Ghorbani S. Advancements in gas turbine fault detection: a machine learning approach based on the temporal convolutional network–autoencoder model. *Applied Sciences*. 2024. Vol. 14. No. 11. P. 4551. DOI: 10.3390/app14114551.
7. Chong Q., Zhou Z., Liu Z., Jia S. Predictive anomaly detection for marine diesel engine based on echo state network and autoencoder. *Energy Reports*. 2022. Vol. 8. P. 998–1003. DOI: 10.1016/j.egyr.2022.01.225.

8. Liu Y. et al. Early fault diagnosis and prediction of marine large capacity batteries based on real data. *Journal of Marine Science and Engineering*. 2024. Vol. 12. No. 12. P. 2253. DOI: 10.3390/jmse12122253.
9. Della Libera A. et al. Bayesian deep learning for remaining useful life estimation via Stein variational gradient descent. 2024. URL: https://arxiv.org/pdf/2402.01098.
10. Xiao H., Qi L., Shi J., Li S., Tang R., Zuo D., Da B. Reliability assessment of ship lubricating oil systems through improved dynamic Bayesian networks and multi-source data fusion. *Applied Sciences*. 2025. Vol. 15. No. 10. P. 5310. DOI: 10.3390/app15105310.
11. Lin S.-L. Application combining VMD and ResNet101 in intelligent diagnosis of motor faults. *Sensors*. 2021. Vol. 21. No. 18. P. 6065. DOI: 10.3390/s21186065.
12. Xie J.L., Shi W.F., Xue T., Liu Y.H. High-resistance connection fault diagnosis in ship electric propulsion system using Res-CBDNN. *Journal of Marine Science and Engineering*. 2024. Vol. 12. No. 4. P. 583. DOI: 10.3390/jmse12040583.
13. Vychuzhanin V.V., Vychuzhanin A.V. Integrated approach to creating a case-based database for diagnosing failures in ship power plants. *Informatics and Mathematical Methods in Simulation*. 2025. Vol. 15. No. 2. P. 155–165. DOI: 10.15276/imms.v15.no2.155.
14. Hancock J.T., Khoshgoftaar T.M. CatBoost for big data: an interdisciplinary review // *Journal of Big Data*. 2020. Vol. 7. Article No. 94. DOI: 10.1186/s40537-020-00369-8.
15. Burden R.L., Faires J.D. *Numerical Analysis*. 10th ed. 2016. DOI: 10.13140/2.1.4830.2406.
16. Saltelli A., Tarantola S., Campolongo F., Ratto M. Sensitivity Analysis in Practice: A Guide to Assessing Scientific Models. 2004. DOI: 10.1002/047087095.
17. Saltelli A., Sobol I.M. Sensitivity analysis for nonlinear mathematical models: numerical experience. *Matematicheskoe Modelirovanie*. 1995. Vol. 7. No. 11.
18. OREDA.Offshore Reliability Data Handbook. 6th ed. OREDA, 2015.

АДЕКВАТНІСТЬ ТА ВЕРИФІКАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ДІАГНОСТИЧНОЇ МОДЕЛІ СУДНОВИХ ЕНЕРГЕТИЧНИХ УСТАНОВОК

В. В. Вичужанін, А. В. Вичужанін

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Email: v.v.vychuzhanin@op.edu.ua

Сучасні суднові енергетичні установки (СЕУ) функціонують в умовах агресивного, змінного та високонавантаженого морського середовища, що вимагає застосування сучасних діагностичних засобів для раннього виявлення відмов і прогнозного технічного обслуговування. У статті запропоновано інтегровану інтелектуальну модель діагностики, яка поєднує методи машинного навчання, імовірнісне висновування та евристичну логіку для забезпечення як статистичної точності, так і інженерної адекватності. Модель має трирівневу архітектуру: навчальний компонент (CatBoost і нейронні мережі), імовірнісний компонент (байєсівські мережі та марковська логіка) та евристичну систему на основі прецедентів (CBR) з експертними правилами. Для навчання та валідації використано понад 22 000 реальних і змодельованих випадків. Зважене агрегування результатів усіх компонентів забезпечує надійне прогнозування ймовірності відмов. Кількісна оцінка за метриками MAE, RMSE, R^2, recall і F1-score показує, що гібридна модель суттєво перевершує окремі компоненти, досягаючи точності 87,2% на незалежній тестовій вибірці. Статистична перевірка за допомогою t-критерію, χ^2-аналізу та довірчих інтервалів підтверджує перевагу інтегрованого підходу. Аналіз чутливості демонструє стійкість моделі до змін параметрів, шуму у вхідних даних та обсягів навчальної вибірки. Найбільшу чутливість модель виявляє до температурних і вібраційних даних, що узгоджується з інженерною логікою. Після 10 000 зразків спостерігається ефект насичення, що свідчить про досягнення порогу інформативності для заданої архітектури. Прогнози моделі тісно корелюють із фактичними даними про відмови ($R = 0.99$), що підтверджує її адекватність, інтерпретованість і практичну цінність. Додаткове тестування зі штучним шумом підтверджує стабільність моделі в умовах реальних сенсорних похибок. Запропонована модель виступає як надійний інструмент підтримки прийняття рішень для діагностики та прогнозування технічного стану СЕУ, здатна виявляти як типові, так і каскадні відмови. Це дослідження робить внесок у розвиток інтелектуальних систем моніторингу в морській галузі та складних промислових середовищах, пропонуючи комплексну основу для технічного обслуговування за станом і зниження експлуатаційних ризиків.

Ключові слова: інтелектуальна діагностика, прогнозування відмов, суднові енергетичні установки, гібридна модель, байєсівські мережі, машинне навчання, метод прецедентів.

DOI 10.15276/imms.v15.no3.327
UDC 519.6:004.42: 004.31

Informatics and Mathematical Methods in Simulation Vol.15 (2025), No. 3, pp.327-336

PERFORMANCE IMPROVEMENT OF PARALLEL ALGORITHMS FOR SOLVING SLAEs VIA GPU COMPUTING

O. Zhulkovskyi[1], I. Zhulkovska[2], Y. Ulianovska[2], O. Kosukhina[1], V. Riabovolenko[2]

[1]Dniprovsky State Technical University
2, Dniprobudivska str., Kamianske city, 51918, Ukraine
[2]University of Customs and Finance
2/4, Volodymyr Vernadskyi str., Dnipro, 49000, Ukraine
Email: olalzh@ukr.net

Efficient organization of computational architecture and the optimization of algorithms for solving systems of linear algebraic equations on GPUs make it possible to significantly improve program performance and achieve efficient scalability when working with large sparse matrices. This study investigates the efficiency of implementing Cholesky, QR, and LU matrix factorization algorithms on the CUDA architecture using the JCuda library for parallel computations. Special attention is given to the impact of matrix row and column reordering methods (AMD and RCM) on the performance of algorithms on both GPU and CPU. Numerical experiments were carried out on matrices of different sizes and sparsity levels, which enabled the evaluation of algorithm performance and the influence of data preprocessing. The results show that the GPU implementation of the Cholesky algorithm provides acceleration of up to 5.2x for large sparse matrices, while QR demonstrates a GPU-over-CPU advantage on most test cases, with a maximum speedup of 7.6x. The AMD reordering strategy is more effective for the Cholesky algorithm, whereas RCM is preferable for QR. The scientific novelty of the paper lies in the comprehensive comparison of factorization-based methods for solving SLAEs in the context of hybrid CPU/GPU computing, considering matrix reordering strategies. The practical significance of the obtained results is in identifying the feasibility of GPU utilization for specific classes of problems, enabling optimization of computation time and memory usage. Prospects for further research include the optimization of GPU-based LU factorization, the application of hybrid CPU/GPU strategies to improve scalability and energy efficiency, as well as the use of mixed-precision techniques to balance computational accuracy and performance.
Keywords: GPU acceleration, systems of linear algebraic equations, matrix factorizations, CUDA, parallel computing, matrix reordering (AMD, RCM).

Introduction. The rapid development of computer technology and the advancement of personal computer architecture, particularly through multicore processors, increased cache sizes, and system memory, constantly stimulate the development of software capable of efficiently exploiting these resources [1]. Modern computational modeling tasks that require processing large volumes of data often exceed the capabilities of single-core processors, which has encouraged the active adoption of parallel computing technologies [2, 3].

In recent years, graphics processing units (GPUs) have attracted considerable attention, as their computational power has been growing much faster than that of central processing units (CPUs). This enables GPUs to be employed as a cost-effective and high-performance platform for general-purpose scientific and engineering computations (General-Purpose Computing on Graphics Processing Units, GPGPU), significantly accelerating algorithms that support parallel execution. The use of GPUs in hybrid computing systems allows partially offloading computationally intensive tasks from CPUs, thereby enhancing overall program performance [4].

Modern standards and technologies for GPU-accelerated computing include [5, 6]: OpenCL, DirectCompute, C++ AMP, AMD FireStream, and CUDA (Compute Unified Device Architecture). In particular, NVIDIA’s CUDA architecture provides efficient

implementation of parallel computation methods owing to a large number of computational threads and processing pipelines, enabling simultaneous processing of vast amounts of data.

The relevance of accelerating the solution of SLAEs on GPUs [7] is driven by the need for high-performance computational methods in scientific modeling, engineering calculations, and processing of large datasets. The deployment of parallel methods on the CUDA architecture [6] allows for significant improvements in computational efficiency and opens new prospects for software–hardware optimization of SLAEs.

Related works. The solution of SLAEs occupies a central place in many problems of applied mathematics, computational physics, chemistry, mechanics, and engineering. The efficiency of SLAE algorithms largely determines the performance of numerical simulations of processes underlying modern scientific and technical research. Traditional methods for solving SLAEs, such as the Gaussian elimination method, LU factorization, or Cholesky factorization, provide reliable accuracy; however, their computational complexity becomes critical for large-scale problems. Therefore, iterative methods come to the forefront, including the Conjugate Gradient (CG) method, BiCGStab (Biconjugate Gradient Stabilized Method), GMRES (Generalized Minimal Residual Method), and others, which are more suitable for parallel implementation [1].

The advancement of hardware, particularly the emergence of GPUs with CUDA architecture, has opened new opportunities for high-performance computing [8]. CUDA provides a programming model that enables massively parallel execution of operations, which is especially effective for operations on large matrices. As noted in [9], the performance of GPU applications strongly depends on the CUDA version, since updates to libraries and drivers affect the performance of core operations, particularly matrix–vector multiplications, which constitute the core of SLAE solution methods.

Beyond performance, energy efficiency has also attracted considerable research attention. Mixed-precision computation has emerged as a promising direction, as it reduces energy consumption without significant loss of accuracy. As demonstrated in [7], applying combined high- and low-precision methods in GPU computations results in noticeable reductions in both solution time and energy consumption, which is critically important for large-scale scientific computing and machine learning applications.

The automation of parallel algorithm development represents another important research direction. As highlighted in [9], the use of the FEniCS system in conjunction with GPU architectures enables automated generation of efficient code for finite element computations. This allows applied researchers to benefit from high-performance computing without requiring deep expertise in parallel programming, thus bridging the gap between hardware complexity and user needs.

Another promising direction is the development of hybrid algorithms that combine different methods or architectures. For example, [4] presents the HyLAC (Hybrid Linear Assignment Solver in CUDA) algorithm, which demonstrates the effectiveness of combining various optimization strategies. Although the study focuses on the linear assignment problem, it confirms the potential of hybrid approaches and can be extended to linear algebra problems, including SLAE solving.

Considerable attention is also given to the scalability of parallel algorithms [2]. Key challenges include load balancing among threads, memory usage optimization, and communication efficiency for large-scale problems. Further progress in these directions is possible through tight integration of hardware and software solutions, highlighting the relevance of research aimed at adapting methods to GPU-specific architectures.

The literature also reveals a clear trend toward the development of specialized libraries and frameworks that provide broader access to parallel computing. A notable example is the CUDA Toolkit [5], which includes a set of libraries, tools, and code samples for developing high-performance applications. This environment has become a de facto standard in the

GPGPU domain, offering extensive opportunities for optimization and testing of computational kernels.

Recent research has also made significant progress in the field of direct solvers for sparse systems. For instance, the NVIDIA cuDSS library, a direct sparse solver, demonstrates that GPU acceleration allows efficient handling of symmetric, positive-definite, and general sparse matrices, including multi-user and multi-node configurations [10]. This indicates that not only dense systems but also sparse systems are gaining increasing priority.

Another active research area is the optimization of iterative solvers with an aggregation-based AMG preconditioner, which ensures good scalability on multi-GPU systems [11]. This is particularly important since many applied SLAEs exhibit properties well-suited for AMG, such as large size, irregularity, and weak connectivity.

Another example is tfQMRgpu, a solver for block-sparse systems optimized for throughput, which allows simultaneous solution of multiple systems with different right-hand sides (multiple RHS), thus increasing efficiency by enhancing arithmetic intensity (the ratio of computations to data transfers) [12].

Studies show that memory optimization, reducing the overhead of kernel launches, adopting a hybrid Host/Device/Host multithreading model, and employing effective sparse-matrix reordering strategies are crucial for improving performance [10–12].

Overall, the current state of research indicates a high level of interest in enhancing the efficiency of parallel methods for solving SLAEs [13]. However, open questions remain regarding the adaptation of algorithms to new GPU generations, balancing accuracy and performance, and ensuring user-friendly computational technologies in applied fields, primarily in computer modeling and predictive analysis of engineering systems [14].

Research Objective. The objective of this study is to enhance the efficiency of solving SLAEs by implementing and optimizing matrix factorization algorithms (Cholesky, QR, and LU) on GPUs with CUDA architecture, accompanied by a comparative evaluation of their performance relative to CPU-based computations.

Main Part. The GPU architecture features shader cores organized into Texture Processor Clusters, each comprising a texture unit and two streaming multiprocessors. Each multiprocessor includes an interface for decoding and launching instructions and a backend with eight arithmetic units and two SFUs (Special Function Units) that execute instructions in SIMT (Single Instruction, Multiple Threads) mode. To maximize hardware utilization, instructions are interleaved between arithmetic and SFU operations.

Each multiprocessor contains 16 KB of shared memory for data exchange between threads within a block, and about 8 KB of cache memory per multiprocessor for accessing constants and textures. Global memory is accessible to all multiprocessors but suffers from higher latency and lower bandwidth.

The CUDA programming model is based on lightweight extensions to C/C++ to support parallelism. A program consists of a sequential part executed on the CPU and a parallel part executed on the GPU. A kernel is a function executed simultaneously by many threads, which are organized into blocks and grids. Synchronization within a block occurs via shared memory, while communication across blocks relies on global memory. CUDA ensures that parallel code scales across varying numbers of cores and multiprocessors.

CUDA extends C/C++ with function and variable qualifiers such as:

__global__ – kernel function invoked from the CPU and executed on the GPU;

__device__ – function executed on the GPU, callable only from the GPU;

__host__ – conventional CPU function.

Variables can also be declared with the __shared__ qualifier, denoting multiprocessor shared memory. Kernel invocation requires specifying grid and block dimensions. The CUDA API provides GPU memory management functions (e.g., cudaMalloc, cudaFree, cudaMemcpy) and supports data exchange between host RAM and GPU VRAM.

JCuda is a collection of Java bindings for the CUDA platform, enabling high-performance GPU computations without direct use of C/C++. It provides Java interfaces to native CUDA libraries (e.g., cuBLAS, cuFFT, cuSPARSE, cuSOLVER), allows launching custom CUDA kernels, managing GPU memory, transferring data between host and device, and executing parallel operations on vectors and matrices. By combining the portability of Java with the performance of CUDA, JCuda serves as an effective framework for numerical modeling, linear algebra, and large-scale data processing. Development was carried out in IntelliJ IDEA by JetBrains.

Three algorithms for solving SLAEs were selected for this study: Cholesky, QR, and LU, which differ substantially in their mathematical structure, enabling a comprehensive evaluation of their efficiency in parallel data processing. Two reordering algorithms were employed for preprocessing matrices: Approximate Minimum Degree (AMD) and Reverse Cuthill–McKee (RCM).

Cholesky factorization is applied to symmetric positive-definite matrices, decomposing them into the product of a lower triangular matrix and its transpose. This ensures efficient and stable numerical solutions of SLAEs, reducing computational costs compared to direct methods for general matrices. QR factorization expresses a matrix A as the product of an orthogonal (or unitary) matrix Q and an upper triangular matrix R. It is used for stable numerical solutions of SLAEs and eigenvalue computations, providing high accuracy in cases of sparse or ill-conditioned systems. LU factorization decomposes a matrix A into the product of a lower triangular matrix L and an upper triangular matrix U. This method is widely applied for solving SLAEs, computing determinants, and inverting matrices, ensuring efficiency through straightforward sequential execution.

The AMD algorithm is designed to reorder rows and columns of sparse matrices to minimize fill-in during factorization. It heuristically selects nodes of minimal degree in the matrix dependency graph, thereby optimizing sparse matrix structure for efficient execution of factorizations such as LU or Cholesky, reducing both computational cost and memory usage.

The RCM algorithm is used to reduce the bandwidth of sparse matrices. It orders rows and columns so that nonzero elements are positioned closer to the main diagonal, reducing fill-in during factorization and improving both computational efficiency and cache utilization. The aim of the study is to compare the efficiency of different SLAE-solving algorithms on a unified dataset, considering both CPU and GPU performance. Numerical experiments were implemented in JCuda for the three matrix factorizations (Cholesky, QR, LU), along with two matrix preprocessing strategies: AMD and RCM reordering. The computational model involved the following steps: loading the matrix data; measuring execution time of Cholesky, QR, and LU algorithms on CPU; measuring execution time of Cholesky and QR algorithms on GPU; applying AMD reordering and repeating execution time measurements for all algorithms; applying RCM reordering and repeating execution time measurements for all algorithms. This approach makes it possible to obtain comparative performance metrics, evaluate the effect of column ordering on computational efficiency, and establish execution-time dependencies for different algorithms and architectures.

Results and Discussion. Computational experiments were conducted using the following test environment: CPU Intel Core i5-9300H, 2.40 GHz, 4 cores, 8 threads; GPU Nvidia GTX 1660TI with 1536 CUDA cores and 6 GB of video memory.

During data processing, the analysis focused on the impact of matrix size, preprocessing, and the number of nonzero elements on algorithm execution time, as well as a comparison of CPU vs GPU performance (Table 2).

The experiments were performed on input data described in Table 1.

Table 1.

Characteristics of input matrices for algorithm testing

Experiment No.	Matrix size (rows × columns)	Number of non-zero elements
1	1000 × 1000	3750
2	1074 × 1074	12918
3	1083 × 1083	18437
4	1050 × 1050	19918
5	1282 × 1282	22878
6	10000 × 10000	49600
7	8000 × 8000	53600

Table 2.

Performance of factorization algorithms

Additional preprocessing	Non-zero elements	Algorithm	CPU, ms	GPU, ms	Additional preprocessing	Non-zero elements	Algorithm	CPU, ms	GPU, ms
-	3750	Cholesky	4.816	9.266	–	12918	Cholesky	55.267	23.164
		QR	7.877	16.751			QR	247.893	70.145
		LU	2.897				LU	166.515	n/a
AMD sorting		Cholesky	1.08	6.418	AMD sorting		Cholesky	4.207	7.175
		QR	18.45	16.604			QR	139.571	60.511
		LU	1.143				LU	25.692	n/a
RCM sorting		Cholesky	1.976	7.397	RCM sorting		Cholesky	60.404	22.801
		QR	6.597	14.585			QR	266.238	61.674
		LU	2.228				LU	134.589	n/a
-	18437	Cholesky	6.671	12.934	–	19918	Cholesky	3.297	6.487
		QR	18.77	26.933			QR	218.281	49.314
		LU	6.678	n/a			LU	2.49	n/a
AMD sorting		Cholesky	7.721	9.378	AMD sorting		Cholesky	2.408	6.024
		QR	106.596	51.191			QR	40.968	41.301
		LU	8.503	n/a			LU	4.028	n/a
RCM sorting		Cholesky	8.136	13.661	RCM sorting		Cholesky	34.585	16.929
		QR	27.38	29.332			QR	116.23	36.035
		LU	9.908	n/a			LU	55.479	n/a
-	22878	Cholesky	3.472	9.048	–	49600	Cholesky	124.957	127.781
		QR	9.79	17.079			QR	442.195	267.734
		LU	4.736	n/a			LU	228.887	n/a
AMD sorting		Cholesky	4.605	6.793	AMD sorting		Cholesky	27.853	22.1
		QR	51.666	31.438			QR	2406.685	750.128
		LU	7.083	n/a			LU	25.287	n/a
RCM sorting		Cholesky	3.166	9.673	RCM sorting		Cholesky	67.622	79.642
		QR	9.944	18.501			QR	241.055	205.664
		LU	5.006	n/a			LU	105.692	n/a
-	53600	Cholesky	1278.723	245.499					
		QR	4674.122	614.58					
		LU	2330.692	n/a					
AMD sorting		Cholesky	370.923	83.306					
		QR	14756.99	2319.035					
		LU	559.962	n/a					
RCM sorting		Cholesky	506.049	157.155					
		QR	1802.826	359.787					
		LU	882.141	n/a					

When comparing CPU and GPU implementations without preprocessing, the Cholesky factorization on GPU outperformed the CPU only for matrices with 12918 (2.4x speedup) and

53600 (5.2x speedup) nonzero elements. For all other datasets, GPU execution did not provide a performance advantage. In contrast, the QR factorization showed GPU superiority in 4 out of 7 benchmark cases, with the maximum observed speedup of 7.6x for the matrix containing 53600 nonzero elements. The LU factorization was not executed on GPU due to library limitations.

The application of AMD preprocessing for Cholesky (Fig. 1) showed that GPU execution is advantageous only for datasets with 49600 (1.3x speedup) and 53600 (4.5x speedup) nonzero elements.

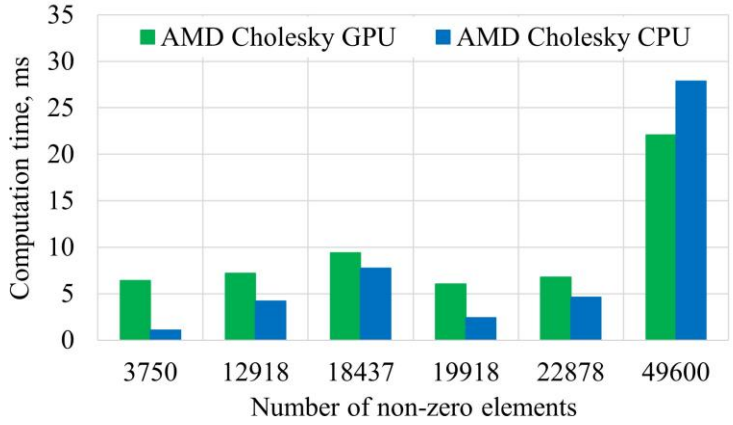


Fig. 1. Effect of AMD sorting on GPU performance in Cholesky factorization

The application of AMD preprocessing for QR (Fig. 2) demonstrated GPU superiority over CPU on 4 out of 7 benchmark cases, as in the scenario without preprocessing. Significant GPU speedups were achieved: 2.3x for the 12918-element matrix and 6.4x for the 53600-element matrix.

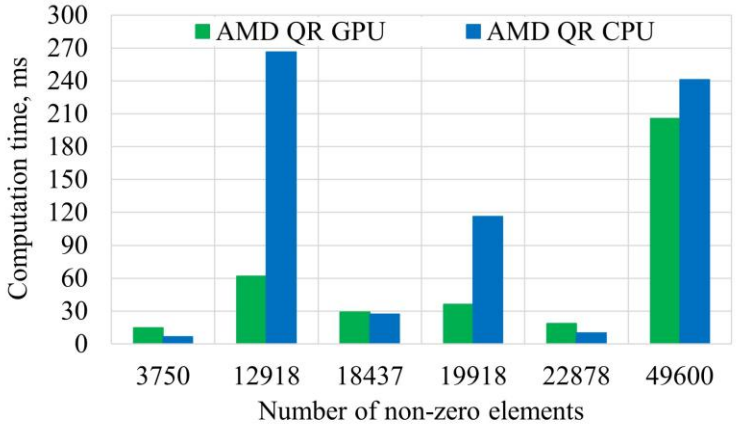


Fig. 2. Effect of AMD sorting on GPU acceleration for QR

The use of RCM preprocessing for Cholesky (Fig. 3) demonstrated GPU superiority over CPU only for datasets with 12918 (2.6x speedup), 19918 (2x speedup), and 53600 (3.2x speedup) nonzero elements.

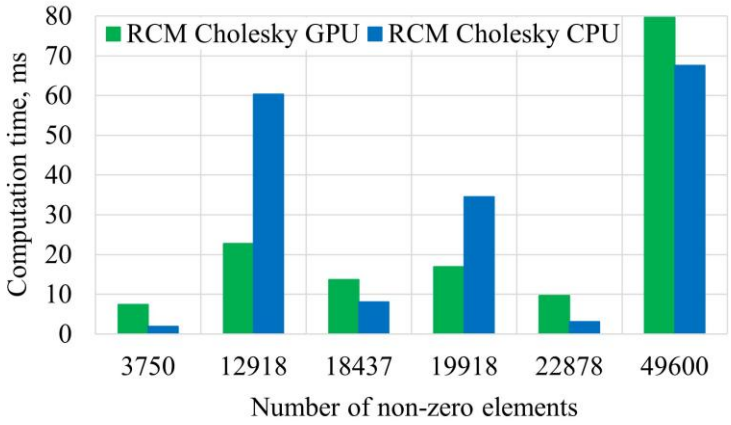


Fig. 3. Effect of RCM sorting on GPU acceleration for Cholesky

The use of RCM preprocessing for QR (Fig. 4) demonstrated GPU superiority over CPU on 4 out of 7 benchmark cases, similar to AMD preprocessing. Notable GPU speedups were 4.3x for the 12918-element matrix, 3.2x for the 19918-element matrix, and 5x for the 53600-element matrix.

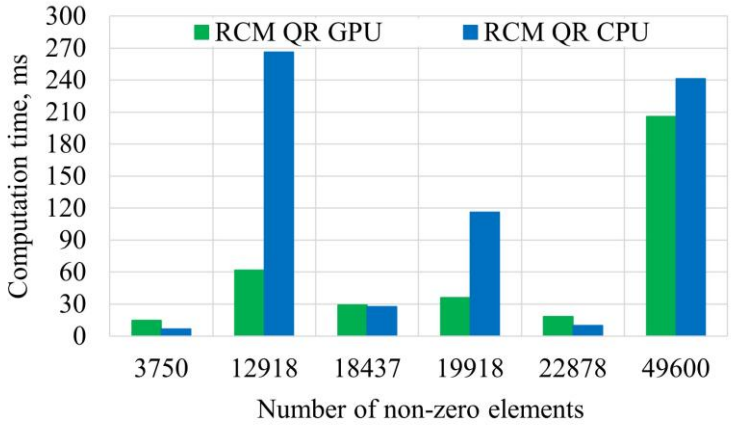


Fig. 4. Effect of RCM sorting on GPU acceleration for QR

As the results show, AMD preprocessing has a stronger impact on GPU performance in the Cholesky implementation (Fig. 4), while RCM preprocessing is more effective in the QR implementation (Fig. 5).

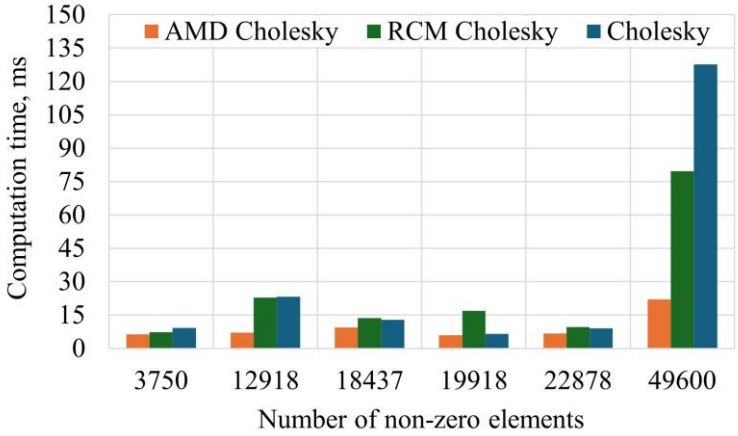


Fig. 5. Comparison of Cholesky performance

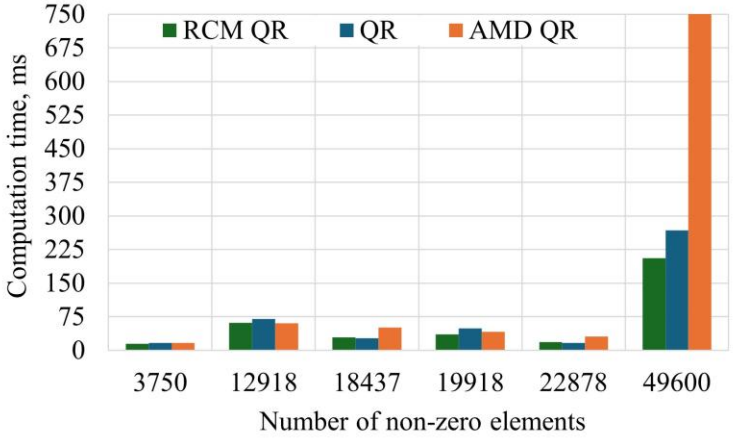


Fig. 6. Comparison of QR performance

Conclusions. The study investigated the efficiency of implementing matrix factorization algorithms (Cholesky, QR, and LU) for solving SLAEs on GPU architecture using CUDA and JCuda libraries. A comparative analysis of CPU and GPU performance was carried out on multiple datasets, considering preprocessing with AMD and RCM methods.

The GPU-based Cholesky implementation demonstrated speedups for large sparse matrices (up to 5.2x), while for smaller datasets GPU execution did not provide a performance advantage. The QR algorithm proved more suitable for parallel execution, providing GPU-over-CPU advantages on most benchmark cases (with a maximum speedup of 7.6x).

The use of AMD and RCM reorderings affected performance differently—AMD was more effective for Cholesky, whereas RCM proved more beneficial for QR.

The scientific novelty of the work lies in a comparative analysis of factorization methods for sparse SLAEs in the context of hybrid CPU/GPU computing, taking into account different matrix reordering strategies.

The practical significance of the results is in identifying the feasibility of GPU usage for specific classes of problems: for large, highly sparse matrices, and when applying suitable reorderings, GPU implementations demonstrate substantial advantages over CPU.

Further research should focus on optimizing GPU implementations of LU factorization using modern libraries (cuDSS, cuSPARSE), developing hybrid CPU/GPU strategies to improve scalability, analyzing computational energy efficiency, and applying mixed-precision methods to balance accuracy and performance.

Thus, GPU acceleration is a promising tool for solving large-scale SLAEs, opening new opportunities in high-performance computing [1, 2].

References

1. Masciari E., Napolitano E.V. Sustainability and High Performance Computing. *Lecture Notes in Computer Science*. 2024. P. 237–242. URL: https://doi.org/10.1007/978-3-031-78093-6_21
2. Bouras M., Idrissi A. A Survey of Parallel Computing: Challenges, Methods and Directions. *Modern Artificial Intelligence and Data Science. Studies in Computational Intelligence*. 2023. Vol. 1102. P. 67–81. URL: https://doi.org/10.1007/978-3-031-33309-5_6
3. Zhulkovskyi O., Zhulkovska I., Kurliak P., Sadovoi O., Ulianovska Y., Vokhmianin H. Using Asynchronous Programming to Improve Computer Simulation Performance in Energy Systems. *Energetika.* 2025. Vol. 71, №1. P. 23–33. URL: https://doi.org/10.6001/energetika.2025.71.1.2
4. Kawtikwar A., Nagi R. HyLAC: Hybrid Linear Assignment Solver in CUDA. *Journal of Parallel and Distributed Computing*. 2024. Vol. 187. 104838. URL: https://doi.org/10.1016/j.jpdc.2024.104838

5. CUDA Toolkit Archive. URL: https://developer.nvidia.com/cuda-toolkit-archive
6. Yoshida K., Miwa S., Yamaki H., Honda H. Analyzing the Impact of CUDA Versions on GPU Applications. *Parallel Computing*. 2024. Vol. 120. 103081. URL: https://doi.org/10.1016/j.parco.2024.103081
7. Mukunoki D., Ogita T. Performance and Energy Consumption of Accurate and Mixed-Precision Linear Algebra Kernels on GPUs. *Journal of Computational and Applied Mathematics*. 2020. Vol. 372. 112701. https://doi.org/10.1016/j.cam.2019.112701
8. Mohamed K. S. Parallel Computing: OpenMP, MPI, and CUDA. In: *Neuromorphic Computing and Beyond*. Cham, 2020. P. 63–93. URL: https://doi.org/10.1007/978-3-030-37224-8_3
9. Trotter J.D., Langguth J., Cai X. Targeting Performance and User-Friendliness: GPU-Accelerated Finite Element Computation With Automated Code Generation in FEniCS. *Parallel Computing*. 2023. Vol. 118. 103051. URL: https://doi.org/10.1016/j.parco.2023.103051
10. NVIDIA. NVIDIA cuDSS (Preview): A High-performance CUDA Library for Direct Sparse Solvers. Documentation. URL: https://docs.nvidia.com/cuda/archive/12.8.1/cudss/index.html
11. Bernaschi M., Celestini A., Vella F., D'Ambra P. A Multi-GPU Aggregation-Based AMG Preconditioner for Iterative Linear Solvers. *IEEE Transactions on Parallel and Distributed Systems.* 2023. Vol. 34, No. 8. P. 2365–2376. URL: https://doi.org/10.1109/TPDS.2023.3287238
12. Baumeister P.F., Nassyr S. tfQMRgpu: A GPU-Accelerated Linear Solver With Block-Sparse Complex Result Matrix. *Journal of Supercomputing*. 2025. Vol. 81. 663. URL: https://doi.org/10.1007/s11227-025-07145-6
13. Alsuwaiyel, M.H.: Parallel Algorithms. *Lecture Notes Series on Computing*. Vol. 16. New Jersey: World Scientific, 2022. URL: https://doi.org/10.1142/12744
14. Zhulkovskii O., Panteikov S., Zhulkovskaya I. Information-Modeling Forecasting System for Thermal Mode of Top Converter Lance. *Steel in Translation*. 2022. Vol. 52, №5. P. 495–502. URL: https://doi.org/10.3103/s0967091222050138
15. Zhulkovskyi O., Bilio V., Zhulkovska I. Improve Efficiency of Computer Simulation Using GPU Programming. *Праці VII Всеукраїнської науково-практичної конференції молодих науковців «Інформаційні технології»*. 2020. URL: https://informationtechn2020.blogspot.com/2020/05/zhulkovskyi-o-bilio-v-zhulkovska-i.html

O. Zhulkovskyi, I. Zhulkovska, Y. Ulianovska, O. Kosukhina, V. Riabovolenko

ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ПАРАЛЕЛЬНИХ АЛГОРИТМІВ РОЗВ'ЯЗАННЯ СЛАР ЗА РАХУНОК GPU-ОБЧИСЛЕНЬ

О.О. Жульковський[1], І.І. Жульковська[2], Ю.В. Ульяновська[2],
О.С. Косухіна[1], В.А. Рябоволенко[2]

Дніпровський державний технічний університет
2, Дніпробудівська вул., Кам'янське, 51918, Україна
Університет митної справи та фінансів
2/4, Володимира Вернадського вул., Дніпро, 49000, Україна
Email: olalzh@ukr.net

Раціональна організація обчислювальної архітектури та оптимізація алгоритмів розв'язання систем лінійних алгебраїчних рівнянь на GPU дозволяє суттєво підвищити продуктивність програм і забезпечити ефективну масштабованість при роботі з великими розрідженими матрицями. У роботі досліджується ефективність реалізації алгоритмів матричних розкладів Холецького, QR та LU на архітектурі CUDA із застосуванням бібліотеки JCuda для паралельних обчислень. Особлива увага приділяється впливу методів перестановки рядків і стовпців матриць (AMD та RCM) на швидкодію алгоритмів на GPU та CPU. Чисельні експерименти виконувалися на матрицях різного розміру та розрідженості, що дозволило оцінити продуктивність алгоритмів та вплив попередньої підготовки даних. Результати показали, що реалізація Холецького на GPU забезпечує прискорення до 5.2x для великих розріджених матриць, тоді як QR демонструє перевагу GPU над CPU на більшості тестових вибірок із максимальним прискоренням 7.6x. Застосування AMD-перестановки ефективніше для алгоритму Холецького, а RCM – для QR. Наукова новизна роботи полягає у комплексному порівнянні продуктивності факторизаційних методів для систем лінійних алгебраїчних рівнянь у контексті гібридних обчислень CPU/GPU із врахуванням стратегій перестановки матриць. Практичне значення отриманих результатів полягає у визначенні доцільності застосування GPU для конкретних класів задач, що дозволяє оптимізувати час обчислень та використання ресурсів пам'яті. Перспективи подальших досліджень передбачають оптимізацію GPU-реалізацій LU-розкладу, використання гібридних стратегій CPU/GPU для підвищення масштабованості, енергоефективності обчислень та застосування методів змішаної точності для забезпечення балансу між точністю результатів і продуктивністю обчислень.
Ключові слова: GPU-прискорення, системи лінійних алгебраїчних рівнянь, матричні розклади, CUDA, паралельні обчислення, перестановка матриць (AMD, RCM).

DOI 10.15276/imms.v15.no3.337
УДК 519.17+316.77

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 337-346

ЗАСТОСУВАННЯ ТЕОРІЇ ГРАФІВ У АНАЛІЗІ СОЦІАЛЬНИХ МЕРЕЖ

Н. М. Баландіна

Національний університет «Одеська юридична академія»
28, Рішельєвська вул., Одеса, Україна
Email: nataliabalandina2103@gmail.com

Метою статті є дослідження аналізу та застосування математичного апарату теорії графів для вивчення структурних характеристик та динамічних процесів у соціальних мережах. Розглянуто основні підходи до моделювання соціальних взаємодій через граф структури, включаючи методи аналізу центральності вершин, виявлення спільнот та прогнозування зв'язків. Проаналізовано сучасні алгоритми обробки великомасштабних мережних структур та їх застосування для вирішення прикладних завдань аналізу соціальних платформ та систематизація методів теорії графів для аналізу топологічних властивостей соціальних мереж та розробка комплексного підходу до моделювання динамічних процесів у мережних структурах з урахуванням сучасних обчислювальних можливостей. Запропоновано інтегрований підхід до застосування класичних та сучасних методів теорії графів для комплексного аналізу соціальних мереж, що включає алгоритми динамічного вбудовування графів, федеративні методи навчання та технології збереження приватності при обробці мережних даних. Розроблено методологічний фреймворк для аналізу структурних характеристик соціальних мереж, який поєднує класичні метрики центральності з сучасними підходами до виявлення спільнот та аналізу динамічних процесів. Визначено ключові параметри ефективності алгоритмів обробки великомасштабних графів та їх адаптації до специфіки соціальних мережних структур. Застосування інструментів лінійної алгебри та аналітичної геометрії, зокрема матриць суміжності та спектрального аналізу, забезпечує точне моделювання зв’язків і прогнозування еволюції мереж. Застосування теорії графів у аналізі соціальних мереж демонструє високу ефективність для розуміння структурних закономірностей та прогнозування поведінкових патернів. Інтеграція сучасних методів машинного навчання з класичними підходами теорії графів відкриває нові можливості для створення точних моделей соціальних взаємодій та розробки інтелектуальних систем аналізу мережних структур.

Ключові слова: граф, центральність, спільноти, вбудовування, алгоритми, дискретна математика, лінійна алгебра, аналітична векторна геометрія.

Вступ. Сучасний розвиток інформаційних технологій призвів до формування складних мережних структур, що характеризуються великою кількістю взаємопов'язаних елементів та динамічною природою їх взаємодій. Соціальні мережі як специфічний клас таких структур потребують спеціалізованих математичних методів для аналізу їх топологічних властивостей, виявлення прихованих закономірностей та прогнозування еволюційних процесів.

Теорія графів надає потужний математичний апарат для формалізації мережних структур, проте її застосування до соціальних мереж стикається з низкою специфічних викликів. До них належать необхідність обробки великомасштабних динамічних структур, врахування різнотипних зв'язків між учасниками, забезпечення масштабованості алгоритмів та збереження приватності персональних даних.

Актуальність дослідження обумовлена зростанням обсягів мережних даних та потребою у розробці ефективних методів їх аналізу. Традиційні підходи теорії графів потребують адаптації до специфіки соціальних мереж, що характеризуються високою динамічністю, неоднорідністю структури та наявністю складних поведінкових патернів учасників.

Огляд літератури. Сучасні дослідження в галузі застосування теорії графів до аналізу соціальних мереж демонструють значний прогрес у розробці нових методологічних підходів та алгоритмічних рішень. Y. Hui, I. M. Zwetsloot, S. Trimborn, S. Rudinac [1, с.3] запропонували інноваційний підхід до динамічного вбудовування графів з використанням domain-informed стратегій негативного семплування, що дозволяє ефективно моделювати еволюційні процеси у соціальних мережах.

Проблематика забезпечення приватності при аналізі соціальних графів розглядається у роботі Z. Wang, W. Wang, Y. Huang, Z. Peng, Z. Yang, M. Yao, C. Wang, X. Fan [2, с.7], які розробили федеративну архітектуру P4GCN для вертикального навчання рекомендаційних систем з використанням двосторонніх графових згорткових мереж, що забезпечує ефективний аналіз без компрометації персональних даних.

Фундаментальні аспекти структурного аналізу мереж досліджуються S. Frenkel, J. Carmesin [3, с. 12], які вивчили вплив локальних сепараторів на формування структури спільнот у великих мережах. Їх дослідження демонструє важливість локальних топологічних характеристик для розуміння глобальної організації соціальних систем.

Бібліометричний аналіз тенденцій досліджень у теорії графів проведений J. A. Dayap, L. F. Casinillo, B. S. Anand, J. S. Estorosos, R. B. Villeta [4, с.15], що надає комплексний огляд розвитку методів домінування в графах та їх застосування до аналізу мережних структур, включаючи соціальні мережі.

Комп'ютерно асистовані методи в теорії графів систематизовані J. Jooken [5, с.8], який представив всебічний огляд сучасних обчислювальних підходів до розв'язання графових задач, що має безпосереднє застосування до аналізу великомасштабних соціальних мереж.

Обчислювальна складність алгоритмів покриття регулярних дерев досліджена J. Bok, J. Fiala, N. Jedličková, J. Kratochvíl [6, с. 11], що надає теоретичні основи для розуміння ефективності алгоритмів обробки деревоподібних структур у соціальних графах.

Топологічні властивості token графів як покриттів розглянуті S. G. Gómez-Galicia, O. B. Zapata- Fonseca [7, с.9], чиє дослідження edge-transitive структур надає нові інструменти для аналізу симетрійних властивостей соціальних мереж.

Проблема ізоморфізму графів Кейлі продуктів графів аналізується M. Mwanza [8, с.6], що має важливе значення для розробки ефективних алгоритмів порівняння структурних характеристик різних соціальних мережних утворень.

Методи augmentation-aware навчання для точної класифікації графів запропоновані M. Kim, J. Choi, S. Lee, J. Jung, U. Kang [9, с.14], які розробили систему AugWard для покращення точності аналізу графових структур через контрольоване збільшення даних.

K. Bougiatiotis, G. Paliouras [10, с.10] представили інноваційний підхід до швидкого багаторелаційного аналізу графів, що використовує математичні властивості простих чисел для оптимізації обчислень на великих мережних структурах.

Мета роботи. Метою дослідження є систематизація та аналіз сучасних методів теорії графів для комплексного вивчення структурних та динамічних характеристик соціальних мереж, розробка інтегрованого підходу до застосування класичних та інноваційних алгоритмів графового аналізу з урахуванням специфічних вимог обробки великомасштабних соціальних мережних структур, включаючи забезпечення масштабованості обчислень, збереження приватності даних та ефективність виявлення структурних закономірностей у динамічних соціальних системах.

Виклад основного матеріалу. Теоретичні основи застосування графів до моделювання соціальних мереж базуються на формалізації соціальних взаємодій через математичні структури. Розглянемо формулу класичного визначення міжпосередницької центральності (betweenness centrality) вершини у графі. Соціальна мережа представляється як граф $G = (V, E)$, де $V = v^1, v^2, \dots, v_{\text{n}}$ - множина вершин, що

відображають учасників мережі, а $E \subseteq V \times V$ - множина ребер, що моделюють зв'язки між ними.

$$C(v) = \sum_{s,t \in V, s \neq v \neq t} \frac{\sigma(s,t|v)}{\sigma(s,t)}$$

де $C(v)$ - показник центральності посередництва для вершини $v, \sigma(s,t)$ - кількість найкоротших шляхів між вершинами s і $t, \sigma(s,t|v)$ - кількість таких шляхів, що проходять через вершину v.

Динамічні аспекти соціальних мереж потребують спеціалізованих підходів до аналізу. Y. Hui, I. M. Zwetsloot, S. Trimborn, S. Rudinac [1, с. 4] розробили методологію domain-informed негативного семплування для динамічного вбудовування графів, що дозволяє ефективно відстежувати еволюцію мережних структур у часі. Їх підхід демонструє значне покращення точності прогнозування зв'язків порівняно з традиційними методами.

Для аналізу параметрів ефективності алгоритмів центральності у соціальних мережах розглянемо розподіл обчислювальної складності основних метрик на табл. 1 (розроблено на основі [1, 2, 4]).

Таблиця 1.

Розподіл параметрів обчислювальної складності алгоритмів центральності

Тип центральності	Обчислювальна складність	Застосування	Масштабованість
Центральність ступеня	$O(V)$	Базовий аналіз	Висока
Центральність близькості	$O(V^2)$	Аналіз доступності	Середня
Центральність посередництва	$O(V^3)$	Аналіз впливу	Низька
PageRank центральність	$O(V+E)$	Ранжування	Висока

У контексті аналізу соціальних мереж теорія графів може слугувати потужним засобом розрахунку впливовості вершин у графі, де вершини представляють користувачів, а ребра – взаємодії між ними. У таблиці 1 підсумовано чотири типи центральності (ступінь, близькість, проміжність та PageRank) щодо обчислювальної складності, застосування та масштабованості. Ці метрики допомагають, коли необхідно визначити ключових учасників мережі – наприклад, впливових користувачів соціальних мереж таких як Instagram чи Twitter (які використовуються для цільової реклами, прогнозування тенденцій або виявлення лідерів думок). Вибір метрики є дуже гнучким та залежить від розміру мережі, а також цілей аналізу, що показує, що теорія графів є гнучким математичним каркасом.

Центральність ступеня (Degree Centrality) дорівнює $O(V)$, де V – кількість вершин, Центральність за ступенем обчислює кількість прямих зв'язків між вершинами. Це робить його ідеальним для базового аналізу великих мереж, таких як соціальні платформи з мільйонами підключених користувачів. Висока масштабованість дозволяє швидко ідентифікувати популярних учасників (наприклад, тих у кого багато підписників). Однак цей підхід не враховує глибші структурні особливості мережі, тому його застосування обмежене для складнішого аналізу.

Центральність близькості (Closeness Centrality) це середня відстань від вершини до всіх інших вершин, та має обчислювальну складність $O(V^2)$. Вона дуже добре працює для аналізу доступності, наприклад, для розрахунку швидкості поширення інформації користувачем мережею. Середня масштабованість робить її придатною для мереж середнього розміру, але на великих графах обчислення є ресурсомістким. Ця методологія застосовується до соціальних мереж для оцінки ефективності комунікації.

Центральність посередництва (Betweenness Centrality) та PageRank мають різні підходи. Центральність посередництва має складність $O(V^3)$, вона вимірює частоту, з якою вершина з'являється на найкоротших шляхах між іншими вершинами, що є ідеальним показником для аналізу впливу, але її низька масштабованість робить її непридатною для великих мереж. PageRank — це масштабований алгоритм ранжування за важливістю вершин, $O(V + E)$, де E кількість ребер, який має дуже схожий алгоритм з Google. У таблиці 1 показано, як теорія графів адаптується, щоб відповідати вимогам аналізу, балансуючи між швидкістю та глибиною).

Як демонструє таблиця 1, різні типи центральності мають суттєво відмінну обчислювальну складність, що критично впливає на їх застосовність до аналізу великомасштабних соціальних мереж.

Проблематика збереження приватності при аналізі соціальних графів знайшла вирішення у федеративних підходах. Z. Wang, W. Wang, Y. Huang, Z. Peng, Z. Yang, M. Yao, C. Wang, X. Fan [2, с. 8] запропонували архітектуру P4GCN, що реалізує вертикальне федеративне навчання для рекомендаційних систем з використанням двосторонніх графових згорткових мереж, забезпечуючи ефективний аналіз без розкриття персональних даних учасників.

Структурний аналіз великих мереж базується на розумінні ролі локальних сепараторів у формуванні глобальної топології. S. Frenkel, J. Carmesin [3, с. 13] продемонстрували, що локальні структурні характеристики суттєво впливають на формування спільнот у великих мережах, що має важливе значення для розробки ефективних алгоритмів кластеризації соціальних графів.

Для систематизації методів виявлення спільнот у соціальних мережах представимо архітектурну модель компонентів системи аналізу на рисунку 1.

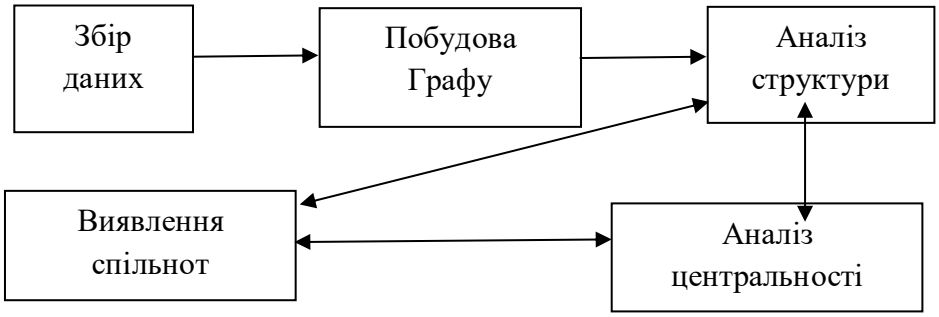


Рис. 1. Структурна модель компонентів системи аналізу соціальних мереж

Представлена на рисунку 1 структурна модель демонструє взаємозв'язок між основними компонентами системи аналізу соціальних мереж, підкреслюючи важливість інтегрованого підходу до обробки мережних структур.

Сучасні тенденції розвитку методів графового аналізу систематизовані у бібліометричному дослідженні J. A. Dayap, L. F. Casinillo, B. S. Anand, J. S. Estorosos, R. B. Villeta [4, с. 16], які проаналізували еволюцію підходів до розв’язання задач домінування в графах та їх застосування до соціальних мережних структур.

Комп'ютерно асистовані методи розв'язання графових задач, представлені J. Jooken [5, с. 9], надають широкий спектр інструментів для ефективного аналізу соціальних мереж, включаючи спеціалізовані алгоритми для обробки динамічних та багаторівневих структур. Теоретичні аспекти обчислювальної складності алгоритмів обробки графів досліджені J. Bok, J. Fiala, N. Jedličková, J. Kratochvíl [6, с. 12], що надає фундаментальні основи для оцінки ефективності методів аналізу деревоподібних підструктур у соціальних мережах. Теорія графів широко використовується для виявлення спільнот у соціальних мережах, користувачів яких можна представити як вершини, а взаємодії – як ребра. У табл. 2 показано розподіл параметрів чотирьох широко використовуваних методів за їх принципом роботи, складністю, точністю та масштабованістю [5, 6, 7]. Ці

методи використовуються для ідентифікації груп, чиї внутрішні зв'язки є щільними, це цікаво для аналізу мереж друзів у таких сервісах, як Facebook або Twitter. Наприклад, у мережах з мільйонами користувачів інформація про спільноту може бути використана для розуміння закономірностей поширення інформації або впливових осіб, а також для формування систем рекомендацій або маркетингових стратегій.

Модулярна оптимізація (Modularity optimization) базується на максимізації модульної функції, яка кількісно визначає щільність зв'язків у спільнотах порівняно з випадково очікуваною щільністю зв'язків. Її складність становить O(V log V), де V – кількість вершин, тому що робить його ефективним для середніх мереж). Точність висока, оскільки алгоритм фокусується на глобальній структурі, але масштабованість середня через ітеративний процес. Аналогічно, метод Louvain є ієрархічним методом кластеризації з поділом вершин на спільноти на кількох рівнях. Він має високу точність та складність O(V log V), що є більш масштабованим, ніж попередній метод, й підходить для динамічних соціальних мереж, де спільноти еволюціонують.

Таблиця 2.

Розподіл параметрів методів виявлення спільнот

Метод	Принцип роботи	Складність	Точність	Масштабованість
Modularity optimization	Максимізація модулярності	O(V log V)	Висока	Середня
Louvain	Ієрархічна кластеризація	O(V log V)	Висока	Висока
Label propagation	Поширення міток	O(V + E)	Середня	Дуже висока
Spectral clustering	Спектральний аналіз	O(V^3)	Дуже висока	Низька

Метод поширення міток (Label propagation) працює шляхом ітеративного присвоєння міток сусіднім вершинам, подібно до дифузії інформації. Швидше для великих графів, оскільки складність становить O(V + E), де E – кількість ребер. Точність середня, оскільки алгоритм чутливий до початкових умов, але масштабованість дуже висока, що корисно для аналізу соціальних мереж у реальному часі з мільярдами взаємодій. На відміну від цього, спектральний кластеринг (Spectral clustering) застосовує спектральний аналіз матриці суміжності, розбиваючи граф на власні вектори. Завдяки високій складності O(V^3), він пропонує дуже високу точність для складних структур, але низьку масштабованість, що обмежує її застосування до невеликих мереж.

У випадку соціальних мереж, метод, який слід використовувати, залежить від розміру даних та вимог. Для великих мереж, таких як Instagram, перевага надається деяким швидким методам кластеризації, таким як Louvain або Label propagation, тоді як Spectral clustering підходить для точнішого аналізу малих груп. У таблиці 2 показано компроміс між точністю та ефективністю, а також те, як теорія графів адаптується до реальних викликів й призводить до кращого розуміння соціальних явищ. Таблиця 2 демонструє компромісність вибору між точністю та масштабованістю різних методів виявлення спільнот, що є критичним фактором при проєктуванні систем аналізу великих соціальних мереж.

Топологічні властивості графових структур, зокрема edge-transitive token графів, досліджені S. G. Gómez-Galicia, O. B. Zapata-Fonseca [7, с. 10], що надає математичні інструменти для аналізу симетрійних характеристик соціальних мережних утворень. Проблематика ізоморфізму графових структур, розглянута M. Mwanza [8, с. 7], має пряме застосування до порівняльного аналізу різних соціальних мереж та виявлення структурних аналогій між ними. Інноваційні підходи до навчання на графових структурах представлені M. Kim, J. Choi, S. Lee, J. Jung, U. Kang [9, с. 15], які розробили систему AugWard для augmentation-aware навчання, що значно покращує точність класифікації графових структур через контрольоване збільшення навчальних даних.

Такий приклад можна спостерігати на рис. 2, а саме структурну модель елементів динамічного аналізу соціальних графів.

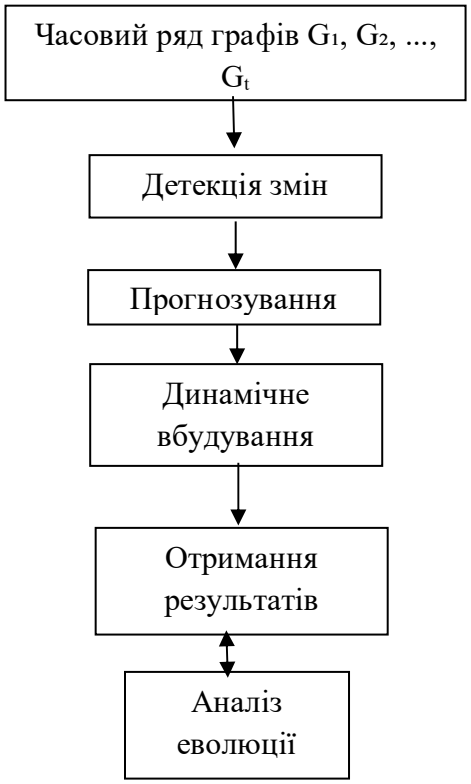


Рис. 2. Структурна модель компонентів динамічного аналізу соціальних графів

Рис. 2 ілюструє комплексний підхід до динамічного аналізу соціальних графів, що включає темпоральні аспекти та методи прогнозування еволюційних процесів у мережних структурах. Багаторелаційний аналіз графів, запропонований K. Bougiatiotis, G. Paliouras [10, с. 11], використовує математичні властивості простих чисел для оптимізації обчислень на складних мережних структурах, що відкриває нові можливості для ефективного аналізу гетерогенних соціальних мереж. Динамічний аналіз соціальних мереж моделюється за допомогою теорії графів, використовуючи вершини як користувачів, ребра – зв’язки, а T – тимчасові зрізи. У табл. 3 наведено порівняння продуктивності чотирьох алгоритмів на основі їх типу та аналізу, часової складності, споживання пам'яті та точності прогнозування [8, 10]. Ці алгоритми можна використовувати для прогнозування змін у таких мережах, як Twitter або LinkedIn, де зв'язки формуються та розриваються постійно. Наприклад, вони оптимізовані для обчислювальних ресурсів для обробки великих даних та допомагають прогнозувати поширення інформації, виявляти тенденції або рекомендувати друзів.

Таблиця 3.

Розподіл параметрів ефективності алгоритмів динамічного аналізу

Алгоритм	Тип аналізу	Часова складність	Пам'ять	Точність прогнозу
Dynamic Node2Vec	Вбудовування вершин	O(|E|d log |V|)	O(|V|d)	85-90%
DynGEM	Автокодери	O(|V|²)	O(|V|d)	80-85%
EvolveGCN	GCN еволюція	O(T|E|d)	O(T|V|d)	90-95%
DySAT	Self-attention	O(T|V|²)	O(T|V|d)	88-92%

Алгоритм Dynamic Node2Vec базується на вбудовуванні вершин за допомогою динамічно адаптованих випадкових блукань. Часова складність становить O(|E|d log |V|), де |E| – кількість ребер, d – розмірність вбудовування, а |V| – кількість вершин, тому він

ефективний для мереж з великою кількістю ребер. Обсяг пам'яті становить O(|V|d), а продуктивність прогнозування становить 85-90%, чого достатньо для таких завдань, як прогнозування нових посилань. Аналогічно, DynGEM стискає граф до латентного простору за допомогою автокодерів. З квадратичною складністю O(|V|²) він менш масштабований для дуже великих мереж, але з пам'яттю O(|V|d) та точністю 80-85% його можна використовувати для глибокого навчання структурних змін.

EvolveGCN — це розширення графових згорткових мереж що застосовує еволюцію графових згорткових мереж (GCN) до графа, що змінюється в часі. Складність становить O(T|E|d), тому він адаптивний до довгих послідовностей та враховує T – кількість часових кроків. Хоча обсяг пам'яті збільшується до O(T|V|d) через часову інформацію, точність 90-95% достатня для динамічних мереж, таких як соціальні платформи реального часу, де точність прогнозування є критично важливою. (DySAT базований на self-attention фокусується на основі тимчасових залежностей й моделює часові залежності вершин. Хоча його обчислювальна складність становить O(T|V|²), що є обчислювальне ресурсомістким, його складність пам'яті становить O(T|V|d), а точність — 88-92%, що робить його досить ефективним інструментом моделювання уваги в мережах.

У соціальних мережах вибір алгоритму змінюватиметься залежно від розміру та динаміки даних. Dynamic Node2Vec для швидкого аналізу, EvolveGCN для високої точності. У таблиці 3 показано компроміси між швидкістю та точністю, а також те, як змінюється теорія графів для застосувань у реальному житті; це сприяє кращому розумінню соціальної еволюції. Таким чином таблиця 3 показує, що сучасні алгоритми динамічного аналізу соціальних графів демонструють високу точність прогнозування при збереженні прийнятної обчислювальної складності для практичних застосувань. У контексті аналізу соціальних мереж теорія графів тісно пов'язана з лінійною алгеброю та аналітичною геометрією й пропонує потужні інструменти для моделювання складної взаємодії користувачів. Матриця суміжності — це базовий об'єкт, який описує структуру графа, де вершини представляють користувачів, а ребра — їхні зв'язки. Наприклад дружбу або взаємодію в соціальній мережі, такій як Twitter або LinkedIn. Застосування методів лінійної алгебри, зокрема аналізу власних значень та векторний аналіз, можуть бути використані для виявлення ключових властивостей мережі, таких як спільноти або впливові вузли. Наприклад, спектральний аналіз матриці суміжності використовується для виконання кластеризації, що дуже важливо для прогнозування трендів або цільової реклами. Матриця суміжності графа соціальної мережі має вигляд

$$\begin{matrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix}$$

Матриця суміжності, як елемент лінійної алгебри, відображає бінарні зв’язки між чотирма вершинами, де 1 вказує на наявність ребра, а 0 — на його відсутність. Її симетрична структура підкреслює неорієнтований характер графа, що є типовим для соціальних мереж, де зв’язки, як правило, взаємні. У контексті аналітичної геометрії цю матрицю можна використовувати для генерації спектральної побудови графа, в яких власні вектори описують геометричну конфігурацію вершин у багатовимірному просторі. Це дозволяє ефективно використовувати методи кластеризації, наприклад, для сегментації аудиторій у маркетингових дослідженнях. Аналіз матриці суміжності за допомогою лінійної алгебри відкриває можливості для обчислення центральності, такої як власний вектор центральності, що вказує на впливовість вершин. У соціальних мережах це можна використовувати для пошуку лідерів думок, які відповідають за поширення інформації. Водночас, структуру мережі можна візуалізувати на основі методів аналітичної геометрії, таких як проекція вершин на основі власних векторів, що спрощує інтерпретацію складних зв'язків. Такі методи стають ще кориснішими для великих мереж, які неможливо проаналізувати вручну.

Використання матриць у соціальних мережах також є актуальним з практичної точки зору для динамічного аналізу, наприклад, для моделювання еволюції зв'язків у часі. Синергія між лінійною алгеброю та аналітичною геометрією була використана, через матрицю суміжності, у поєднанні з такими алгоритмами, як спектральна кластеризація або PageRank, для розуміння глибоких структур соціальної організації. Таким чином, окрім того, що наведена матриця є математичним інструментом, вона слугує сполучною ланкою між теоретичними основами та практичними проблемами аналізу соціальних мереж, що має велике значення в розробці ефективних стратегій у цифровому середовищі.

Висновки. Проведене дослідження демонструє, що застосування теорії графів до аналізу соціальних мереж представляє собою потужний методологічний підхід, який дозволяє ефективно моделювати, аналізувати та прогнозувати поведінку складних мережних структур. Математичний апарат теорії графів надає формальні інструменти для кількісного опису топологічних властивостей соціальних мереж та виявлення прихованих закономірностей у їх структурі. Аналіз сучасних методів показав значний прогрес у розробці алгоритмів динамічного аналізу соціальних графів. Інноваційні підходи до вбудовування графів з урахуванням темпоральних аспектів дозволяють відстежувати еволюційні процеси у мережах з високою точністю. Федеративні методи навчання забезпечують можливість аналізу великомасштабних структур при збереженні приватності персональних даних, що є критично важливим для практичних застосувань. Встановлено, що ефективність алгоритмів аналізу соціальних мереж суттєво залежить від вибору відповідних метрик центральності та методів виявлення спільнот. Класичні підходи, такі як центральність ступеня та посередництва, залишаються релевантними для базового аналізу, проте складні структурні характеристики потребують застосування сучасних методів спектрального аналізу та машинного навчання на графах. Дослідження виявило важливість локальних топологічних характеристик для розуміння глобальної організації соціальних мереж. Локальні сепаратори та структурні мотиви відіграють ключову роль у формуванні спільнот та визначенні інформаційних потоків у мережі. Це знання має практичне значення для оптимізації алгоритмів кластеризації та прогнозування поширення інформації. Комп'ютерно-асистовані методи графового аналізу відкривають нові можливості для обробки великомасштабних соціальних мереж. Розвиток спеціалізованих алгоритмічних підходів, включаючи багаторелаційний аналіз та методи на основі теорії чисел, демонструє перспективність міждисциплінарного підходу до розв'язання графових задач. Виявлено значний потенціал інтеграції класичних методів теорії графів з сучасними підходами машинного навчання. Augmentation-aware методи навчання та динамічні графові нейронні мережі показують високу ефективність у задачах класифікації та прогнозування, що робить їх перспективними для створення інтелектуальних систем аналізу соціальних мереж. Результати аналізу обчислювальної складності різних алгоритмів підкреслюють необхідність збалансованого підходу до вибору методів аналізу залежно від розміру мережі та специфічних вимог завдання. Використання теорії графів, разом з інструментами лінійної алгебри та аналітичної геометрії, для аналізу структури та динаміки соціальних мереж. Ці інструменти використовуються для розробки як прогностичних моделей, так й стратегій оптимізації в галузі цифрових соціальних платформ. Перспективи подальших досліджень включають розробку гібридних методів, що поєднують переваги різних підходів до аналізу графів, створення адаптивних алгоритмів для обробки гетерогенних мережних структур та розвиток теоретичних основ для аналізу багатошарових соціальних мереж з урахуванням їх динамічної природи.

Список літератури

1. Hui Y., Zwetsloot I. M., Trimborn S., Rudinac S. Domain-Informed Negative Sampling Strategies for Dynamic Graph Embedding in Meme Stock-Related Social Networks. 2024.

DOI: https://doi.org/10.48550/ARXIV.2411.00606. URL: https://arxiv.org/abs/2411.00606

2. Wang Z., Wang W., Huang Y., Peng Z., Yang Z., Yao M., Wang C., Fan X. P4GCN: Vertical Federated Social Recommendation with Privacy-Preserving Two-Party Graph Convolution Network (Version 3). 2024. DOI: https://doi.org/10.48550/ARXIV.2410.13905. URL: https://arxiv.org/abs/2410.13905
3. Frenkel S., Carmesin J. How Local Separators Shape Community Structure in Large Networks (Version 1). 2025. DOI: https://doi.org/10.48550/ARXIV.2504.14501. URL: https://arxiv.org/abs/2504.14501v1
4. Dayap J. A., Casinillo L. F., Anand B. S., Estorosos J. S., Villeta R. B. Domination in Graph Theory: A Bibliometric Analysis of Research Trends, Collaboration and Citation Networks. 2025. DOI: https://doi.org/10.48550/ARXIV.2503.08690. URL: https://arxiv.org/abs/2503.08690v1
5. Jooken J. Computer-assisted graph theory: a survey (Version 1). 2025. DOI: https://doi.org/10.48550/ARXIV.2508.20825 URL: https://arxiv.org/abs/2508.20825v1
6. Bok J., Fiala J., Jedličková N., Kratochvíl J. Computational complexity of covering regular trees (Version 1). 2025. DOI: https://doi.org/10.48550/ARXIV.2507.00564. URL: https://arxiv.org/abs/2507.00564v1
7. Gómez-Galicia S. G., Zapata-Fonseca O. B. Edge-transitive token graphs as covers. 2025. DOI: https://doi.org/10.48550/ARXIV.2505.20632 URL: https://arxiv.org/abs/2505.20632v1
8. Mwanza M. On the Isomorphism Problem of Cayley Graphs of Graph Products (Version 1). 2025. DOI: https://doi.org/10.48550/ARXIV.2503.15165. URL: https://arxiv.org/abs/2503.15165v1
9. Kim M., Choi J., Lee S., Jung J., Kang U. AugWard: Augmentation-Aware Representation Learning for Accurate Graph Classification. 2025. DOI: https://doi.org/10.48550/ARXIV.2503.21105. URL: https://arxiv.org/abs/2503.21105v1
10. Bougiatiotis K., Paliouras G. From Primes to Paths: Enabling Fast Multi-Relational Graph Analysis (Version 1). 2024. DOI: https://doi.org/10.48550/ARXIV.2411.11149. URL: https://arxiv.org/abs/2411.11149

Н. М. Баландіна

APPLICATION OF GRAPH THEORY IN SOCIAL NETWORK ANALYSIS

N. M. Balandina

National University “Odesa Law Academy”
28, Rishelievska, Odesa, Ukraine
Email: nataliabalandina2103@gmail.com

The purpose of the article is to study the analysis and application of the mathematical apparatus of graph theory to study structural characteristics and dynamic processes in social networks. The main approaches to modeling social interactions through graph structures are considered, including methods of vertex centrality analysis, community detection and relationship prediction. Modern algorithms for processing large-scale network structures and their application to solving applied problems of social platform analysis are analyzed and the systematization of graph theory methods for analyzing topological properties of social networks and the development of a comprehensive approach to modeling dynamic processes in network structures considering modern computing capabilities. An integrated approach to the application of classical and modern graph theory methods for the complex analysis of social networks is proposed, which includes dynamic graph embedding algorithms, federated learning methods, and privacy-preserving technologies when processing network data. A methodological framework for analyzing the structural characteristics of social networks has been developed, which combines classical centrality metrics with modern approaches to community detection and analysis of dynamic processes. Key parameters of the efficiency of algorithms for processing large-scale graphs and their adaptation to the specifics of social network structures have been determined. The application of graph theory in social network analysis demonstrates high efficiency for understanding structural regularities and predicting behavioral patterns. The integration of modern machine learning methods with classical graph theory approaches opens new opportunities for creating accurate models of social interactions and developing intelligent systems for analyzing network structures.
Keywords: graph, centrality, communities, embeddings, algorithms, discrete mathematics.

DOI 10.15276/imms.v15.no3.347
УДК 539.384

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 347-353

РІШЕННЯ ЗАДАЧІ ПРО ВИГИН ЗАТИСНЕНОЇ ПО КОНТУРУ ПЛАСТИНИ З ТОНКИМ ЛІНІЙНИМ ВКЛЮЧЕННЯМ МЕТОДОМ МІНІМІЗАЦІЇ ПОХИБКИ ПО ЕНЕРГІЇ

В.В. Грібова, Л.В. Бовнегра, А.В. Торопенко

Національний університет «Одеська політехніка»
1, Шевченка пр., м. Одеса, 65044, Україна
Emails: gribova@op.edu.ua, dlv5@ukr.net, toropenko.a.v@op.edu.ua

Складчасті оболонки, тонкостінні стержні та інші конструкції, що отримуються на базі з'єднань тонких пластин, мають широке використання в машинобудуванні, в авіаційній та кораблебудівній промисловостях. Наявність в конструкціях підкріплюючих стержнів, опор, прямолінійних дефектів типу тріщин і включень або інших неоднорідностей значно ускладнює їхній розрахунок. Проєктування і створення надійних в експлуатації і достатньо економічних конструкцій приводить до необхідності розглядати все більш складні краєві задачі і, відповідно розв'язувати все більше число диференціальних рівнянь, що їх описують. Фундаментом науки про міцність є механіка руйнувань, яка базується на вияві характеру особливостей напружень в околі кінців дефектів типу тріщин і тонких включень. Основою методики розв'язання задачі є побудова моделі, що базується на методі мінімізації похибки за енергією. Основними результатами є побудова системи рішень бігармонійного рівняння в області з прямолінійним включенням, застосування методу граничної колокації для знаходження коефіцієнтів лінійної комбінації.

Метою роботи є розв'язання складних краєвих задач механіки руйнування для тонкостінних конструкцій із включеннями, шляхом побудови математичної моделі на основі методу мінімізації енергетичної похибки та застосування граничної колокації.

Ключові слова. Система бігармонійних функцій, метод граничної колокації, клас функцій з особливостями, що не інтегруються, вигини пластини, метод мінімізації похибки за енергією.

Вступ. Розглядається задача про вигин пластини з тонким лінійним включенням. Відомо, що наявність в конструкціях підкріплюючих стержнів, опор, прямолінійних дефектів типу тріщини і включень значно ускладнює їх розрахунок, так як перераховані елементи в конструкціях є концентраторами напружень. Дослідження в цьому напрямку були розпочаті В.М. Толкачовим, розвинуті О.В. Онищуком, Г.Я. Поповим і продовжені в роботах С.Т. Грибняка, Ю.С. Процерова, В.В. Реута і інших авторів. Рішення задачі розшукується у вигляді лінійної комбінації повної системи бігармонійних функцій, що враховують наявність включення. Для знаходження невідомих коефіцієнтів, вперше, описано метод мінімізації похибки по енергії. Для контроля результатів невідомі коефіцієнти знаходилися також методом граничної колокації. Метою роботи є розв'язання складних краєвих задач механіки руйнування для тонкостінних конструкцій із включеннями, шляхом побудови математичної моделі на основі методу мінімізації енергетичної похибки та застосування граничної колокації.

Основна частина. Розглянемо прямокутну пластину ($|x|<a,\ |y|<b$), всередині якої на відрізку $y=0, |y|\le c$ присутнє тонке жорстке включення. Враховуючи, що поза включенням на пластину не діє розподілене навантаження, приходимо до однорідного бігармонійного рівняння відносно прогинів пластини:

$$\Delta^2\omega(x,y)=0, \quad |x|<a,\ |y|<b \text{ окрім } y=0, |x|<c, \tag{1}$$

де $\omega(x,y)$ – прогини пластини.

Включення переміщується вертикально під дією прикладеного до нього навантаження *R*. В математичній постановці включення можна розглядати як розріз з межами $y=\pm 0,\ |x|\le c$. На межі розрізу виконуються умови:

$$\omega(x,\pm 0)=W_0 \quad |x|\le c, \tag{2}$$

$$\omega_y'(x,\pm 0)=0 \quad |x|\le c, \tag{3}$$

На сторонах пластини задані умови затиснення:

$$\omega(\pm a,y)=\omega_x'(\pm a,y)=0, \quad |y|\le b, \tag{4}$$

$$\omega(x,\pm b)=\omega_y'(x,\pm b)=0, \quad |x|\le a. \tag{5}$$

Потрібно знайти розподіл прогинів, згинальних моментів, узагальнених перериваючих сил.

З урахуванням парності задачі по x і y наближене представлення прогину $\omega_N(x,y)$ можна записати у вигляді [1]

$$\omega(x,y)=\sum_{n=0}^{N} a_n u_n(x,y); \tag{6}$$

де $u_0(x,y)=\mathrm{Re}\left(\ln\left(z+\left(z^2-1\right)^{\frac{1}{2}}\right)-z\left(z^2-1\right)^{\frac{1}{2}}\right);$

$u_1(x,y)=\mathrm{Re}\left(\left(z\bar{z}-1\right)\ln\left(z+\left(z^2-1\right)^{\frac{1}{2}}\right)\right);$

$u_{4n-2}(x,y)=\mathrm{Re}\left(z^{2n-1}\left(z^2-1\right)^{\frac{3}{2}}\right),\ n=\overline{1,N};$

$u_{4n-1}(x,y)=\mathrm{Re}\left(2iyz^{2n-2}\left(z^2-1\right)^{\frac{1}{2}}\right),\ n=\overline{1,N};$

$u_{4n}(x,y)=\mathrm{Re}\,z^{2n-2},\ n=\overline{1,N};$

$u_{4n+1}(x,y)=\mathrm{Re}\,\bar{z}z^{2n-1},\ n=\overline{1,N}.$

Невідомі коефіцієнти $a_n(n=\overline{0,N})$ шукаються, вперше, методом мінімізації похибки за енергією. Даний метод є близьким в ідейному відношенні до методу, запропонованому Бірманом, Поповим Г.Я., Онищуком О.В. Ідею методу викладемо на прикладі наступної краєвої задачі для рівняння вигину пластин:

$$\Delta^2\omega(x,y)=q(x,y), \quad \left((x,y)\in\Omega\right) \tag{7}$$

У випадку затискання пластини по краям

$$\omega|_\Gamma=f_0(S),\frac{\partial\omega}{\partial n}|_\Gamma=f_1(S) \quad \left((x,y)\in\Gamma=d\Omega\right) \tag{8}$$

Нехай $\omega(x,y)$– точне, $\omega_N(x,y)$– наближене рішення задачі (7), (8). Відповідно [1], $\omega_N(x,y)$ можна представити у вигляді

$$\omega_N(x,y)=\sum_{i=1}^{N} c_i u_i(x,y)+\omega_q(x,y), \tag{9}$$

де $u_i(x,y)$, $i=\overline{1,N}$– повна система рішень рівняння (7) в області Ω

$\omega_q(x,y)$ – часткове рішення рівняння (7).

Як відомо [6], потенційна енергія вигину тонкої пластини пропорційна величині

$$W(u)=\int_\Omega\left(\left(\Delta u\right)^2-2(1-\nu)\left(u''_{xx}u''_{yy}-\left(u''_{xy}\right)^2\right)\right)d\Omega\ , \tag{10}$$

де u – вигин пластини, ν – коефіцієнт Пуассона.

Розглянемо білінійну форму $\mathrm{E}(u,\nu)$, пов'язану з потенційною енергією вигину пластини:

$$\mathrm{E}(u,\mathrm{v})=\int_{\Omega}\left[\Delta u\Delta\mathrm{v}+(1-\nu)\left(2\frac{\partial^2 u}{\partial x\partial y}\frac{\partial^2\mathrm{v}}{\partial x\partial y}-\frac{\partial^2 u}{\partial x^2}\frac{\partial^2\mathrm{v}}{\partial y^2}-\frac{\partial^2 u}{\partial y^2}\frac{\partial^2\mathrm{v}}{\partial x^2}\right)\right]d\Omega \tag{11}$$

Очевидно

$$\mathrm{E}_{\Omega}(u,u)=W(u) \tag{12}$$

В основі методу лежить тотожність [5]:

$$\mathrm{E}_{\Omega}(u,\mathrm{v})=E_{\Gamma}(u,\mathrm{v}),\ E_{\Gamma}(u,\mathrm{v})=\oint_{\Gamma}\left(\frac{\partial u}{\partial n}M\mathrm{v}-uV\mathrm{v}\right)dS+\int\int_{\Omega}u\Delta^2\mathrm{v}d\Omega\ , \tag{13}$$

що дозволяє вирахувати $E_{\Omega}(u,\mathrm{v})$ для невідомого всередині Ω точного рішення $u(x,y)$ і відомої бігармонічної функції $\mathrm{v}(x,y)$ $\left(\Delta^2\mathrm{v}=0\right)$.

Покажемо, що у випадку граничних умов (8), невідомі коефіцієнти $a_n\left(n=\overline{1,N}\right)$ можуть бути знайдені з умов мінімуму функціоналу енергії погрішності

$$F(a_1,....,a_N)=E(\omega-\omega_N,\omega-\omega_N), \tag{14}$$

де ω – невідоме точне, ω_N – наближене рішення задачі (7), (8).

Дійсно, мінімізуючи F і записуючи умову існування екстремуму

$$\frac{\partial F}{\partial a_n}=0\quad\left(n=\overline{1,N}\right), \tag{15}$$

приходимо до системи лінійних алгебраїчних рівнянь відносно невідомих a_n

$$\sum_{n=1}^{N}a_nE(u_n,u_m)=b_m\ \left(m=\overline{1,N}\right) \tag{16}$$

$$b_m=E(\omega-\omega_q,u_m)$$

Праві частини b_m в (16) залежать від невідомої функції ω, однак з допомогою відомої тотожності (13), отримуємо вираз для b_m з допомогою відомих значень ω і $\frac{\partial\omega}{\partial n}$ на межі області Ω:

$$b_m=\oint_{\Gamma}\left[\left(f_1(s)-\frac{\partial\omega_q}{\partial n}\right)Mu_m-\left(f_0(s)-\omega_q\right)Vu_m\right]dS \tag{17}$$

Відмітимо, що формула (17) справедлива, якщо межа Γ області Ω є гладкою. У випадку, якщо межа Γ є кусково-гладкою, то вираз (17) варто уточнити.

Нехай межа Γ складається з n гладких кусків і точок злому межі $(x_i,y_i)\ \left(i=\overline{1,n}\right)$. У виразі (17), варто врахувати скачки відповідних величин в даних точках, після чого (17) прийме вигляд:

$$b_j=\sum_{i=1}^{N}\left(\oint_{\Gamma}\left(\left(f_1(s)-\frac{\partial\omega_q}{\partial n}\right)Mu_j-\left(f_0(s)-\omega_q\right)Vu_j\right)dS\right)+\left(f_1(x,y)-\frac{\partial\omega_q(x,y)}{\partial n}\right)<Mu_j>$$

$$-\left(\left(f_0(x,y)-\omega_q(x,\mathrm{y})\right)<Vu_j>\Big|_{\substack{x=x_i\\y=y_i}}\right),\ \left(j=\overline{1,n}\right), \tag{18}$$

де $<u>=u\left(x(s_i-0),y(s_i-0)\right)-u\left(x(s_i+0),y(s_i+0)\right)$,

$$<\frac{\partial u}{\partial n}>=\frac{\partial u}{\partial n}\left(x\left(s_i-0\right),y\left(s_i-0\right)\right)-\frac{\partial u}{\partial n}\left(x\left(s_i+0\right),y\left(s_i+0\right)\right),$$
$$<Mu>=Mu\left(x\left(s_i-0\right),y\left(s_i-0\right)\right)-Mu\left(x\left(s_i+0\right),y\left(s_i+0\right)\right),$$
$$<Vu>=Vu\left(x\left(s_i-0\right),y\left(s_i-0\right)\right)-Vu\left(x\left(s_i+0\right),y\left(s_i+0\right)\right),\qquad \left(i=\overline{1,N}\,j=\overline{1,n}\right)$$
$$Mu=-D\left(\frac{\partial^2}{\partial n^2}+\nu\frac{\partial^2}{\partial s^2}\right)u,\ Vu=-D\left(\frac{\partial}{\partial n}\left(\Delta+\left(1-\nu\right)\frac{\partial^2}{\partial s^2}\right)\right)u$$

D – циліндрична жорсткість, ν – коефіцієнт Пуассона, s – дотична до межі $\Gamma=\partial\Omega$.
Реалізація методу мінімізації похибки по енергії, застосована до задачі (1) – (5), з урахуванням подання прогинів пластини у вигляді (6) і формул (16), (18), призводить до наступної системи лінійних алгебраїчних рівнянь, відносно невідомих коефіцієнтів $a_i,\left(i=\overline{0,N}\right)$

$$\sum_{i=0}^{N}a_iE\left(u_i,u_j\right)=b_j\qquad\left(j=\overline{0,N}\right)\tag{19}$$
$$b_j=E\left(\omega,u_j\right).$$

де $E\left(u,\mathrm{v}\right)=\oint\limits_{\Gamma}\left(\frac{\partial u}{\partial n}M_n\mathrm{v}-uV_n\mathrm{v}\right)ds-W_0<V_n\mathrm{v}>\big|_{x=a,y=b}$,
$\Gamma=\left\{\left(x=a,0<y<b\right)\cup\left(y=b,0<x<a\right)\right\}$,
$b_j=W_0\int\limits_0^c V_yu_j\left(x,\pm0\right)dx,$
$M_n=-D\left(\frac{\partial^2}{\partial n^2}+\nu\frac{\partial^2}{\partial s^2}\right),$
$V_n=-D\frac{\partial}{\partial n}\left(\Delta+\left(1-\nu\right)\frac{\partial^2}{\partial s^2}\right),$

n – нормаль, s – дотична до межі Γ, D – циліндрична жорсткість, ν – коефіцієнт Пуассона, в подальшому для спрощення беремо c = 1.

Для перевірки правильності результатів, задача (1) – (5) була вирішена, також, методом граничної колокації.

При вирішення задачі (1) – (5) методом граничної колокації, використовувалось подання прогину у вигляді (6). Для знаходження невідомих коефіцієнтів a_i на Γ межі Ω $\Gamma=\left\{\left(y=\pm0,0<x<1\right)\cup\left(x=a,0<y<b\right)\cup\left(y=b,0<x<a\right)\right\}$, займаємою пластиною, вибирались M точок колокації $\left(M=N+1\right)$. Точки вибирались зі скупченням до кінців проміжків, а саме:

$$y=0,x_k=\cos\left(\frac{\pi\left(2k-1\right)}{4n_1}\right),k=\overline{1,n_1},\tag{20}$$
$$x=a,y_k=b\cos\left(\frac{\pi\left(2k-1\right)}{4n_2}\right),k=\overline{1,n_2},$$
$$y=b,x_k=a\cos\left(\frac{\pi\left(2k-1\right)}{4n_3}\right),k=\overline{1,n_3},\quad n_1+n_2+n_{\ 3}=M$$

Реалізація граничних умов (2) – (5) в точках колокації (20), приводить до системи N+1 лінійних алгебраїчних рівнянь відносно N+1 невідомих $a_i\left(i=\overline{0,N}\right)$.

Розрахунки були проведені для квадратних пластин (a=b), при відносній довжині включення $\varepsilon = c/a$, рівній 0,66;0,5;0,2;0,1. Результати, отримані з допомогою обох викладених методів, практично співпали.

На рис. 1 приведено розподілення прогинів для пластини з розмірами $a = b = 2, \varepsilon = 0.5$. Прогини максимальні на включенні, де вони рівні $W_0 = 1,$ і зменшуються до нуля на контурі пластини, що свідчить про добре відповідність умовам (2) – (5) обома методами.

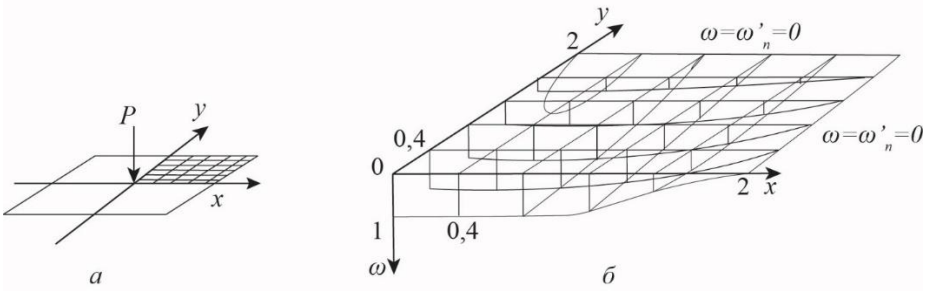


Рис. 1. Розподіл прогинів пластини

Оптимальне, з точки зору відповідності граничним умовам (2) – (5), розміщення точок колокації наведені в таблиці 1, де n_1 – кількість точок колокації при $y = \pm 0$, $0 < x < 1$, n_2 – при $x = a, 0 < y < a$, n_3 – при $y = a, 0 < x < a$.

Таблиця 1.

Кількість точок колокації

ε	n_1	n_2	n_3
0,66	4	3	3
0,5	4	3	3
0,2	4	3	3
0,1	3	3	3

Розраховувалась рівнодіюча контактних зусиль P:

$$D^{-1}P = a_0 \int_0^1 \left(\frac{16}{\sqrt{1-x^2}} + \frac{16}{\left(1-x^2\right)^{\frac{3}{2}}} \right) dx + \sum_{k=0}^{N} 8 a_k P_k \tag{21}$$

$$P_k = \int_0^1 \left(1-x^2\right)^{-\frac{3}{2}} \left[2k\left(2k+1\right)x^{2k+2} - \left(8k^2+1\right)x^{2k} + 2k\left(2k-1\right)x^{2k-2} \right] dx$$

Для розрахунку P_k скористаємося наступними регуляризованими значеннями розбіжних інтегралів:

$$\int_{-1}^{1} \frac{dx}{\left(1-x^2\right)^{\frac{3}{2}}} = 0, \quad \int_{-1}^{1} \frac{x^2}{\left(1-x^2\right)^{\frac{3}{2}}} = -\pi, \quad \int_{-1}^{1} \frac{x^{2k}}{\left(1-x^2\right)^{\frac{3}{2}}} = -\pi \frac{(2k-1)!!}{(2k-2)!!} \left(k \geq 2\right) \tag{22}$$

отримані із [4]:

$$\int_0^1 x^{2k} \left(1-x^2\right)^{\lambda} dx = \frac{1}{2} B\left(k+\frac{1}{2}, \lambda+1\right) \text{ при } \lambda = -\frac{3}{2} \tag{23}$$

У висновку отримуємо

$$P_k = 0, D^{-1}P = 8\pi a_0$$

Механічна інтерпретація першої з рівностей (22) дана в [3, 4].

Значення безрозмірного коефіцієнта $\alpha = 10^3 \left(Pa^2\right)^{-1} DW_0$, при різних значеннях ε, приведено в таблиці 2. Як видно, при зменшенні відповідної довжини включення ε, значення α наближаються до відповідного значення α для зосередженої сили

$\alpha = 5,60$, приведенному у [6].

Таблиця 2.

Значення безрозмірного коефіцієнта $\alpha = 10^3 \left(Pa^2\right)^{-1} DW$

ε	0,66	0,5	0,2	0,1
α	0,76	1,81	4,05	4,90

Графіки згинальних моментів M_x, M_y вздовж лінії $y = +0,\ 0 < x < a$ наведені на рис. 2. При $(x,y) \to (1,0)$ $M_x, M_y \to \infty$ як $r^{\frac{1}{2}}, r = \sqrt{(x-1)^2 + y^2}$. Для опису цього факту в літературі [6] вводиться поняття коефіцієнта інтенсивності напружень:

$$K_x = \lim \frac{M_x}{P} \frac{\sqrt{r}}{\sqrt{c}}, \quad K_y = \lim \frac{M_y}{P} \frac{\sqrt{r}}{\sqrt{c}}, \tag{24}$$

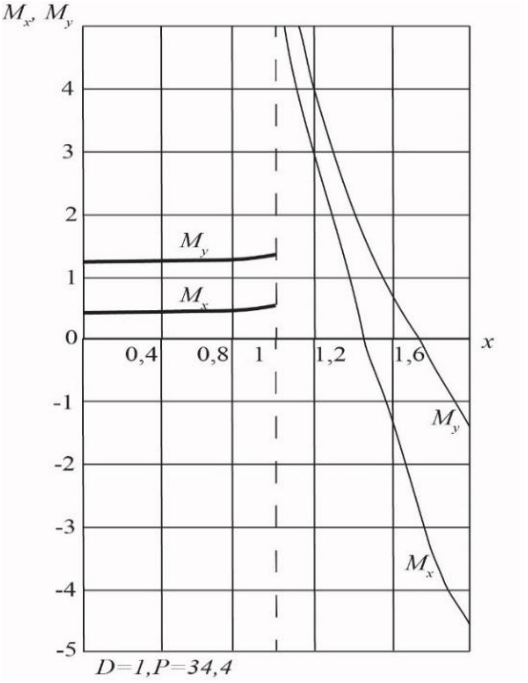
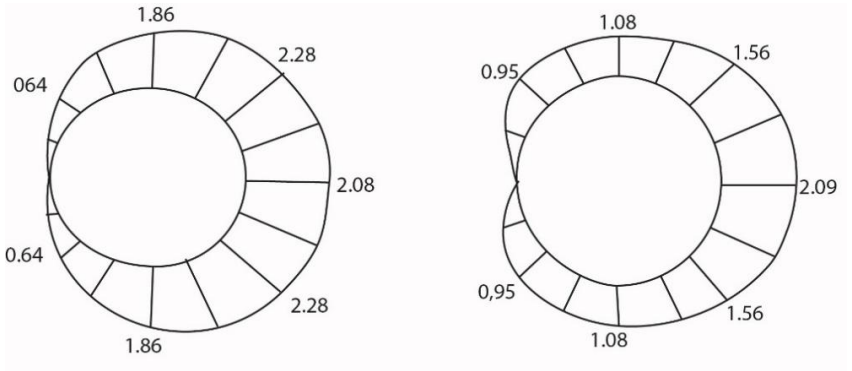


Рис. 2. Графіки згинальних моментів M_x, M_y вздовж лінії $y = \pm 0,\ 0 \le x \le a$

Епюри величин K_x, K_y при $r = 10^{-4}$ наведені на рис.3. Якісна картина аналогічна результатам роботи [6], де розглядались безкінечні пластини.



а *б*

Рис. 3. Епюри $K_x(a)$, $K_y(b)$

Отримані результати показують, що використання методу граничної колокації достатньо ефективне при вирішенні задач вигину нескінчених пластин з включеннями.

Список літератури

1. Кривий О. Ф., Морозов Ю. О. Особливості поля напружень в околі міжфазного кругового включення при змішаних умовах контакту із кусково-однорідним трансверсально-ізотропним простором. *Прикладна механіка*. 2024. Т. 60, № 3. С. 91–100. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001493980
2. A. Usov, Yu. Morozov, M. Kunitsyn, A. Tonkonozhenko, I. Chernush. Investigation of the influence of structural inhomogeneities on the strength of welded joints of functionally gradient materials. *Proceedings of Odessa Polytechnic University*, 2020. Is.1(60), DOI: https://doi.org/10.15276/opu.1.60.2020.03
3. Kryvyi, O.F., Morozov, Y. O. Influence of Concentrated Forces on an Interface Inclusion under the Conditions of Smooth Contact in the Inhomogeneous Transversely Isotropic Space. *J Math Sci*. 2024 V.279. P.197–212. https://doi.org/10.1007/s10958-024-07005-3
4. Kryvyi, O. F., Morozov, Y. O. Stress Field Features in Vicinity of Interfacial Circular Inclusion Under Mixed Contact Conditions with Piecewise Homogeneous Transversely Isotropic Space. *Int Appl Mech.* 2024. V.60. P. 331–340. https://doi.org/10.1007/s10778-024-01286-6
5. Грібова В. В., Пєрстньова В. В. Розрахунок деформації прямокутної пластини з тонким лінійним включенням. *Actual problems of practice and science methods of their solution*: *IV International Science Conference*. *Milan*. 2022. С. 515–518.
6. Грібова В. В., Бовнегра Л. В., Торопенко О. В. Метод граничної коллокації при моделюванні задач про вигини шарнірно-опертої пластини з тонким лінійним включенням. *Informatics and Mathematical Methods in Simulation* 2024. Vol.14. No. 4, P. 344-349. DOI 10.15276/imms.v14.no4.344

SOLUTION OF THE PROBLEM OF BENDING OF A PLATE CLAMPED ALONG ITS CONTOUR WITH A THIN LINEAR INCLUSION BY THE METHOD OF MINIMIZING THE ENERGY ERROR

V. Gribova, L. Bovnegra, A. Toropenko

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: gribova@op.edu.ua, dlv5@ukr.net, toropenko.a.v@op.edu.ua

Folded shells, thin-walled rods, and other structures based on thin plate joints are widely used in mechanical engineering, aviation, and shipbuilding industries. The presence of reinforcing rods, supports, straight defects such as cracks and inclusions, or other inhomogeneities in structures significantly complicates their calculation. The design and creation of reliable and sufficiently economical structures necessitates the consideration of increasingly complex boundary value problems and, accordingly, the solution of an increasing number of differential equations that describe them. The foundation of the science of strength is fracture mechanics, which is based on identifying the nature of stress characteristics in the vicinity of crack-type defects and thin inclusions. The basis of the method for solving the problem is the construction of a model based on the method of minimizing the energy error. The main results are the construction of a system of solutions to a biharmonic equation in a region with a straight inclusion and the application of the boundary collocation method to find the coefficients of the linear combination. The aim of the work is to solve complex boundary problems of fracture mechanics for thin-walled structures with inclusions by constructing a mathematical model based on the energy error minimization method and applying boundary collocation.

Keywords: system of biharmonic functions, boundary collocation method, class of functions with non-integrable features, plate deflections, energy error minimization method.

DOI 10.15276/imms.v15.no3.354
УДК 004.056.5:691.32

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 354-366

ОГЛЯД СУЧАСНИХ ЗАХИСНИХ МАТЕРІАЛІВ ДЛЯ ЗАПОБІГАННЯ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ ВІКОННІ КОНСТРУКЦІЇ

Н.Р. Дзяний, Х.С. Бесага, О.І. Гарасимчук, М.Є. Швед

Національний університет «Львівська політехніка»
12, Степана Бандери вул., Львів, 79013, Україна
Emails: nazarii.r.dzianyi@lpnu.ua, khrystyna.s.besaga@lpnu.ua, oleh.i.harasymchuk@lpnu.ua, mariia.y.shved@lpnu.ua

Представлено комплексний аналіз проблеми несанкціонованого зняття конфіденційної інформації через віконні конструкції. Розглянуто основні канали витоку даних: акустичний, що використовує лазерні системи для зчитування звукових коливань з поверхні скла, та електромагнітний, що виникає через вихід радіочастотних сигналів (Wi-Fi, Bluetooth) за межі приміщення. Проведено огляд та порівняльний аналіз сучасних пасивних методів захисту, що реалізовані безпосередньо в матеріалах вікон і не потребують зовнішнього живлення. Досліджено три ключові категорії матеріалів: модифіковане віконне скло, спеціалізовані самоклеючі плівки та стаціонарні функціональні покриття. На основі аналізу встановлено, що звичайне скло, навіть у багатошарових склопакетах, забезпечує лише часткове пригнічення вібрацій і не є надійним бар'єром проти сучасних засобів шпигунства. Натомість, спеціалізовані рішення, що містять металізовані шари, нано-сітки з благородних металів або діелектричні структури, демонструють значно вищу ефективність. У статті наведено кількісні показники екранування, вимірювані в децибелах (дБ), для різних матеріалів, що підтверджено міжнародними тестами (зокрема за стандартом ASTM F3057-14). Захисні плівки, такі як Signals Defense SD2500, забезпечують екранування до 40+ дБ, а інноваційні покриття на основі срібних нано-сіток можуть досягати рекордних показників 48–58 дБ, зберігаючи при цьому високу оптичну прозорість. Акцентовано на перспективності діелектричних покриттів, зокрема на основі діоксиду гафнію (HfO_2), які підвищують відбиття лазерного променя, залишаючись візуально непомітними. Зроблено висновок, що для досягнення максимального рівня кіберзахисту оптимальним є комбінування кількох підходів. Застосування багатокамерних склопакетів у поєднанні з нанесенням високотехнологічних покриттів або захисних плівок на внутрішнє скло створює надійний та довговічний бар'єр, що забезпечує конфіденційність інформаційного простору та стійкість до електронного шпигунства.

Ключові слова: кіберстійкість вікон, пасивний захист інформації, захисні віконні плівки, функціональні покриття для скла, діоксид гафнію, нано-сітки.

Вступ. Віконне скло традиційно є одним з найвразливіших місць щодо несанкціонованого зняття інформації. Через вікна зловмисники можуть дистанційно «читати» конфіденційні дані за допомогою лазерних систем акустичної розвідки (так званих лазерних мікрофонів), що знімають звукові коливання з поверхні скла і перетворюють їх на аудіосигнал [1]. Так само, звичайні вікна майже не перешкоджають виходу радіосигналів (Wi-Fi, Bluetooth тощо) з будівлі [2], що відкриває широкі можливості для електронного шпигунства. Тому нині існує нагальна потреба в кіберстійких віконних матеріалах – таких, що унеможливлюють або суттєво ускладнюють зчитування інформації через вікна.

Методи захисту інформації від «витоку» через вікна бувають активними і пасивними. Активні методи включають встановлення на шибках вібраційних випромінювачів або шумових генераторів, що створюють завади (наприклад, система Glass-Shield генерує випадкові коливання у склі і робить перехоплену лазером розмову нерозбірливою [3, 4]). Проте активні методи вартісні, потребують енергії та є легкодоступними з точки зору виявлення самого факту застосування захисту. Пасивні

методи реалізовані у самому матеріалі вікна – спеціальному склі, плівці чи покритті – захищають інформацію без додаткового обслуговування і є непомітні. Нижче проведено огляд сучасних пасивних рішень: спеціальних видів віконного скла, захисних самоклеючих плівок та стаціонарних покриттів на склі, що забезпечують кіберстійкість вікна. Розглянуто їхній склад, технологію отримання, захисні властивості, а також надано порівняння ефективності та рекомендації щодо оптимального вибору матеріалу.

Огляд літератури (аналіз досліджень і публікацій). Проблема несанкціонованого зняття інформації через вікна є предметом наукових досліджень протягом останніх десятиліть. Хоча зловмисники традиційно використовують акустичні канали витоку (так звані «лазерні мікрофони») та електромагнітні (витік Wi-Fi, Bluetooth), більшість досліджень донедавна зосереджувалась лише на окремих аспектах цієї проблеми.

Аналіз наявної літератури показує, що попередні роботи, які стосуються захисту інформації через вікна, можна розділити на кілька ключових груп:

1. Дослідження фізичних принципів витоку інформації.

Ця група робіт зосереджена на розумінні того, як саме звукові та радіосигнали поширюються через віконне скло. Фундаментальні дослідження, проведені Дудикевичем В.Б. та співавторами [1, 5], підтверджують, що вібраційні характеристики скла є ключовими для захисту від акустичного зондування. Зокрема, було доведено, що збільшення товщини скла та застосування багатокамерних склопакетів суттєво зменшує амплітуду коливань [5]. Робота [6] додатково деталізує вплив вібрацій на відхилення лазерного променя, що є основою для розуміння принципів протидії лазерному шпигунству. Дослідження Zeng Y. та колег [7] підтверджує ці висновки, надаючи кількісні дані, що коливання у двокамерних вікнах значно менші, ніж у одинарних.

2. Аналіз та розробка пасивних захисних матеріалів.

Ця категорія охоплює дослідження певних матеріалів, які можуть забезпечити кіберстійкість.

Спеціалізовані плівки**.** Біла книга компанії Signals Defense [8] та технічні специфікації [9] детально описують, як металізовані плівки ефективно екранують радіочастотні сигнали та ІЧ-випромінювання. Продукти, як HAVERKAMP PROFILON® [10], демонструють високі показники блокування RF- та IR-випромінювань, що підтверджено незалежними тестами.

Функціональні покриття**.** Публікації [11, 12] розглядають патентовані технології, такі як багатошарові Low-E покриття з сріблом та електромагнітне екранування, що забезпечує значне послаблення сигналу. Стаття [13] є особливо важливою, оскільки вона експериментально підтверджує, що навіть одношарове діелектричне покриття з діоксиду гафнію (HfO_2) може ефективно відбивати лазерний промінь, залишаючись прозорим. У роботах [14, 15] представлено передові дослідження в галузі нано-сіток з срібла та MXene, які забезпечують рекордне екранування при високій прозорості.

3. Дослідження активних і комбінованих систем захисту.

Хоча наш огляд зосереджений на пасивних методах, важливо відзначити роботи, що досліджують активні або гібридні системи. Наприклад, дослідження, описане в [3], стосується оптимізації лазерних датчиків для протидії ЛЗАР. Прес-реліз [4] описує систему Glassbel Glass-Shield, яка поєднує пасивні властивості скла з активним шумовим генератором. Ці роботи підкреслюють потребу в поєднанні матеріалознавства з електронними засобами для створення максимально надійного захисту.

Узагальнюючи, аналіз наявної літератури показує, що хоча окремі аспекти захисту були досліджені раніше, існує потреба в комплексному огляді та порівнянні різних пасивних рішень. Наше дослідження спрямоване на систематизацію інформації та проведення порівняльного аналізу, що допоможе зробити обґрунтований вибір між різними кіберстійкими матеріалами для вікон.

Мета роботи. Мета даного дослідження – проаналізувати та порівняти сучасні пасивні рішення для підвищення кіберстійкості вікон, які унеможливлюють або суттєво ускладнюють несанкціоноване зняття інформації.

Основний розділ. На відміну від активних систем, які вимагають постійного живлення та можуть бути виявлені, пасивні методи захисту, інтегровані в саму структуру вікна, пропонують непомітне, довговічне та економічно вигідне рішення для запобігання витоку інформації. Цей розділ присвячений детальному аналізу та порівнянню ключових пасивних технологій, що забезпечують кіберстійкість вікон. Розглянемо властивості спеціальних видів скла, ефективність захисних самоклеючих плівок та стаціонарних покриттів, а також їхній вплив на блокування лазерного прослуховування та витоку радіосигналів. На основі проведеного огляду буде обґрунтовано, які саме матеріали є найбільш ефективними та перспективними для застосування в сучасних умовах.

Звичайне віконне скло з потенційними захисними властивостями від кібератак.

Об’ємний електричний опір звичайного натрій-кальцієвого скла становить ~10^12 Ω·см (для порівняння, у свинцевого скла ~10^14 Ω·см) [16]. Боросилікатне скло BOROFLOAT® 33 має дуже високий світловий коефіцієнт пропускання у видимому діапазоні та незначну власну флуоресценцію, що робить його придатним для оптичних застосувань. Коефіцієнт термічного розширення BOROFLOAT® 33 – близько 3.25×10−6/K (20–300 °C), тобто у три рази нижчий, ніж у содово-вапняного скла [17]. Свинцевмісне радіаційно-захисне скло LX-57B містить ~55% оксиду свинцю і характеризується високою прозорістю: при товщині ~9 мм його світлопропускання становить ~87,8% у видимому діапазоні. Це скло забезпечує ефективний захист від рентгенівського випромінювання, не втрачаючи прозорості з часом (не жовтіє під дією радіації) [18]. Так, більшість видів скла має належні характеристики щодо світлопропускання, але жодне з них саме по собі не забезпечує необхідних властивостей з точки зору захисту від зчитування інформації з його поверхні

Але разом з тим, властивості самого скла суттєво впливають на здатність вікна передавати звукові коливання. Теоретичні та експериментальні дослідження показують, що чим товстіше скло, тим менше воно вібрує під впливом звуку [5]. Зокрема, максимальну амплітуду вимушених коливань спостерігають на тонких шибках ~1–2 мм; при товщині понад 2,5–3 мм вібрація значно зменшується [5]. Таким чином, для кращого захисту від лазерного прослуховування рекомендується застосовувати віконне скло товщиною не менше 3 мм. Ще ефективніше знижують вібрацію багатошарові та багатокамерні склопакети. Ламіноване скло (триплекс), що складається з двох шарів скла, переклеєних полімерною плівкою (PVB), поглинає значну частину звукових коливань: пластична проміжна плівка виконує роль демпфера, «гасить» вібрації і зменшує передачу звуку через скло [19]. Таке акустичне ламіноване скло широко застосовується для звукоізоляції приміщень і побічно ускладнює лазерне зчитування інформації. Крім того, подвійні склопакети дають суттєву перевагу: випробування показали, що коливання скла у подвійній рамі (двокамерному вікні) приблизно на 74% менші, ніж у одинарному вікні тієї ж товщини [7].

Моделювання також підтвердило перевагу подвійного скла: при однаковій сумарній товщині склопакета двошарове вікно має на 55% меншу амплітуду вібрацій, ніж одне скло, і навіть на 40% меншу, ніж потрійний склопакет [7]. Отже, двошарові ізольовані склопакети є оптимальними для пасивного пригнічення коливань та протидії лазерному зніманню звуку.

Щоб ускладнити лазерному далекоміру отримання стабільного відбитого променя можна також застосовувати і інший підхід – порушити оптичну однорідність вікна. Для цього застосовують рифлене, гофроване або матоване скло зі спеціально витравленим рельєфом. Нерівна поверхня розсіює лазерний промінь, не даючи йому відбитися строго назад до приймача, завдяки чому зняття інформації стає менш можливим. Подібний метод (гофровані шибки) згадується в наукових роботах як пасивний захід захисту

мовної інформації [6]. Однак постійно матове чи рифлене вікно є незручним у використанні (непрозоре для ока), тому цей підхід обмежений випадками, коли огляд через скло не потрібний.

До простих пасивних методів можна віднести також спеціальне тоноване або дзеркальне скло. Воно спрямоване більше на візуальну конфіденційність, але частково впливає й на лазерне прослуховування. Тоновані (затемнені) шибки поглинають частину світла і можуть трохи зменшити інтенсивність відбитого лазерного променя. Дзеркальне напилення (скло з однобічною дзеркальною поверхнею) відбиває значну частку видимого та інфрачервоного випромінювання, тому теоретично здатне знизити ефективність лазерного перехоплення. Проте звичайні сонцезахисні покриття, розроблені для відбиття сонячного тепла, не забезпечують належного антилазерного ефекту. Наприклад, дослідники з'ясували, що архітектурні плівки на основі сполук міді максимально блокують світло на хвилі ~500 нм (видимий діапазон), тоді як лазери працюють в діапазону 650–1550 нм, тому такі покриття фактично не захищають від прослуховування [20]. Отже, звичайне тонування скла є недостатнім для кіберзахисту – необхідні спеціальні матеріали, розраховані на блокування саме тих діапазонів, які використовують лазерні мікрофони та інші сенсори.

Самоклеючі захисні плівки для віконного скла**.** Одним із найпоширеніших способів підвищення кіберстійкості існуючих віконних конструкцій є використання самоклеючих багатошарових захисних плівок товщиною від кількох десятків до кількох сотень мікрометрів [9, 10, 22]. Такі плівки, як правило, наносяться на внутрішню поверхню скляних елементів і здатні одночасно виконувати низку функцій.

Принцип дії захисних плівок полягає в тому, що спеціальне прозоре покриття відбиває лазерне та інфрачервоне (ІЧ) випромінювання, що сприяє запобіганню несанкціонованому зчитуванню акустичних або електронних сигналів через скляні огороджувальні конструкції.

Типова захисна плівка складається з прозорого гнучкого полімерного базового шару (переважно поліетилентерефталату, ПЕТ), на який наносяться спеціалізовані функціональні покриття – металеві, оксидні або інші тонкі шари. Зі зворотного боку розташовується клейовий (адгезивний) шар, що забезпечує надійне кріплення плівки до поверхні скла.

Залежно від оптичних характеристик, зокрема рівня світлопропускання, розрізняють кілька типів захисних плівок: прозорі (майже непомітні на склі), частково прозорі (тоновані), а також дзеркальні (з низьким коефіцієнтом пропускання світла).

У контексті технічного захисту інформації найбільш ефективними є металізовані та дзеркальні плівки, які здатні відбивати ближнє та середнє інфрачервоне випромінювання. Завдяки цьому вони забезпечують екранування віконних конструкцій і унеможливлюють зчитування вібраційних коливань скла за допомогою лазерних засобів спостереження.

Світовими лідерами у цій сфері є спеціалізовані плівки типу *Signals Defenses* (SD) та *PROFILON AntiSpy*. Наприклад, американська плівка Signals Defense SD2500 пропускає менш як 1% випромінювання в діапазоні 800–2500 нм (майже повністю блокує інфрачервоні та радіочастотні сигнали), при цьому залишається напівпрозорою (~53% пропускання видимого світла) [21]. Виробник зазначає, що такі плівки утримують Wi-Fi та інші електронні сигнали всередині приміщення, запобігаючи їх перехопленню ззовні (принцип «безпека за рахунок ізоляції») [21]. Віконна плівка SD 2500 (Signals Defense) протестована за стандартом ASTM F3057-14 і демонструє в середньому понад 40 дБ послаблення радіочастотного сигналу в діапазоні 30 МГц – 6 ГГц. Це прозора металева плівка, розроблена для захисту від дистанційного перехоплення даних (відповідає вимогам безпеки США щодо електронного прослуховування) [9].

Інша серія – HAVERKAMP PROFILON® Laser/AntiSpy (Німеччина) – представлена плівками, призначеними спеціально для захисту від лазерного

прослуховування і електронного шпигунства. Вони є прозорими або слабко тонованими і майже не впливають на огляд, але мають найвищий у світі рівень блокування RF- та IR-випромінювань [10]. Тести, проведені державними установами США та Великобританії, підтвердили ефективність цих плівок [10]: покриті ними вікна екранують лазерні промені відповідних довжин хвиль, не даючи зчитати коливання скла.

Захисна плівка SpyLock 35 забезпечує оптичну прозорість ≥75% VLT (Visible Light Transmission) та екранування електромагнітного випромінювання не менше 32 дБ в діапазоні частот від 10 МГц до 26 ГГц. Ці характеристики підтверджені випробуваннями за методикою ASTM F3057-14 [22] Провідна захисна плівка RDF72 забезпечує близько 33 дБ послаблення електромагнітного поля на частоті 1 ГГц при коефіцієнті пропускання ~72% (видиме світло) . Плівка призначена для внутрішнього наклеювання на вікна; має легкий зелений відтінок і не значно знижує рівень освітлення, гарантуючи екранування ~99.9% потужності сигналу [23].

Практичний досвід показує, що нанесення правильно підібраної відбиваючої плівки може радикально ускладнити роботу лазерного прослуховування. За даними експериментів, якщо на склі є металізована плівка, зловмиснику доведеться збільшити потужність лазера принаймні в 10–30 разів, аби отримати прийнятний сигнал [24]. Найкращий ефект досягається у випадку подвійного скла: віддзеркалення і розсіювання променя максимальні, коли плівка наклеєна на зовнішнє скло, а лазер намагається зняти сигнал з внутрішнього. У такому разі перехоплення стає практично неможливим, адже значна частина лазерної енергії губиться на відбитті від плівки. Якщо ж плівку наклеїти з внутрішнього боку одинарної шибки, ефект дещо менший, але теж відчутний: плівка відбиває пряме ІЧ-випромінювання лазера і збиває фазу відбитого променя, заважаючи демодуляції звуку [24].

Захисні плівки виготовляються різними методами напилення й шарування матеріалів. Широко застосовуються металізовані плівки, де на прозорий поліестер нанесено ультра тонкий шар металу – зазвичай алюмінію, міді, срібла або нікель-хрому. Цей металевий шар виконує роль дзеркала для електромагнітних хвиль: він відбиває інфрачервоне світло і радіохвилі, зменшуючи їх проходження назовні. Для підсилення ефекту й розширення діапазону блокування структуру плівки доповнюють прозорими провідними оксидами – наприклад, шаром індій-олов'яного оксиду (ITO) або індій-цинкового оксиду. Оксидні шари одночасно прозорі у видимому спектрі й електропровідні, тому добре екранують СВЧ- та ІЧ-випромінювання [25]. Деякі сучасні плівки замість суцільного металу містять наносітку: наприклад, сітка з найтоншого мідного дроту з щільністю ~100 отворів/дюйм забезпечує дуже високий рівень екранування RF/EMI при помірному зменшенні прозорості [26]. Існують також експериментальні зразки з наночастинками: наприклад, додавання наночастинок певних оксидів у лакове покриття плівки може підвищити її вибіркове поглинання у заданому діапазоні [27]. Втім, надмірне поглинання небажане, адже призводить до нагрівання матеріалу і може з часом пошкодити плівку; тому перевага надається відбиваючим (дзеркальним або сітчастим) структурам [27, 28].

Окрім суто захисної функції, багато плівок поєднують інші корисні властивості. Так, металізовані плівки часто одночасно будуть і сонцезахисними – знижують нагрів приміщення, екранують UV випромінювання та мінімізують утворення світлових відблисків. Додатково більшість таких плівок виконують роль протиударних: зміцнюють скло, утримують уламки при розбитті і навіть забезпечують певний рівень протиосколкового захисту при вибухах [29]. Це робить їх привабливими для банків, офісів, військових об'єктів, де потрібна як кібер-, так і фізична безпека.

Слід зазначити, що ефективність плівки сильно залежить від її правильного вибору і монтажу. При наклеюванні важливо уникнути бульбашок і зазорів по краях – інакше лазерний промінь може частково пройти через дрібні дефекти. Такі плівки зазвичай довговічні (гарантія 10+ років), але з часом допускається виникнення поверхневих

дефектів (подряпин), тому рекомендується застосування захисних заходів від механічних навантажень. Загалом, сучасні високотехнологічні плівки є одним з найкращих і найгнучкіших рішень: вони відносно недорогі, можуть бути встановлені на існуючі вікна і демонструють високу ефективність у блокуванні як лазерних, так і радіочастотних атак. Більш того, окремі моделі плівок сертифіковані за стандартами *TEMPEST* (вимоги до секретних приміщень) [8].

Спеціальні покриття на віконному склі. Цей підхід передбачає нанесення на скло стаціонарного тонкого функціонального покриття під час виробництва або модернізації вікна. На відміну від плівок, що кріпляться механічно, покриття зазвичай напилюються на поверхню скла методом вакуумного осадження (магнетронне напилення, піролітичне осадження тощо) і виконують роль екранувального шару від електромагнітних впливів. Фактично, це аналог плівки, інтегрований у структуру самого скла.

Одне з найпростіших рішень – нанести на скло ультратонкий напівпрозорий шар металу з високою відбивною здатністю. У сучасних енергозберігаючих склопакетах використовуються, наприклад, шари срібла товщиною ~100 нм (т. зв. низькоемісійні *Low-E* покриття). Такі шари відбивають теплове ІЧ-випромінювання, а також значну частину ближнього ІЧ-діапазону, що частково перекриває робочі довжини хвиль лазерних мікрофонів. Проте срібло сильно відбиває і видиме світло (скло набуває дзеркального вигляду), тому типове Low-E покриття пропускає лише ~70–80% видимого світла. Для підвищення прозорості застосовують багатошарові інтерференційні покриття: чергуючи металеві й діелектричні шари, можна налаштувати спектральну характеристику. Наприклад, автори розробили багатошарове покриття з чергуванням тонких шарів срібла, нікель-хромового сплаву і діелектрика (SiO_2 або ITO), яке забезпечує високий коефіцієнт відбиття в ІЧ-діапазоні при 50–70% прозорості [11]. Такі багатошарові структури можуть наноситися і на скло: декілька виробників пропонують скло з електромагнітним екрануванням – як правило, це триплекс із напиленою на внутрішню сторону провідною сіткою або шаром оксиду металу, захищеним додатковим шаром скла [12].

Перспективним напрямком є використання нано-сіток та графеноподібних матеріалів. Дослідження показують, що сітчасті металеві покриття з розміром чарунок у десятки мікрон можуть створити ефективний широкосмуговий екран із прозорістю понад 90% [28]. Також випробовуються прозорі наноматеріали – напр. плівки з MXene та срібних нанодротів – які здатні екранувати СВЧ- та ближній ІЧ-діапазон, пропускаючи видиме світло (досягаються показники ослаблення ~40–50 дБ на GHz частотах при ~85% прозорості) [28]. У іншій своїй роботі [27] вченими також розроблено гібридну плівку: сітчастий каркас із наношарів MXene, заповнений срібними нанодротами. Отримано гнучке прозоре покриття з коефіцієнтом пропускання ~81% та екрануванням ~24,6 дБ. Комбінована структура забезпечує баланс між електропровідністю і прозорістю, придатний для захисту екранів та гнучкої електроніки. Втім, ці технології поки що перебувають на стадії розробки і не представлені на масовому ринку.

Спеціальне скло Pilkington DatastopTM з прозорим провідним покриттям забезпечує значне екранування електромагнітних коливань. При побудові екранованого приміщення з використанням Datastop (у вигляді подвійного склопакета) незалежні випробування показали послаблення сигналу в межах 40–70 дБ у діапазоні 10 МГц – 10 ГГц (понад 60 дБ на частотах 1–5 ГГц). Для досягнення максимального захисту покриття Datastop повинно мати електричний контакт по периметру з металевою рамою (створюючи безперервну клітку Фарадея) [30]. Архітектурне скло з потрійним низькоемісійним покриттям Solarban 70XL здатне блокувати значну частку RF-випромінювання. В дослідженні Vitro зазначено, що ламіноване скло з одним шаром потрійного Ag-покриття забезпечує ~40 дБ екранування, а з двома такими шарами – до ~54 дБ при збереженні високої прозорості. Це відповідає ~99–99,99% зниженню потужності радіосигналу [31]. Провідне оксидне покриття NSG TEC 7 (фтор-допований

SnO_2) характеризується листовим опором ~6–8 Ω/□ і високим світлопропусканням (~80–85% видимого світла). Хімічно стійке піроелектричне покриття наноситься он-лайн методом CVD, що забезпечує довговічність. Хоча екранувальна ефективність FTO-покриття дещо нижча, ніж у срібловмісних, скло NSG TEC 7 здатне забезпечувати порядку десятків децибел послаблення RF-сигналів, залишаючись прозорим [32]. Дослідниками з Університету Пітсбурга [14] виготовлено вмонтовану в скло срібну сітку з шириною ліній ~1.6–3.5 μm і товщиною до 2 μm. Така сітка досягла рекордних показників: екранування ~48–58 дБ при прозорості 90.3% – 83% відповідно. Срібна сітка, заповнена в мікролітографічно витравлені канали скла, формує прозорий електропровідний шар з найвищою ефективністю серед відомих технологій екранування. У роботі [33] запропоновано дво-смугову частотно-вибіркову структуру (FSS) на склі, що незалежно від поляризації забезпечує придушення сигналу Wi-Fi: до 45 дБ на частоті 2,4 ГГц і 43 дБ на 5,4 ГГц. При цьому конструкція залишається прозорою для ока (~70% VLT) та може інтегруватися у віконне скло без помітного впливу на освітленість.

Цікавий підхід запропоновано у роботі [13]: замість металів використано діелектрик з дуже високим показником заломлення, щоб підвищити відбивання лазера від скляної поверхні. Експериментально випробувано одношарове покриття з діоксиду гафнію (HfO_2), нанесене методом вакуумного напилення. Діоксид гафнію має показник заломлення ~2,0 (проти ~1,5 у звичайного скла), тож тонка плівка HfO_2 діє як просвітлювальне чи відбивальне інтерференційне покриття залежно від довжини хвилі. В результаті вимірювань зразків скла з таким покриттям встановлено, що в діапазонах 300–350 нм, 500–700 нм та 1000–1500 нм коефіцієнт відбиття від скла збільшується майже вдвічі порівняно з чистим склом. Зокрема, на важливій довжині ~550 нм відбиття зросло в 1,8 рази [13]. При цьому покриття не погіршує прозорості: HfO_2 є безбарвним і хімічно стійким, не розчиняється у воді та витримує високі температури. Візуально скло з таким напиленням практично не відрізняється від звичайного (людина не помітить різниці), тож зловмисник може навіть не здогадуватися, що шибка захищена. Це велика перевага, адже лазерний мікрофон може бути задіяний проти такого скла, але отриманий сигнал буде значно слабкішим, ніж очікувалося (частина променя розсіється і відіб'ється вбік). Важливим є те, що діоксид гафнію належить до класу неорганічних сполук, шари яких характеризуються високою адгезією до скла та забезпечують тривалу експлуатаційну стабільність. Завдяки хімічній інертності HfO_2 зберігає структурну цілісність за дії вологи, ультрафіолетового випромінювання та інших зовнішніх факторів, що зумовлює його довговічність. Матеріал вирізняється високою твердістю, оптичною прозорістю та стійкістю до механічних пошкоджень, що робить його практично невидимим у застосованих покриттях. Крім того, технологія нанесення діоксиду гафнію є відносно простою та сумісною зі стандартними виробничими процесами. Сукупність зазначених властивостей дозволяє розглядати HfO_2 як один із найбільш перспективних матеріалів для формування антилазерних покриттів, що поєднують ефективність, довговічність і непомітність.

Додаткові рішення**.** Окрім згаданих підходів, варто зазначити використання додаткових елементів, що підвищують захист. Наприклад накладні *панелі-протишпигуни*: прозорі панелі, що можна опускати перед вікном і які містять шар рідини або пластику, що динамічно змінює прозорість (під впливом електрики). Електрохромне скло може за командою миттєво стати матовим, порушивши видимість і лазерне прослуховування. Такі технології наразі дорогі, але в перспективі можуть стати частиною «розумних» кіберзахисних вікон.

Перспективними є також активно-пасивні системи: коли спеціальне прозоре покриття поєднується з електронікою. Згаданий продукт *Glass-Shield* від компанії *Glassbel* – це ламіноване скло зі струмопровідним прозорим шаром та під'єднаними електродами, що подають випадкові коливання (шум) на скло. В результаті лазер, навіть проникнувши через пасивні захисні шари, зчитує лише хаотичні коливання, а не

реальний голос, і розмова залишається конфіденційною. Хоча такі рішення виходять за рамки матеріалознавства (вимагають джерела сигналу), їх поява свідчить про тенденцію до комбінування матеріалів і електронних засобів для максимального захисту.

Отже, розглянуті три групи матеріалів – спеціальне скло, самоклеючі плівки, покриття – мають свої переваги й недоліки. Нижче подано таблицю, яка узагальнює ключові рішення для вікон (звичайне скло, скло з плівками, скло з функціональними покриттями), що забезпечують стійкість до зчитування інформації. Зазначено тип матеріалу, основу (склад скла або плівки), метод екранування, основні властивості (видима прозорість, ефективність екранування в дБ, поверхневий опір, діелектричні втрати, коефіцієнт термічного розширення, стійкість до корозії), а також придатність для використання у кіберзахищених об'єктах (таблиця 1).

Таблиця 1.

Узагальнення ключових рішень для вікон (звичайне скло, скло з плівками, скло з функціональними покриттями), що забезпечують стійкість до зчитування інформації

Категорія	Назва та тип матеріалу	Виробник / Джерело	Прозорість	Екранування (дБ)	Поверхневий опір (Ω/□)	Коеф. терм. розширення (CTE)	Діелектричні втрати	Стійкість до корозії	Придатність до захисту
Звичайне скло [16]	Натрій-кальцієве скло	Патент США	~90%	~0	~10^12	≈9×10⁻⁶	Дуже малі	Добра	Ні
Звичайне скло [17]	Боросилікатне скло BOROFLOAT® 33	SCHOTT	89–91%	N/A	10^16	~3.25×10⁻⁶	Малі	Висока	Так
Звичайне скло[18]	Плюмбумвмісне скло (LX-57B)	A&L Shielding	~86–88%	N/A	N/A	~8×10⁻⁶	Незначні	Висока	Ні
Скло + плівка[22]	Vianovix SpyLock 35	Vianovix	≥75%	≥32 дБ	N/A	~60×10⁻⁶	Малі	Помірна	Так
Скло + плівка [9]	Signals Defense SD 2500	Signals Defense	~53%	>46 дБ	N/A	~60×10⁻⁶	Малі	Висока	Так
Скло + плівка [23]	YShield® RDF72	YShield	~72%	~33 дБ	~10	~60×10⁻⁶	Малі	Середня	Так
Скло з покриттям [30]	Pilkington DataStop™	NSG Pilkington	70–80%	~45 дБ	1–2	≈9×10⁻⁶	Малі	Висока	Так
Скло з покриттям [31]	Vitro Solarban 70XL	Vitro Architectural Glass	~64%	~40–54 дБ	5–15	≈9×10⁻⁶	Малі	Середня	Частково
Скло з покриттям [32]	NSG TEC 7	NSG Pilkington	~80–85%	~20–30 дБ (оцінка)	7–8	≈7×10⁻⁶	Малі	Висока	Так
Інновації [14]	Embedded Silver Mesh (Ag сітка)	Univ. of Pittsburgh	83–90.3%	48–58 дБ	<1	~9×10⁻⁶	Малі	Висока	Так
Інновації [15]	MXene/Ag NW Hybrid Film	Beijing Univ. Chem. Tech.	~81%	24.6 дБ	N/A	~8×10⁻⁶	Високі	Помірна	Так
Інновації [33]	Dual-band FSS Glass	North Dakota State Univ.	~70%	43–45 дБ	N/A	~9×10⁻⁶	Малі	Середня	Так

Обговорення результатів дослідження. Проведений аналіз демонструє, що існуючі пасивні рішення для кіберзахисту вікон мають різні механізми дії та ефективність. Звичайне скло, навіть товсте або багатошарове (триплекс, склопакети), хоча і зменшує амплітуду коливань під впливом звуку, не забезпечує повного блокування лазерного

прослуховування чи екранування радіосигналів. Його ефективність є скоріше побічним ефектом, ніж цілеспрямованою захисною властивістю. Застосування рифленого або матованого скла, хоча й порушує оптичну однорідність, суттєво обмежує функціональність вікна, роблячи його непрозорим. Таким чином, звичайне скло не може бути використане як повноцінний кіберстійкий матеріал.

На противагу цьому, спеціалізовані плівки (наприклад, Signals Defense та PROFILON AntiSpy) та функціональні покриття (Pilkington Datastop, скло з потрійним Low-E покриттям) демонструють значно вищу ефективність. Вони працюють за принципом відбиття та поглинання електромагнітного випромінювання, включаючи інфрачервоний діапазон, що використовується лазерними мікрофонами, та радіочастотний спектр (Wi-Fi, Bluetooth).

Найбільш значущі наукові результати, отримані в ході дослідження, можна узагальнити наступним чином.

Самоклеючі плівки є найгнучкішим і найдоступнішим рішенням для модернізації вже існуючих вікон. Вони забезпечують високий рівень екранування (до 40+ дБ), що відповідає вимогам стандарту ASTM F3057-14. Їх ефективність залежить від складу (металізовані шари, наносітки) та правильного монтажу. Плівки також можуть мати додаткові функції, такі як сонцезахист і протиударні властивості, що робить їх багатофункціональним інструментом захисту.

Функціональні покриття, що наносяться на скло під час виробництва, є більш довговічними та естетично привабливими. Вони можуть бути інтегровані безпосередньо в багатошарові склопакети, створюючи єдину захищену структуру. Дослідження показали, що покриття на основі срібних наносіток та спеціально розроблених інтерференційних структур можуть забезпечувати екранування до 50-60 дБ при високій прозорості, що є рекордним показником.

Використання діелектричних покриттів, зокрема діоксиду гафнію (HfO_2), є перспективним, оскільки вони підвищують відбиття лазерного променя без значного впливу на прозорість вікна. Це робить їх непомітними для зловмисника, що є важливою перевагою з точки зору конфіденційності.

Аналіз літературних джерел дозволяє стверджувати, що для досягнення максимального захисту оптимальним є комбінування декількох підходів. Зокрема, використання багатокамерних склопакетів у поєднанні з функціональним покриттям або високоефективною захисною плівкою на внутрішньому склі створює найбільш надійний бар'єр проти лазерного та радіочастотного шпигунства.

Висновки. Порівняння переваг і недоліків показує, що універсального матеріалу не існує. Кожен підхід має компроміси між прозорістю, екрануванням, довговічністю та технологічністю. Монолітне скло є базовим матеріалом з відмінною оптичністю та високою механічною довговічністю, проте без додаткових заходів не забезпечує захисту від електромагнітних загроз. Плівки привабливі простотою встановлення та можливістю модернізації наявних вікон. Неметалізовані полімерні плівки можуть слугувати для зміцнення (проти уламків) і тонування, але не екранують радіочастоти. Натомість металізовані плівки надають помірний рівень захисту (десятки децибел ослаблення) і здатні підвищити безпеку інформаційного середовища, хоча їх довговічність обмежена: з часом можливі зношення, відшарування країв, помутніння або подряпини, що погіршують оптичні властивості. Функціональні покриття (ITO, Low-E) інтегруються у структуру скла під час виробництва, забезпечуючи довготривалу дію та рівномірне екранування по всій поверхні. Їх перевага – поєднання прозорості та екранування: тонкі оксидні шари практично не впливають на видимість, зате знижують проникність скла для радіохвиль на порядки. Такі покриття стабільніші за плівки (не піддаються випадковому механічному пошкодженню, якщо нанесені всередині склопакета), але їх нанесення потребує високотехнологічних процесів і додає вартості; вони не підлягають ремонту без заміни всього скляного модуля. MXene- та FSS-рішення нині перебувають

на стадії досліджень. MXene-плівки вирізняються гнучкістю та потенціалом досягти високого екранування при мінімальній товщині, однак відкритими залишаються питання їх довговічності (стійкість до окиснення, вологи, ультрафіолету) і масштабування виробництва. FSS-візерунки забезпечують вибіркове екранування, даючи змогу «відкрити вікно» для потрібних сигналів або світла, не жертвуючи безпекою. Недолік – складність дизайну та виготовлення: для ефективної роботи FSS-елементи повинні мати мікрометрові розміри і точну періодичність, що вимагає прецизійних методів друку або травлення. Щоб зберегти прозорість, металева сітка повинна бути досить тонкою, а це знижує її міцність; тому такі покриття доцільно захищати, ламінуючи їх між шарами скла. Ймовірно, саме такі комбіновані матеріали здатні забезпечити оптимальний баланс між прозорістю та екрануванням і, ймовірно, визначатимуть розвиток технологій кіберстійких вікон для SCIF, центрів обробки даних та інших критичних об'єктів у найближчому майбутньому.

Вибір конкретного рішення залежатиме від необхідного рівня захисту, допустимого впливу на прозорість та бюджету. Для максимального захисту секретного приміщення варто комбінувати підходи: наприклад, встановити ламіновані подвійні склопакети з вбудованим покриттям (оксидним або сітчастим), а додатково всередині наклеїти захисну плівку. Така багаторівнева оборона зробить витік інформації практично неможливим: навіть якщо лазер частково пройде скло, його відбиватиме плівка; а RF-сигнали будуть ослаблені і покриттям, і плівкою. Звісно, у більшості випадків достатньо чогось одного – плівки як найбільш гнучкого рішення. Встановлення спеціалізованої багатофункціональної плівки на існуючі вікна дає значний ефект за відносно низької вартості і мінімального впливу на зовнішній вигляд. Якщо ж будівля лише проектується, доцільно обрати склопакети із кіберстійким покриттям – наприклад, енергозберігаючі пакети з додатковим захисним напиленням або з інтегрованою металевою сіткою.

Список літератури

1. Дудикевич В. Б., Собчук І. С., Ракобовчук В. О. Пасивний захист інформації від лазерного зондування. *Вісник НУ «Львівська політехніка»*. 2013. №771. С. 118–123. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3667/dudykevychvbsobchukisrakobovchukvo.pdf
2. Ängskog P., Bäckström M., Vallhagen B. Measurement of Radio Signal Propagation through Window Panes and Energy Saving Windows. *Proc. IEEE International Symposium on Electromagnetic Compatibility*. 2015. P. 74–79. URL: https://www.diva-portal.org /smash/get/diva2:860029/FULLTEXT01.pdf
3. Дудикевич В. Б., Опірський І. Р., Дзяний Н., Ракобовчук Л., Гаранюк П. Дослідження оптимізації параметрів лазерного датчика вібрації для протидії лазерним системам розвідки. *Кібербезпека: освіта, наука, техніка*. 2022. №3(15). С. 110–123. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/339
4. Trend Topic (Glassbel). Surveillance-proof window glass (Glassbel Glass-Shield). *Прес-реліз Glassbel*. 2020.
5. Дудикевич В. Б. Собчук І. С., Гаранюк П. І., Ракобовчук В. О., Дей В. А. Аналіз захисних характеристик сучасних видів скла в широкому діапазоні частот по акустичному каналу витоку. *Інформатика та математичні методи в моделюванні*. 2014. Т. 4. №4. С. 324–331. URL: http://www.irbis-nbuv.gov.ua/publ/REF-0000600525
6. Партика А. Дослідження впливу параметрів вібруючої поверхні на значення відхилення відбитого лазерного променю. *Наук. вісник НУ «Львівська політехніка».* 2014. №797. С. 3–8. URL: https://ena.lpnu.ua:8443/server/api/core/bitstreams/340f09e5-92e9-460a-ba0d-cf946b14935c/content
7. Zeng Y., Pan P., Cao Y. Test and analysis of window vibration for anti-laser-eavesdropping. *Applied Acoustics.* 2021. Vol. 176. 107871. URL: https://www.sciencedirect.com/science/article/abs/pii/S0003682X20309762

8. Signals Defense LLC. RF Window Film: An Innovative Solution for Data and Privacy Protection. *White Paper*. Oct 2023. URL: https://signalsdefense.com/rf-window-film-an-innovative-solution-for-data-and-privacy-protection/
9. Bonwyke Ltd. SD2500/2510 Technical Specification. 2020. URL: https://www.bonwyke.co.uk/wp-content/uploads/2020/08/SD2500_2510TechSpec_2016.pdf
10. Haverkamp GmbH. Profilon Shielding Films – Protection against eavesdropping. 2025. URL: https://www.folienverbund.ch/wp-content/uploads/2022/04/HAVERKAMP_PROFILON-AntiSpy.pdf
11. US Department of Defense. Low Emissivity and EMI Shielding Window Films. US Patent US20110308693A1. 2011. URL: https://patentimages.storage.googleapis.com/9b/51/83/1c1ede29d97e2a/US20110308693A1.pdf
12. Pilkington (NSG Group). DataStop Electromagnetic Shielding Glass – Product Brochure. 2010. URL: https://www.ramayes.com/data%20files/tempest%20security/new_datastop_brochure.pdf
13. Ракобовчук Л. М., Дзяний Н. Р., Антоневич М. С. Захисні характеристики плівок від лазерних систем акустичної розвідки на прикладі одношарового відбиваючого покриття діоксиду гафнію. *Український наук. журн. інформаційної безпеки*. 2023. Т. 29. №1. С. 32–40. URL: https://www.researchgate.net/publication/370827426
14. Li M., Zarei M., Mohammadi K., Walker S. B., LeMieux M., Leu P. W. Silver Meshes for Record-Performance Transparent Electromagnetic Interference Shielding. ACS Applied Materials & Interfaces. 2023. Vol. 15. P. 30591–30599. URL: https://doi.org/10.1021/acsami.3c04428
15. Jin M., Chen W., Liu L.-X., Zhang H.-B., Ye L., Min P., Yu Z.-Z. Transparent, conductive and flexible MXene grid/silver nanowire hierarchical films for high-performance electromagnetic interference shielding. *Journal of Materials Chemistry A*. 2022. Is. 27. URL: https://doi.org/10.1039/D2TA03689D
16. US Patent. Transparent EMI-shielded window. US4152741. URL: https://patents.google.com/patent/US4152741
17. University of Chicago. Borofloat 33 – Technical Data Sheet. URL: https://psec.uchicago.edu/glass/borofloat_33_e.pdf
18. Radiation Shielding Glass – Technical Datasheet. AL Shielding. URL: https://alshielding.com/wp-content/uploads/2019/07/Radiation_Shielding_Glass_2.0mm_max_lead_equivalency.pdf
19. bQuiet. The Science Behind Soundproof Windows. *Блогова стаття*. 2025. URL: https://bquiet.ca/the-science-behind-soundproof-windows/
20. Signals Defense. Shielding Films. URL: https://signalsdefense.com/shielding-films/
21. Mass International. Smartgard Signals Defense Anti-Eavesdropping Glazing. URL: https://www.massinternational.com/shop-2/smartgard-ballistic-blast-rated-glazing/smartgard-signals-defense-anti-eavesdropping-glazing
22. Solartek Films. Vianovix Spylock 35 Shielding Report. URL: https://solartekfilms.co.uk/assets/window-film/datasheets/Vianovix-Spylock-35-shielding-report.pdf
23. YShield. RDF72 HF Shielding Window Film – Product Page. URL: https://www.yshield.com/en/yshield-shielding-window-film-rdf72-hf-width-152-cm-1-meter_171_1102/
24. Дзяний Н. Р. Захист мовної інформації від лазерних систем акустичної розвідки. Дис. д-ра філософії (техн. наук). Львів: НУ «Львівська політехніка», 2024. 190 с.
25. Dontech. EMI/RFI Shielding Products; MDPI *Applied Sciences*. 2023. Vol. 13(8). 4846. URL: https://dontech.com/design-elements/emi-rfi-shielding-products/ https://www.mdpi.com/2076-3417/13/8/4846

26. Parker Chomerics (Parker Hannifin Corp.). Win-shield G EMI Shielded Glass Windows – Spec Sheet. 2013. URL: https://www.parker.com/content/dam/Parker-com/Literature/Chomerics/Parker-Chomerics-WIN-SHIELD-G-TB1085.pdf
27. Klochko N. P., Barbash V. A. Biodegradable transparent films with copper iodide and nanocellulose for UV and high-energy visible light protection. *Solar Energy*. 2021. Vol. 220. P. 852–863. URL: https://www.sciencedirect.com/science/article/abs/pii/S0038092X21002954
28. Deng Y., Chen Y., Liu W., Wu L., Wang Z., Xiao D., Meng D., Jiang X., Liu J., Zeng Z., Wu N. Transparent electromagnetic interference shielding materials using MXene (Review). *Carbon Energy*. 2024. Vol. 6(11). e593. URL: https://onlinelibrary.wiley.com/doi/full/10.1002/cey2.593
29. Safe Living Technologies. Signal Protect Clear RF Shielding Window Film – Product Specifications. 2023. URL: https://safelivingtechnologies.com/content/Products/SignalProtectClearWindowFilmSpecifications.pdf
30. Pilkington (NSG Group). NSG TEC European Technical Datasheet. 2025. URL: https://pilkington.com.tr/wp-content/uploads/2025/06/NSG_TEC_European_technical_datasheet.pdf
31. Vitro Architectural Glass. TD-151 Technical Data. URL: https://www.vitroglazings.com/media/111k3zcc/vitro-td-151.pdf
32. Pilkington (NSG Group). NSG TEC European Technical Datasheet. 2025. URL: https://pilkington.com.tr/wp-content/uploads/2025/06/NSG_TEC_European_technical_datasheet.pdf
33. Farooq U., Iftikhar A., Najam A. I., Khan Sh. A., Shafique M. F. An optically transparent dual-band frequency selective surface for polarization independent RF shielding. *Optics Communications*. 2023. Vol. 546. 129824. DOI: https://doi.org/10.1016/j.optcom.2023.129824

Н.Р. Дзяний, Х.С. Бесага, О.І. Гарасимчук, М.Є. Швед

REVIEW OF MODERN PROTECTIVE MATERIALS FOR PREVENTING CONFIDENTIAL INFORMATION LEAKAGE THROUGH WINDOW STRUCTURES

N. Dzianyi, Kh. Besaga, O. Harasymchuk, M. Shved

Lviv Polytechnic National University
12, Stepan Bandera St., Lviv, 79013, Ukraine
Emails: nazarii.r.dzianyi@lpnu.ua, khrystyna.s.besaga@lpnu.ua,
oleh.i.harasymchuk@lpnu.ua, mariia.y.shved@lpnu.ua

The paper examines window structures as potential channels of data leakage. Two main vectors are considered: the acoustic channel, which employs laser systems to capture sound vibrations from glass surfaces, and the electromagnetic channel, which arises from the leakage of radio frequency signals (Wi-Fi, Bluetooth) beyond the premises. A review and comparative analysis of modern passive protection methods—implemented directly in window materials without requiring external power supply—has been conducted.

Three key categories of materials were studied: modified window glass, specialized self-adhesive films, and stationary functional coatings. The analysis shows that ordinary glass, even in multilayer double-glazed units, provides only partial suppression of vibrations and cannot be regarded as a reliable barrier against advanced espionage tools. In contrast, specialized solutions containing metallized layers, nanoscale grids of noble metals, or dielectric structures demonstrate significantly higher efficiency. The paper presents quantitative shielding indicators, measured in decibels (dB), for different materials, confirmed by international testing (including ASTM F3057-14). Protective films such as Signals Defense SD2500 provide shielding up to 40+ dB, while innovative coatings based on silver nanogrids can achieve record values of 48–58 dB while maintaining high optical transparency. Special attention is given to dielectric coatings, particularly hafnium dioxide (HfO_2), which enhance laser beam reflection while remaining visually undetectable.

It is concluded that achieving the maximum level of cyber protection requires a combination of several approaches. The use of multi-chamber double-glazed units, combined with the application of high-tech coatings or protective films on the inner glass, creates a reliable and durable barrier that ensures information confidentiality and resilience against electronic espionage.

Keywords: window cyber resilience, passive information protection, protective window films, functional glass coatings, hafnium dioxide, nanogrids.

DOI 10.15276/imms.v15.no3.367
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 367-376

АСПЕКТИ ПОБУДОВИ ТА ЗАСТОСУВАННЯ СИСТЕМ АНАЛІЗУ КЛАВІАТУРНОГО ПОЧЕРКУ ДЛЯ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

С.В. Євтушенко

Національний університет «Одеська юридична академія»
2, Академічна вул., Одеса, 65000, Україна
Email: serhiyevtushenko@gmail.com

Предметом дослідження в статті є системи аналізу клавіатурного почерку для автентифікації користувачів з використанням методів штучного інтелекту та їх інтеграція з сенсорами мобільних пристроїв. Мета роботи – аналіз аспектів побудови та застосування систем аналізу клавіатурного почерку для автентифікації користувачів з використанням методів штучного інтелекту та дослідження перспектив їхнього розвитку для створення мультимодальних біометричних систем. У статті вирішуються такі завдання: формування моделі архітектури багаторівневих систем клавіатурної динаміки; систематизація методів штучного інтелекту для аналізу темпоральних патернів набору тексту; аналіз підходів до інтеграції гіроскопів та акселерометрів мобільних пристроїв для створення мультимодальних біометричних систем; дослідження методів інтерпретації результатів моделей глибокого навчання в контексті біометричної автентифікації. Використовуються такі методи: математичного оброблення темпоральних послідовностей клавіатурного вводу; глибокого навчання з архітектурами LSTM, CNN та Transformer; статистичного аналізу поведінкових патернів; машинного навчання з контрольованими та неконтрольованими алгоритмами; ансамблевих підходів для підвищення точності класифікації. Здобуто такі результати: сформульовано принципи побудови багаторівневої архітектури систем клавіатурного почерку; систематизовано методи штучного інтелекту для аналізу біометричних характеристик набору тексту; проаналізовано сучасні комерційні реалізації з показниками EER 0.10-0.20% для провідних систем; досліджено перспективи інтеграції сенсорів мобільних пристроїв для досягнення EER до 6.4% в мультимодальних системах. Висновки: застосування методу поєднання клавіатурної динаміки з даними гіроскопів та акселерометрів дозволяє створювати високоточні системи безперервної автентифікації з підвищеною стійкістю до атак імітації та можливістю адаптації до еволюції поведінкових патернів користувачів.
Ключові слова: клавіатурний почерк; біометрична автентифікація; штучний інтелект; глибоке навчання; мультимодальні системи.

Вступ. Клавіатурний почерк або keystroke dynamics представляє унікальну поведінкову біометричну технологію, яка аналізує індивідуальні особливості набору тексту для автентифікації користувачів. У сучасних умовах зростання кіберзагроз та необхідності забезпечення безперервної автентифікації користувачів, системи аналізу клавіатурного почерку набувають особливого значення як ефективний та економічно доцільний метод біометричної ідентифікації. На відміну від фізіологічних біометричних характеристик, поведінкові особливості набору тексту важче підробити або скопіювати, що робить цю технологію особливо привабливою для сучасних систем кібербезпеки.

Динаміка клавіатурного вводу відображає унікальні нейромоторні патерни кожної людини, які формуються протягом років навчання та практики набору тексту. Ці патерни включають час утримання клавіш (dwell time), інтервали між натисканнями (flight time), ритм набору та характеристики тиску. Сучасні дослідження демонструють, що інтеграція методів штучного інтелекту з аналізом клавіатурного почерку дозволяє досягати високих показників точності автентифікації при збереженні зручності використання для кінцевих користувачів.

Особливе значення набуває розвиток систем безперервної автентифікації, які здатні контролювати ідентичність користувача протягом всієї сесії роботи, що критично

важливо для захисту від атак з перехоплення сесій та внутрішніх загроз. Інтеграція сенсорів смартфонів, зокрема гіроскопів та акселерометрів, відкриває нові горизонти для мультимодальної біометричної автентифікації, що поєднує традиційний аналіз клавіатурного почерку з аналізом рухових патернів пристрою.

Теоретичні основи та класифікація систем клавіатурного почерку. Клавіатурний почерк належить до категорії поведінкових біометричних технологій, які на відміну від фізіологічних характеристик, аналізують набуті або навчені поведінкові патерни. Фундаментальною основою цієї технології є припущення, що кожна людина має унікальний стиль набору тексту, який відображає індивідуальні особливості нейромоторної координації, фізіологічних характеристик рук та пальців, а також сформованих протягом життя звичок набору тексту [1].

Історичні корені концепції клавіатурного почерку сягають XIX століття, коли телеграфісти могли розпізнавати один одного за характерним стилем передачі азбуки Морзе, відомим як "кулак відправника". Під час Другої світової війни ця техніка виявилася цінною для розрізнення дружніх операторів від ворожих на основі їхніх відмінних патернів передачі сигналів. Сучасні системи аналізу клавіатурного почерку успадкували цей принцип, адаптувавши його для цифрових клавіатур та сенсорних екранів.

Динамічні характеристики клавіатурного почерку включають декілька ключових параметрів. Час утримання клавіші (dwell time) представляє інтервал між натисканням та відпусканням окремої клавіші, відображаючи індивідуальні особливості тиску пальців та механіки набору. Час польоту (flight time) характеризує інтервали між послідовними натисканнями клавіш та має декілька варіантів вимірювання: down-down (між натисканнями двох клавіш), up-down (між відпусканням однієї клавіші та натисканням наступної), up-up (між відпусканням двох послідовних клавіш). Ці параметри формують унікальний темпоральний відбиток для кожного користувача [2].

Статистичні параметри клавіатурного почерку охоплюють широкий спектр метрик, включаючи середні значення та дисперсію часових інтервалів, аналіз розподілів ймовірностей для різних комбінацій клавіш, патерни швидкості набору та консистентності ритму. Особливе значення мають діграми (двосимвольні послідовності) та триграми (трисимвольні послідовності), які дозволяють аналізувати контекстуальні особливості набору конкретних комбінацій символів. Біометричні особливості включають глобальні характеристики (загальна швидкість набору, частота помилок, використання спеціальних клавіш) та локальні характеристики (специфічні темпоральні патерни для окремих клавіш та їх комбінацій) [3].

Сучасні системи також інтегрують аналіз патернів виправлення помилок, використання клавіш-модифікаторів (Shift, Ctrl, Alt), навігаційних клавіш та специфічних стилів капіталізації тексту. Ці розширені характеристики дозволяють створювати більш детальні та стійкі біометричні профілі користувачів, що підвищує загальну точність автентифікації та знижує ймовірність успішних атак імітації.

Архітектура та компоненти систем аналізу клавіатурного почерку. Сучасні системи аналізу клавіатурного почерку мають багаторівневу архітектуру (рис. 1), яка включає шари збору даних, попередньої обробки, екстракції ознак, класифікації та прийняття рішень. Шар збору даних забезпечує реєстрацію подій клавіатури в реальному часі з високоточними мітками часу, абстракцію від різних типів клавіатур та фільтрацію системних подій. Особливої уваги потребує забезпечення точності часових вимірювань, оскільки навіть мілісекундні відхилення можуть суттєво впливати на якість біометричних шаблонів [4].

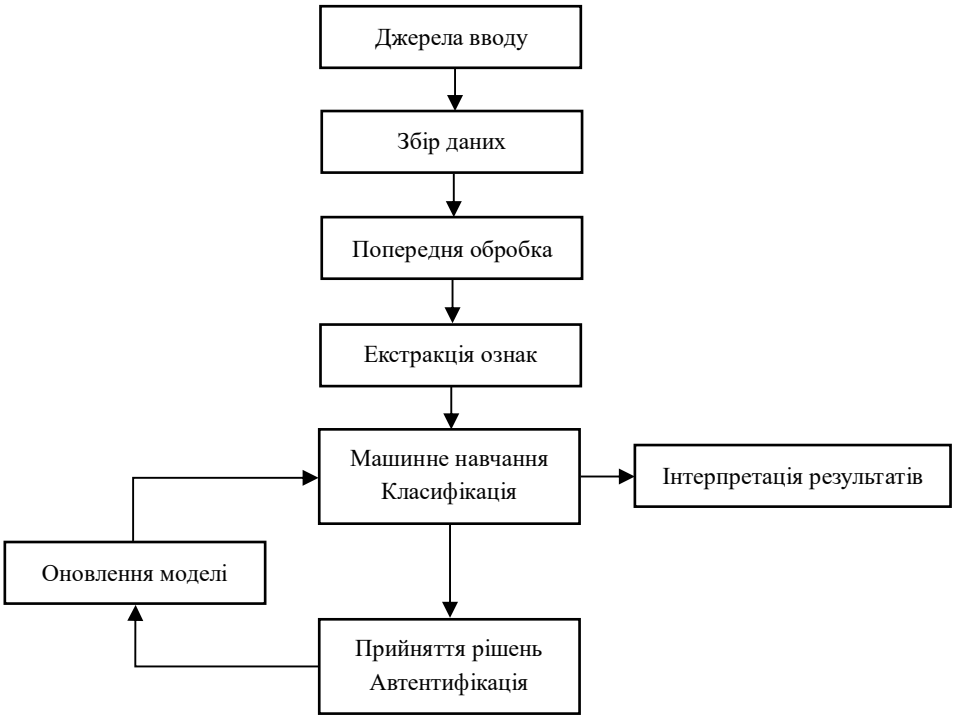


Рис. 1. Узагальнена архітектура систем аналізу клавіатурного почерку

Модуль попередньої обробки відповідає за нормалізацію часових вимірювань між різними системами, детекцію та обробку аномальних подій клавіатури, сегментацію безперервного набору на значущі фрагменти для аналізу, та оцінку якості зібраних даних. Критично важливим є врахування різних типів клавіатур, операційних систем та конфігурацій, які можуть впливати на темпоральні характеристики набору. Алгоритми нормалізації повинні компенсувати апаратні затримки та системні особливості для забезпечення кросплатформенної сумісності.

Механізм екстракції ознак включає генерацію користувацьких біометричних шаблонів, конструювання багатовимірних векторів ознак, застосування методів зменшення розмірності (PCA, LDA) та селекцію найбільш дискримінативних характеристик. Сучасні підходи використовують як традиційні статистичні методи, так і глибокі нейронні мережі для автоматичного виявлення латентних патернів у клавіатурних даних. Особливого значення набуває здатність системи адаптуватися до еволюції поведінкових патернів користувача протягом часу [5].

Система класифікації та співставлення реалізує різноманітні алгоритми машинного навчання, включаючи статистичні методи (гаусівські моделі сумішей, байєсівські класифікатори), методи на основі відстаней (евклідова, манхеттенська, махаланобіс), класичні алгоритми машинного навчання (SVM, Random Forest, Neural Networks) та сучасні архітектури глибокого навчання (LSTM, CNN, Transformer). Кожен з цих підходів має специфічні переваги та обмеження, що робить важливим вибір оптимального методу для конкретного застосування.

Модуль прийняття рішень забезпечує динамічне управління порогами прийняття/відхилення, ймовірнісні рішення автентифікації на основі показників довіри, безперервну автентифікацію під час активного набору тексту та механізми адаптивного навчання для оновлення профілів користувачів. Особливої уваги потребує баланс між безпекою та зручністю використання, що досягається через інтелектуальне налаштування порогів на основі контексту та ризик-профілю конкретного користувача [6].

Методи штучного інтелекту в аналізі клавіатурного почерку. Інтеграція методів штучного інтелекту в системи аналізу клавіатурного почерку призвела до суттєвого покращення точності автентифікації та розширення можливостей інтерпретації

результатів. Контрольовані методи машинного навчання включають метод опорних векторів (SVM), який демонструє конкурентоспроможну продуктивність з мінімальною кількістю навчальних зразків (до 5 зразків на користувача) та показниками Equal Error Rate (EER) від 4.5% до 10.2%. Гаусівські моделі сумішей (GMM) ефективно обробляють негаусівські розподіли клавіатурних даних, особливо в конфігураціях GMM-UBM (Universal Background Model) [7].

Дерева рішень та Random Forest популярні завдяки їх інтерпретованості, непараметричній природі та толерантності до викидів. Методи на основі відстаней, такі як манхеттенська відстань, найближчі сусіди та підрахунок викидів (z-score), ідентифіковані як найефективніші детектори для виявлення зловмисників. Алгоритм k-найближчих сусідів (KNN) використовується як у контрольованому, так і неконтрольованому режимах для класифікації та детекції аномалій.

Неконтрольовані методи навчання включають алгоритми кластеризації, такі як k-means для групування користувачів та ідентифікації поведінкових патернів, k-medoids та нечіткий c-means для обробки неевклідових метрик та перекриваючих кластерних призначень. Ієрархічна кластеризація дозволяє виявляти групи користувачів зі схожими патернами набору без попередньо визначеної кількості кластерів. One-class SVM спеціально використовується для детекції викидів у клавіатурній динаміці, коли недоступні мічені дані зловмисників.

Архітектури глибокого навчання демонструють революційні результати в аналізі клавіатурного почерку. Рекурентні нейронні мережі, зокрема LSTM (Long Short-Term Memory), показують видатні результати: архітектура TypeNet досягає EER 2.2% для фізичних клавіатур та 9.2% для сенсорних екранів. Двонаправлені LSTM використовуються для захоплення як прямих, так і зворотних темпоральних залежностей у послідовностях клавіатурного вводу. GRU (Gated Recurrent Units) пропонують альтернативу LSTM з меншою кількістю параметрів, забезпечуючи швидше навчання при збереженні порівнянної продуктивності [8].

Згорткові нейронні мережі (CNN) застосовуються для аналізу клавіатурного почерку через перетворення темпоральних даних у зображеноподібні репрезентації, досягаючи EER до 4.5%. Одновимірні згортки застосовуються безпосередньо до темпоральних послідовностей клавіатурного вводу для екстракції ознак. Гібридні CNN-RNN архітектури поєднують згорткову екстракцію ознак з рекурентним моделюванням послідовностей.

Трансформерні архітектури представляють найновіші досягнення в галузі, включаючи TypeFormer як першу успішну адаптацію трансформерної архітектури для клавіатурної динаміки. Механізми self-attention дозволяють моделям фокусуватися на релевантних частинах послідовностей набору при прийнятті рішень про автентифікацію. Multi-head attention забезпечує паралельну обробку різних аспектів клавіатурних послідовностей, що веде до кращого розуміння довготривалих залежностей [9].

Ансамблеві методи та гібридні підходи демонструють синергетичні ефекти при поєднанні різних алгоритмів. Традиційні ансамблеві підходи включають Random Forest з бутстрап-семплуванням та ансамблі класифікаторів, що поєднують SVM, KNN та дерева рішень, досягаючи точності 95.65%. Буст-алгоритми, такі як AdaBoost та XGBoost, показують послідовне навчання з ваговою корекцією помилок та градієнтний бустинг з регуляризацією відповідно. Табл. 1 містить порівняльний аналіз описаних методів штучного інтелекту.

Інтерпретація результатів штучного інтелекту в клавіатурному почерку. Пояснювальний штучний інтелект (Explainable AI) набуває критичного значення для систем біометричної автентифікації, оскільки користувачі та організації потребують розуміння логіки прийняття рішень системою. Градієнт-базовані методи включають карти сальєнтності для виділення важливих клавіатурних характеристик при прийнятті рішень про автентифікацію, Grad-CAM (Class Activation Mapping), адаптований для

аналізу клавіатурних послідовностей, та інтегровані градієнти як методи атрибуції для розуміння рішень моделі [10].

Таблиця 1.

Порівняльний аналіз методів штучного інтелекту для аналізу клавіатурного почерку

Метод	EER, %	Переваги	Недоліки	Область застосування
SVM	4.5-10.2	Мінімальна кількість навчальних зразків, стійкість до перенавчання	Чутливість до вибору ядра, складність інтерпретації	Статична автентифікація
Random Forest	5.0-8.5	Висока інтерпретованість, стійкість до викидів	Схильність до перенавчання на зашумлених даних	Аналіз важливості ознак
GMM	6.0-12.0	Ефективна обробка негаусівських розподілів	Чутливість до ініціалізації параметрів	Моделювання користувацьких профілів
LSTM	2.2-9.2	Захоплення довготривалих залежностей, адаптивність	Висока обчислювальна складність	Безперервна автентифікація
CNN	4.5-7.0	Автоматична екстракція ознак, стійкість до шуму	Втрата темпоральної інформації	Аналіз патернів набору
Transformer	1.8-5.5	Паралельна обробка, механізм уваги	Вимоги до великих наборів даних	Складні темпоральні залежності
Ансамблеві методи	3.0-6.0	Підвищена точність, стійкість	Збільшена обчислювальна складність	Критичні системи

Модель-агностичні методи включають LIME (Local Interpretable Model-agnostic Explanations) для локальних пояснень рішень щодо клавіатурних патернів, SHAP (SHapley Additive ExPlanations) для важливості ознак у патернах набору, та пермутаційну важливість для розуміння внеску ознак через контрольовані збурення. Ці методи дозволяють аналізувати, які саме аспекти клавіатурного почерку найбільше впливають на рішення про автентифікацію.

Візуалізація уваги стає особливо важливою для трансформерних архітектур, де теплові карти уваги показують, які частини клавіатурних послідовностей отримують найвищу увагу. Аналіз голів дозволяє зрозуміти патерни фокусування різних голів уваги, а темпоральні патерни уваги аналізують, як моделі зважують різні часові сегменти набору тексту.

Упередженість та етичні аспекти потребують систематичного аналізу. Метрики справедливості, такі як Skewed Impostor Ratio (SIR), використовуються для оцінки міжгруповой та внутрішньогрупової упередженості. Демографічний аналіз показує вплив статі, віку та домінуючої руки на клавіатурну автентифікацію. Мовно-специфічна упередженість виявляється при аналізі багатомовних клавіатурних патернів, де перехід між мовами може суттєво знижувати точність автентифікації [11].

Практичні виклики інтерпретації включають проблему "чорної скриньки" глибоких моделей навчання, особливо LSTM та CNN архітектур, які часто не мають інтерпретованості. Існує компроміс між продуктивністю моделі та її поясненістю, що потребує застосування post-hoc методів пояснення. Доменно-специфічні вимоги включають пояснення невдач автентифікації без розкриття вразливостей безпеки, надання зрозумілого зворотного зв'язку користувачам щодо змін у поведінці набору, та дотримання регуляторних вимог щодо поясненості біометричних систем.

Сучасні застосування та реалізації систем клавіатурного почерку. Комерційні та корпоративні системи автентифікації демонструють зрілість технології клавіатурного почерку та її готовність до широкого впровадження. Plurilock Security Inc. є провідним

комерційним постачальником з контрактами від Міністерства оборони США, здатним ідентифікувати користувачів протягом 3 секунд та 12 натискань клавіш. Компанія забезпечила контракти на $1.3 мільйона у 2025 році серед американських комерційних клієнтів, надаючи безперервну автентифікацію через поведінкові біометрики та машинне навчання з реальними впровадженнями в лікарняних системах та корпоративних клієнтах [12].

BehavioSec, придбана LexisNexis у 2022 році, зосереджується на поведінкових біометриках для виявлення шахрайства та запобігання захопленню облікових записів, маючи сильні позиції в європейському банківському секторі з впровадженням серед мільйонів користувачів банківських додатків. TypingDNA пропонує API для біометрики набору тексту для розробників, партнерства з рішеннями управління ідентичністю для інтеграції MFA, фокусуючись на електронному навчанні та запобіганні шахрайству.

Інтеграція з багатофакторною автентифікацією демонструє суттєві переваги зменшення тертя, знижуючи вимоги OTP на 66.3% при вході та 85.8% при відновленні облікового запису, зменшуючи час автентифікації на 63.3% для входу та 78.9% для відновлення облікового запису. Користувачі віддають перевагу клавіатурній динаміці + OTP над автентифікацією лише OTP. Ризик-орієнтована автентифікація функціонує як адаптивний рівень автентифікації, підвищуючи показники ризику при відхиленні патернів набору від базової лінії та запускаючи додаткову автентифікацію при перевищенні порогів ризику [13].

Реальні сценарії впровадження охоплюють фінансові послуги для виявлення шахрайства під час процесів входу та транзакцій, запобігання захопленню облікових записів, дотримання вимог сильної автентифікації клієнтів та підвищення безпеки онлайн-банкінгу. У сфері охорони здоров'я системи використовуються для багатофакторної автентифікації в системах DHIMS 2, безперервної автентифікації медичних працівників, поєднання з біометрикою відбитків пальців для підвищеної безпеки та дотримання вимог HIPAA.

Урядові та оборонні застосування включають впровадження Міністерства оборони США, захист критичної інфраструктури, виявлення та пом'якшення внутрішніх загроз, безперервний моніторинг доступу привілейованих користувачів. В освітній сфері системи застосовуються для верифікації особи студентів на онлайн-іспитах, забезпечення академічної чесності, запобігання шахрайству в середовищах дистанційного навчання та приватної автентифікації для освітніх платформ [14].

Показники продуктивності комерційних систем як-от BehavioSec заявляють EER 0.10-0.20, інші системи повідомляють про показники точності близько 88%. Найкращі системи досягають точності понад 95% для ідентифікації користувачів, а моделі глибокого навчання показують до 82% точності для завдань ідентифікації. Фактори продуктивності включають статичну автентифікацію, придатну для верифікації входу, динамічну автентифікацію, кращу для безперервного моніторингу, мультимодальні підходи з вищою точністю при поєднанні з іншими біометриками, та якість набору даних, де продуктивність значно варіюється залежно від методів збору даних.

Майбутні напрямки досліджень. Інтеграція гіроскопів та акселерометрів з аналізом клавіатурного почерку представляє революційний напрямок розвитку мобільних біометричних систем. Останні дослідження 2025 року демонструють, що системи клавіатурної динаміки на основі сенсорів смартфонів можуть досягати EER до 6.4% при поєднанні даних акселерометра та гіроскопа з патернами клавіатурного вводу. Інтеграція даних датчиків руху знижує помилки автентифікації приблизно на 1-2% порівняно з підходами лише на основі клавіш [15].

Рух пристрою під час набору може створювати унікальні "підписи руху", які доповнюють класичні патерни клавіатурного вводу. LSTM-базовані підходи, що поєднують дані акселерометра та гіроскопа, виявляють особливий інтерес для дослідження.

Аналіз поведінки набору на сенсорному екрані порівняно з традиційною клавіатурною динамікою виявляє фундаментальні відмінності. Фізичні відмінності включають нижчі сили набору на віртуальних клавіатурах, знижену продуктивність набору порівняно з фізичними клавіатурами, вищий суб'єктивний дискомфорт у областях рук/зап'ясть та шия/плечі, різні патерни активації м'язів у згиначах та розгиначах пальців.

Аналіз орієнтації мобільного пристрою та патернів руху включає багатопозиційні моделі автентифікації, які враховують набір у сидячому положенні (найстабільніші патерни), набір під час ходьби/мобільний набір (підвищена варіабельність, що потребує адаптивних порогів) та набір у розслабленому положенні (проміжні характеристики стабільності).

Виклики збору та аналізу мобільної клавіатурної динаміки включають обмеження збору даних з обмеженнями ОС Android щодо збору фонових даних без власних реалізацій, вимоги до користувацьких клавіатур з обмеженнями доступу третіх сторін, що потребують спеціалізованих методів вводу, проблеми приватності користувачів з балансуванням безпеки з вимогами захисту даних, варіацією між пристроями з різними виробниками та розмірами екранів, що впливають на стабільність патернів. Технічні виклики охоплюють обмежені обчислювальні ресурси на мобільних платформах, оптимізацію використання батареї для безперервного моніторингу, варіації мережевого підключення, що впливають на хмарну обробку, гетерогенність апаратного забезпечення між виробниками та моделями пристроїв [16].

Виклики та перспективи розвитку. Сучасні системи аналізу клавіатурного почерку стикаються з рядом технічних та концептуальних викликів, які визначають напрямки майбутніх досліджень. Поведінкова варіабельність залишається фундаментальною проблемою, оскільки патерни набору тексту піддаються впливу втоми, настрою, фізичних станів, емоційного стану та навчальних ефектів. Ефект адаптації користувача протягом часу потребує постійного оновлення моделей, що створює компроміс між стабільністю системи та здатністю до адаптації. Залежність від пристрою проявляється у варіаціях продуктивності між різними клавіатурами, пристроями та операційними системами, що ускладнює створення універсальних біометричних профілів.

Питання масштабованості стають критичними при впровадженні систем у великих організаціях, де деградація продуктивності з ростом кількості користувачів потребує ефективних алгоритмічних рішень та оптимізації інфраструктури. Вразливості безпеки включають потенціал для replay-атак, загрози кейлогерів у скомпрометованих середовищах, потенційну витоку поведінкових даних та необхідність детекції "живості" для забезпечення людського оператора замість автоматизованого вводу [17].

Етичні та регуляторні аспекти набувають зростаючого значення з розвитком законодавства про захист персональних даних. Дотримання GDPR вимагає мінімізації даних, прозорості та права на видалення, що може конфліктувати з потребами накопичення даних для покращення точності моделей. Потенційна упередженість проти користувачів з інвалідністю потребує інклюзивного дизайну систем, а прозоре розкриття моніторингу та справедливий дизайн системи є обов'язковими для етичного впровадження.

Розширення Інтернету речей передбачає кросплатформну автентифікацію з синхронізацією клавіатурних патернів між множинними пристроями, інтеграцію розумного дому з клавіатурною поведінкою як частиною ширших поведінкових профілів, злиття з пристроями що носяться з інтеграцією даних смарт-годинників та фітнес-трекерів.

Особливо перспективний напрямок для систем клавіатурного почерку представляють федеративне навчання [18] та граничні обчислення, дозволяючи навчання моделей без централізованого збору чутливих біометричних даних.

Висновки. Системи аналізу клавіатурного почерку для автентифікації користувачів пройшли шлях від експериментальних досліджень до зрілих комерційних рішень, які

демонструють високу ефективність у реальних умовах впровадження. Інтеграція методів штучного інтелекту, зокрема глибокого навчання та трансформерних архітектур, суттєво покращила точність автентифікації, з сучасними системами, що досягають EER нижче 5% в оптимальних умовах. Особливого значення набуває здатність до безперервної автентифікації та інтеграції з багатофакторними системами безпеки. Викликає інтерес інтеграція сенсорів мобільних пристроїв, зокрема гіроскопів та акселерометрів для підвищення точності мультимодальних біометричних систем. Методи інтерпретації результатів штучного інтелекту стають критично важливими для забезпечення довіри користувачів та дотримання регуляторних вимог. Розвиток пояснювального ШІ дозволяє створювати прозорі та зрозумілі системи автентифікації, що особливо важливо для критичних застосувань у фінансовій, медичній та урядовій сферах. Майбутні дослідження фокусуються на подоланні існуючих викликів варіабельності поведінки, кросплатформної сумісності та масштабованості через розвиток адаптивних алгоритмів та федеративного навчання. Успіх технології клавіатурного почерку визначається балансом між безпекою, зручністю використання та приватністю, що досягається через інтелектуальне поєднання традиційних статистичних методів з сучасними архітектурами штучного інтелекту та всеосяжним підходом до інтерпретації результатів аналізу.

Список літератури

1. Al-Khafajiy M., et al. Biometric-Based Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services. *Applied Sciences*. 2021. Vol. 11, № 4. Article 1642. DOI: https://doi.org/10.3390/app11041642
2. BIOSIG 2022 Conference Proceedings: 21st International Conference of the Biometrics Special Interest Group. Darmstadt, Germany, September 14-16, 2022. IEEE, 2022. DOI: https://doi.org/10.1109/BIOSIG55365.2022
3. BIOSIG 2023 Conference Proceedings: 22nd International Conference of the Biometrics Special Interest Group. Darmstadt, Germany, September 20-22, 2023. LNI P-339. IEEE, 2023. DOI: https://doi.org/10.1109/BIOSIG58226.2023
4. Buriro A., Luccio F. Mobile Biometrics: Innovations, Challenges, and Emerging Trends. *Advanced Information Networking and Applications*. AINA 2025. Lecture Notes on Data Engineering and Communications Technologies. 2025. Vol. 252. DOI: https://doi.org/10.1007/978-3-031-57916-5
5. A. Rahman et al., Multimodal EEG and Keystroke Dynamics Based Biometric System Using Machine Learning Algorithms. *IEEE Access*. 2021. Vol. 9, P. 94625-94643, https://doi.org/10.1109/ACCESS.2021.3092840
6. Korchenko O., Tereikovskyi I., Ziubina R., Tereikovska L., Korystin O., Tereikovskyi O., Karpinskyi V. Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images. *Applied Sciences*. 2025. Vol. 15, № 5. Article 2553. DOI: https://doi.org/10.3390/app15052553
7. Mhenni A., Cherrier E., Rosenberger C., Essoukri Ben Amara N. Double serial adaptation mechanism for keystroke dynamics authentication based on a single password. *Computers & Security*. 2019. Vol. 83. P. 151–166. DOI: https://doi.org/10.1016/j.cose.2019.02.002
8. Migdal D., Rosenberger C. Statistical modeling of keystroke dynamics samples for the generation of synthetic datasets. *Future Generation Computer Systems*. 2019. Vol. 100. P. 907–920. DOI: https://doi.org/10.1016/j.future.2019.04.045
9. Monrose F., Rubin A. D. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*. 2000. Vol. 16, № 4. P. 351–359. DOI: https://doi.org/10.1016/S0167-739X(99)00059-X
10. Muratuly D., Denissova N., Krak Y., Apayev K. Biometric Authentication of Students to Control the Learning Process in Online Education. *Scientific Journal of Astana IT University*. 2022. Vol. 10, № 10. DOI: http://dx.doi.org/10.37943/LYFW8581

11. Pisani P. H., Lorena A. C. A systematic review on keystroke dynamics. *Journal of the Brazilian Computer Society*. 2013. Vol. 19, № 4. P. 573–587. DOI: https://doi.org/10.1007/s13173-013-0117-7
12. Rahman A., et al. Multimodal EEG and keystroke dynamics based biometric system using machine learning algorithms. *IEEE Access*. 2021. Vol. 9. P. 94625-94643. DOI: https://doi.org/10.1109/ACCESS.2021.3092840
13. Rahmani K., Babaie S. A. A lightweight biometric-assisted authentication approach for internet of things. *Peer-to-Peer Networking and Applications*. 2025. Vol. 18. Article 195. DOI: https://doi.org/10.1007/s12083-025-02006-8.
14. Roy S., Roy U., Sinha D. D. Systematic Literature Review on Latest Keystroke Dynamics Based Models. *IEEE Access*. 2022. Vol. 10. P. 93569–93599. DOI: https://doi.org/10.1109/ACCESS.2022.3197756
15. Sulavko A., Panfilova I., Inivatov D., Lozhnikov P., Vulfin A., Samotuga A. Biometric-Based Key Generation and User Authentication Using Voice Password Images and Neural Fuzzy Extractor. *Applied System Innovation*. 2025. Vol. 8, № 1. Article 13. DOI: https://doi.org/10.3390/asi8010013
16. Teh P. S., Teoh A. B. J., Yue S. A survey of keystroke dynamics biometrics. *The Scientific World Journal*. 2013. Article ID 408280. 24 p. DOI: https://doi.org/10.1155/2013/408280
17. Tereikovskyi I., Tereikovska L., Korystin O., Mussiraliyeva S., Sambetbayeva A. User Keystroke Authentication and Recognition of Emotions Based on Convolutional Neural Network. *Advances in Artificial Systems for Medicine and Education III*. AIMEE 2019. Advances in Intelligent Systems and Computing. 2020. Vol. 1126. P. 26–35. DOI: https://doi.org/10.1007/978-3-030-39162-1_3
18. Євтушенко С.В. Про перспективи федеративного навчання для систем автентифікації на основі аналізу клавіатурного почерку. *LVIII Міжнародна науково-практична конференція "Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку"*, м. Ловеч (Болгарія). 2025. С. 173-177

С.В. Євтушенко

ASPECTS OF CONSTRUCTION AND APPLICATION OF KEYSTROKE DYNAMICS ANALYSIS SYSTEMS FOR USER AUTHENTICATION

S. V. Yevtushenko

National University "Odesa Law Academy"
2, Academic St., Odesa, 65000, Ukraine
Email: serhiyevtushenko@gmail.com

The subject of the article is keystroke dynamics analysis systems for user authentication using artificial intelligence methods and their integration with mobile device sensors. The purpose of the work is to analyze aspects of building and applying keystroke dynamics analysis systems for user authentication using artificial intelligence methods and to study the prospects for their development for creating multimodal biometric systems. The article solves the following tasks: forming a model of the architecture of multilevel keystroke dynamics systems; systematizing artificial intelligence methods for analyzing temporal patterns of text typing; analyzing approaches to integrating gyroscopes and accelerometers of mobile devices to create multimodal biometric systems; studying methods for interpreting the results of deep learning models in the context of biometric authentication. The following methods are used: mathematical processing of temporal sequences of keyboard input; deep learning with LSTM, CNN, and Transformer architectures; statistical analysis of behavioral patterns; machine learning with supervised and unsupervised algorithms; ensemble approaches to improve classification accuracy. The following results were obtained: the principles of building a multi-level architecture of keystroke dynamics systems were formulated; artificial intelligence methods for analyzing biometric characteristics of typing were systematized; modern commercial implementations with EER indicators of 0.10-0.20% for leading systems were analyzed; the prospects for integrating mobile device sensors to achieve EER up to 6.4% in multimodal systems were investigated. Conclusions: the use of the method of combining keystroke dynamics with gyroscope and accelerometer data allows creating high-precision continuous authentication systems with increased resistance to imitation attacks and the ability to adapt to the evolution of user behavioral patterns.

Keywords: keystroke dynamics; biometric authentication; artificial intelligence; deep learning; multimodal systems.

DOI 10.15276/imms.v15.no3.377
УДК 004.056.53:162.5:159.955

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 377-385

МОДЕЛЮВАННЯ ДИНАМІКИ ЛОГІЧНИХ ПАТЕРНІВ КІБЕРЗЛОЧИНЦІВ

О.Я. Ковальчук[1], Р.І. Іваницький[2], Л.В. Бабала[1]

[1]Західноукраїнський національний університет
11, Львівська, Тернопіль, 46009, Україна
[2]Тернопільський національний педагогічний університет імені Володимира Гнатюка
2, М. Кривоноса, Тернопіль, 46027, Україна
Emails: olhakov@gmail.com, romikiv@ukr.net, ludaduma7@gmail.com

У роботі досліджено вплив когнітивних упереджень на поведінку кіберзлочинців у контексті розширених постійних загроз. Проаналізовано чотири ключові когнітивні упередження: нехтування базовою частотою, упередження підтвердження, аверсію до втрат та помилку невідшкодованих витрат. Встановлено, що нехтування базовою частотою призводить до переоціювання значущості окремих індикаторів цілей; упередження підтвердження спонукає до селективного аналізу інформації; аверсія до втрат визначає вибір між агресивними та прихованими методами кібератак; помилка невідшкодованих витрат зумовлює прив'язаність до субоптимальних злочинних стратегій. Розроблено математичний апарат для формалізації когнітивних упереджень через параметричні моделі з відповідними коефіцієнтами для упередження підтвердження, аверсії до втрат та невідшкодованих витрат. Запропоновано адаптивну когнітивно-темпоральну модель (АКТМ), що інтегрує множинні упередження у єдину динамічну систему з механізмами навчання та адаптації. Модель враховує темпоральну еволюцію когнітивного профілю кіберзлочинців та забезпечує адаптивний перерозподіл уваги між упередженнями залежно від конкретних умов кібератаки. Визначено практичні застосування моделі для розробки персоналізованих систем виявлення загроз, оптимізації стратегій активної оборони та створення адаптивних пасток-систем для хибного націлювання зловмисників. Обґрунтовано можливість використання когнітивних упереджень для підвищення ефективності захисних механізмів через провокування прогнозованих помилок у рішеннях кіберзлочинців.

Ключові слова: математичне моделювання, логічні патерни, когнітивний профіль, кібербезпека, розширені постійні загрози, прийняття рішень, кіберзлочинність.

Вступ. Феномен розширених постійних загроз (Advanced Persistent Threats, APT) – складних, довготривалих та цілеспрямованих атак на інформаційні системи (ІС) належить до найбільш небезпечних проявів сучасної кіберзлочинності. Його специфіка полягає у поєднанні високотехнологічних засобів атаки з тривалим і прихованим проникненням до ІС. Середній час перебування APT у мережі без виявлення може сягати понад пів року, що створює передумови для масштабних втрат і стратегічних загроз [1]. На відміну від класичних кіберінцидентів, APT не мають на меті швидке завдання шкоди. Їхня мета – систематичне накопичення даних, контроль за інформаційними потоками та вплив на критично важливі ресурси.

APT здатні змінювати баланс сил на геополітичному та економічному рівнях. Так, у 2010 році атака Stuxnet вперше продемонструвала можливість фізичного знищення промислового обладнання шляхом маніпуляцій програмним забезпеченням систем управління технологічними процесами [2]. Операція Aurora, спрямована проти корпорацій Google та Adobe, виявила масштаби державного кібершпигунства та необхідність переосмислення підходів до інформаційної безпеки [3]. Північнокорейське угруповання APT38 у 2015–2016 рр. здійснило серію атак через мережу SWIFT, викравши сотні мільйонів доларів, що продемонструвало новий рівень фінансово мотивованого кіберзлочину [4]. Особливу складність становить те, що APT поєднують технічні та когнітивні компоненти. Технічний рівень виявляється у використанні zero-day вразливостей, кастомізованого шкідливого програмного забезпечення та методів

приховування слідів [5]. Когнітивний рівень полягає у застосуванні соціальної інженерії, маніпуляції інформаційними потоками та використанні людських вразливостей. Саме цей симбіоз зумовлює ефективність APT і робить їх об'єктом міждисциплінарних досліджень. Когнітивне моделювання може стати дієвим інструментом у вивченні APT та забезпечити можливість аналізувати динаміку взаємодії між технічними та людськими факторами, будувати сценарії розвитку атак і прогнозувати поведінку як зловмисників, так і потенційних жертв. Так нещодавні дослідження у сфері агентного моделювання показують можливість відтворення APT-кампаній з урахуванням когнітивних упереджень користувачів, що значно підвищує точність прогнозу щодо їхнього впливу на систему [6]. Когнітивне моделювання відкриває перспективи формування нових підходів до забезпечення кібербезпеки, де ключову роль відіграє розуміння не лише технічних вразливостей, а й людського фактору.

Це дослідження продовжує цикл робіт з питань розробки інноваційних підходів до запобігання, виявлення та мінімізації наслідків кібератак [7–9].

Мета роботи. Метою даної роботи є розробка адаптивної когнітивно-темпоральної моделі логічних патернів кіберзлочинців у контексті APT на основі математичної формалізації когнітивних упереджень для підвищення ефективності прогнозування тактик атак та оптимізації захисних стратегій.

Для досягнення мети дослідження поставлено та вирішено такі завдання:

- ідентифікувати та формалізувати ключові когнітивні упередження (логічні патерни), що впливають на процеси прийняття рішень операторами APT під час довготривалих кібератак;
- розробити математичний апарат для моделювання нехтування базовою частотою, упередження підтвердження, аверсії до втрат та помилки невідшкодованих витрат у контексті кібероперацій;
- створити адаптивну когнітивно-темпоральну модель, що інтегрує множинні упередження у єдину динамічну систему з механізмами навчання та адаптації;
- обґрунтувати механізми темпоральної еволюції когнітивного профілю зловмисників під впливом зовнішніх умов і накопиченого досвіду;

Когнітивні упередження в APT: ризики ігнорування статистичної поширеності в кібероперації. Нехтування базовою частотою (base rate neglect) є загальновідомим когнітивним упередженням, яке полягає у схильності людини недооцінювати або повністю ігнорувати статистичну поширеність (базову частоту) події при оцінюванні її ймовірності у конкретній ситуації [11]. Люди схильні надавати перевагу специфічній інформації про частковий випадок, нехтуючи при цьому загальною статистичною інформацією [12]. У контексті кібербезпеки, зокрема при аналізі поведінки операторів APT, це упередження може суттєво впливати на процеси прийняття рішень під час проведення атак. Професіонали з безпеки є настільки ж вразливими до когнітивних упереджень, як і пересічні люди, внаслідок чого їхні рішення можуть виявитися менш оптимальними, ефективними або результативними [13]. Враховуючи зростаючу складність цільових атак, інструменти виявлення APT швидко впроваджуються в індустрії кібербезпеки. За оцінками експертів, глобальні продажі рішень для захисту від APT зростуть з 6,9 мільярда доларів у 2022 році до приблизно 15,2 мільярда доларів до 2026 року [14], що підкреслює критичну важливість розуміння поведінкових аспектів таких атак.

При проведенні APT-атак оператори часто стикаються з необхідністю прийняття рішень щодо цільових файлів або облікових записів на основі неповної інформації. Нехтування базовою частотою може проявлятися у переоцінці значущості певних ключових слів або назв файлів, які здаються релевантними або цінними. Наприклад, якщо зловмисник зустрічає файл з назвою, що містить слова «конфіденційно» або «секретно», він може помилково припустити, що такі файли завжди містять цінну інформацію, ігноруючи при цьому статистичну ймовірність того, що більшість файлів з такими назвами можуть бути звичайними документами. Традиційні системи виявлення

вторгнень (Itrusion Detection Systems, IDS) страждають від низької точності виявлення, високого рівня помилкових спрацювань та складності ідентифікації невідомих атак [15], що робить розуміння когнітивних упереджень зловмисників потенційно корисним для розробки більш ефективних захисних механізмів.

Упередження підтвердження в операціях APT. Упередження підтвердження, що визначається як схильність обирати варіанти, які підтримують власні переконання з пулу інформації, впливає на більшість рішень злочинців, що скоюють APT [16]. Це когнітивне упередження проявляється у їхній поведінці через надмірну увагу до доказів, що підтверджують їхні первинні гіпотези, при одночасному ігноруванні суперечливих свідчень.

Когнітивні моделі можуть ефективно відображати поведінку кіберзлочинців з різними рівнями аверсії (негативної реакції на певний тригер) до втрат та упередження підтвердження, досягаючи точності класифікації принаймні 0,83 у прогнозуванні когнітивних вразливостей [17]. Коли оператор APT виявляє файл з обліковими даними сервера та формує гіпотезу про існування цільового сервера з важливими файлами, навіть після численних невдалих спроб автентифікації він може продовжувати дотримуватися початкової гіпотези, інтерпретуючи невдачі як тимчасові технічні проблеми, а не як спростування своїх припущень.

Математично це можна представити через параметр $\theta_c \in [0, 1]$, що позначає частоту виявлення підтверджуючих доказів серед усіх дій з перевірки файлів облікових даних. За умови $\theta_c >> 0{,}5$ можна стверджувати про наявність високого рівня упередження підтвердження у поведінці зловмисника [18].

Аверсія до втрат є когнітивною вразливістю, що призводить до негативної емоційної реакції на втрати, навіть у тому разі, коли переваги переважають над ризиками [19]. Кіберзлочинці, схильні до уникнення втрат, віддають перевагу малоризиковим методам збору даних. На початковому етапі ідентифікації сервісів вони обмежуються скануванням найбільш поширених портів, відкладаючи перевірку інших на пізніші етапи та здійснюючи її приховано. Подібна тактика імітує звичайну мережеву активність, що знижує ймовірність виявлення з боку правоохоронних органів.

Відповідно до теорії перспектив, асиметричне сприйняття зловмисниками втрат або здобутків $\omega \in R$ може бути представлене функцією суб'єктивної корисності $u(\omega, \lambda_l)$, в якій λ_l R+ позначає коефіцієнт, що контролює аверсію до втрат [20].

У процесі виявлення сервісів аверсію до втрат можна представити рівностями (1)–(2):

$$\Psi(\alpha, \beta, \lambda_l) = \frac{1}{1 + e^{-\tau(\upsilon(\alpha,\lambda_l) - \upsilon(\beta,\lambda_l))}}, \quad (1)$$

$$\upsilon(\omega, \lambda_l) = \begin{cases} \omega^{\delta} & \text{якщо } \omega \geq 0 \\ -\lambda_l(-\omega)^{\delta} & \text{якщо } \omega < 0 \end{cases}, \quad (2)$$

де параметри $\alpha \in R$ та $\beta \in R$ представляють оцінені втрати або виграші агресивного виявлення сервісів та прихованого виявлення сервісів відповідно.

Агресивне виявлення сервісів (α):

- виграші: швидке отримання повної інформації про відкриті порти та сервіси; економія часу; можливість швидко перейти до наступного етапу атаки;
- втрати: високий ризик виявлення системами захисту; можливе блокування IP-адреси; втрата стелс-режиму; ризик припинення всієї операції.

Приховане виявлення сервісів (β):

- виграші: низький ризик виявлення; збереження анонімності; можливість тривалої присутності в мережі без підозр

– втрати: значно більше часу на збір інформації; неповні дані про цілі; можливість втратити вікно можливостей; ризик того, що вразливості будуть виправлені до завершення сканування.

$\Psi(\alpha, \beta, \lambda_l) \in [0, 1]$ – це ймовірність застосування агресивного виявлення сервісів. Якщо $\alpha > \beta$ (виграші агресивного підходу перевищують приховані), то $\Psi(\alpha, \beta, \lambda_l) \to 1$ (висока ймовірність агресивної поведінки). Якщо $\alpha < \beta$ (втрати агресивного підходу занадто великі), то $\Psi(\alpha, \beta, \lambda_l) \to 0$ (перевага прихованому підходу).

Параметр λ_l посилює негативне сприйняття втрат: чим більше λ_l, тим більше зловмисник уникає агресивних дій навіть при потенційно високих виграшах. Це дозволяє моделювати різні типи зловмисників: від обережних (високе λ_l) до ризикових (низьке λ_l). $\delta \in \mathrm{R}$ представляє параметр, що контролює кривизну $\upsilon(\omega, \lambda_l)$.

$\tau \in \mathrm{R}$ визначає, наскільки «стабільним» або «непередбачуваним» є кіберзлочинець у своїх рішеннях; наскільки «рішуче» він приймає рішення між агресивним та прихованим скануванням.

Високе τ (висока чутливість):

– кіберзлочинець приймає чіткі, категоричні рішення;
– навіть невелика різниця між $\upsilon(\alpha, \lambda_l)$ та $\upsilon(\beta, \lambda_l)$ призводить до однозначного вибору;
– Ψ швидко наближається до 0 або 1;
– поведінка зловмисника «або повністю агресивно, або повністю приховано».

Низьке τ (низька чутливість):

– кіберзлочинець приймає більш різноманітні «розмиті» рішення;
– навіть значна різниця між варіантами може призвести до проміжних значень Ψ;
– більше невизначеності в поведінці зловмисника;
– поведінка: змішаний підхід, часткове сканування.

Помилка невідшкодованих витрат у виборі цілей розширеними стійкими загрозами. Ще однією важливою когнітивною упередженістю, що впливає на прийняття рішень кіберзлочинцями, є помилка невідшкодованих витрат (sunk cost fallacy). Цей психологічний феномен характеризує схильність до прийняття субоптимальних рішень на основі раніше витрачених ресурсів, а не майбутніх очікуваних прибутків [21]. У сенсі APT злочинці, які припускаються помилки невідшкодованих витрат, виявляють виражену схильність до продовження дій, які вже поглинули значні часові та обчислювальні ресурси, незалежно від їх поточної життєздатності чи стратегічної цінності.

Для формалізації цієї поведінкової моделі розглянемо ландшафт загроз, що складається з Ω доступних цілей, де кожна ціль $\mu \in \Omega = \{1, ..., \Omega\}$ представляє потенційну можливість досягнення. Сприйняту корисність цілі μ можна квантифікувати через функцію оцінювання $V(\mu) : \Omega \to \mathrm{R}$.

інійна модель корисності може бути представлена рівністю (3):

$$V(\mu) = \rho(\mu) + \mu_s k(\mu), \tag{3}$$

де $\rho(\mu) : \Omega \to \mathrm{R}$ – функція винагороди, що квантифікує очікувану користь від розподілу ресурсів на ціль μ; $k(\mu) : \Omega \to \mathrm{R}$ позначає кумулятивну функцію невідшкодованих витрат, що представляє ресурси, раніше витрачені на μ. Параметр $\mu_s \in \mathrm{R}_+$ служить масштабуючим коефіцієнтом, який регулює величину впливу невідшкодованих витрат на процеси прийняття рішень.

Ймовірність вибору цілі визначається шляхом застосування процедури softmax-нормалізації та описується рівністю (4):

$$p_s(\mu) = \frac{V(\mu)}{\sum_{j=1}^{\Omega} V(j)}, \tag{2}$$

де ймовірність вибору цілі μ пропорційна її сприйнятій корисності відносно сукупної корисності всіх доступних цілей.

Ця математична модель відображає основну характеристику помилки невідшкодованих витрат, що полягає у систематичному переоцінюванні кіберзлочинцями раніше використовуваних тактик, що потенційно призводить до тривалого залучення до скомпрометованих або субоптимальних векторів атак (методів реалізації кібератаки, що здатні дати результат, проте поступаються оптимальним за ефективністю досягнення цілей зловмисника) [22].

Адаптивна когнітивно-темпоральна модель динаміки логічних патернів кіберзлочинців. Аналіз окремих когнітивних упереджень, що впливають на поведінку операторів APT забезпечив можливість зробити висновок про необхідність розробки концептуальної комплексної моделі, яка б враховувала динамічну взаємодію різних психологічних факторів у часі та їх адаптивну зміну під впливом зовнішніх умов і накопиченого досвіду [17]. Традиційні підходи до моделювання поведінки кіберзлочинців розглядають когнітивні упередження як статичні характеристики [18, 23], що не відображає реальну динаміку довготривалих APT-кампаній, які можуть тривати місяцями або роками.

У цій роботі запропоновано інноваційну адаптивну когнітивно-темпоральну модель (АКТМ), що інтегрує множинні когнітивні упередження у єдину динамічну систему з механізмами навчання та адаптації. На відміну від статичних моделей, АКТМ моделює когнітивний профіль зловмисника як багатовимірний вектор упереджень, що еволюціонує протягом тривалої APT-кампанії під впливом результатів попередніх дій, зміни умов захищеності цільової мережі та накопичення операційного досвіду.

Математичний апарат моделі. Формально, когнітивний стан оператора APT у дискретний момент часу t можна представити у вигляді багатовимірного вектора

$$\Phi(t) = [\theta_c(t), \lambda_l(t), \mu_s(t), \xi_a(t)], \tag{5}$$

де $\theta_c(t) \in [0,1]$ – коефіцієнт упередження підтвердження в момент t;

$\lambda_l(t) \in R_+$ – параметр аверсії до втрат в момент t;

$\mu_s(t) \in R_+$ – коефіцієнт впливу невідшкодованих витрат в момент t;

$\xi_a(t) \in [0,1]$ – індекс адаптивної пам'яті (параметр, що характеризує здатність кіберзлочинця модифікувати свою поведінку на основі попереднього досвіду).

Параметр $\xi_a(t)$ відображає кумулятивний вплив попередніх результатів на поточні рішення та визначається рівністю (6):

$$\xi_a(t) = \frac{1}{t}\sum_{i=1}^{t} \gamma^{j-1} R_i, \tag{6}$$

де $\gamma \in (0,1)$ – коефіцієнт забування (discount factor), $R_i \in \{-1, 0, 1\}$ – результат дії в момент i (-1 – невдача, 0 – нейтральний результат, 1 – успіх).

Механізм темпоральної еволюції. Еволюція когнітивного профілю описується системою різницевих рівнянь (оскільки APT-операції відбуваються дискретними етапами):

$$\Phi(t+1) = \Phi(t) + \Delta t \cdot G(\Phi(t), E(t), H(t)) + \varepsilon(t), \tag{7}$$

де $G: R^4 \times R^n \times R^m \to R^4$ – функція когнітивного оновлення;

$E(t) \in R^n$ – вектор зовнішніх умов (рівень захищеності мережі, час до виявлення, доступність цілей);

$H(t) \in R^m$ – вектор накопиченої історії операцій (успіхи, невдачі, виявлення);

$\varepsilon(t) \sim N(0, \Sigma)$ – стохастичний шум з коваріаційною матрицею Σ;

Δt – дискретний крок часу.

Функція G моделюється рівністю (8):

$$G(\Phi(t), E(t), H(t)) = A \cdot \tanh(W_1\Phi(t) + W_2E(t) + W_3H(t) + b), \quad (8)$$

де A, W_1, W_2, W_3 – матриці параметрів, b – вектор зміщення, tanh (гіперболічний тангенс) забезпечує обмеженість змін.

Адаптивний механізм прийняття рішень. Для кожної потенційної цілі $\omega \in \Omega$ функція корисності в момент t визначається як зважена комбінація індивідуальних компонентів упереджень:

$$U(\omega, t) = w_1(t)\cdot U_c(\omega, t) + w_2(t)\cdot U_l(\omega, t) + w_3(t)\cdot U_s(\omega, t) + w_4(t)\cdot U_a(\omega, t), \quad (9)$$

де $U_c(\omega, t)$ – корисність з точки зору упередження підтвердження;

$U_l(\omega, t)$ – корисність з урахуванням аверсії до втрат;

$U_s(\omega, t)$ – корисність з врахуванням невідшкодованих витрат;

$U_a(\omega, t)$ – адаптивна компонента на основі накопиченого досвіду.

Ваги $w(t) = [w_1(t), w_2(t), w_3(t), w_4(t)]$ визначаються через контекстно-залежний механізм уваги

$$w(t) = \text{softmax}(\Phi(t) \odot C(t)), \quad (10)$$

де softmax – математична функція, яка перетворює вектор дійсних чисел у вектор ймовірностей, сума яких дорівнює 1; $C(t)$ контекстний вектор поточної ситуації, $\odot$ – операція Адамара (поелементний добуток).

Кожна компонента корисності адаптується до конкретного когнітивного упередження:

$$U_c(\omega, t) = \theta_c(t) \cdot \text{conf}(\omega, t) + (1 - \theta_c(t)) \cdot \text{obj}(\omega, t), \quad (11)$$

де conf(ω, t) – ступінь підтвердження попередніх гіпотез цілі ω, obj(ω,t) – об'єктивна цінність цілі.

$$U_l\upsilon(\omega, t) = \begin{cases} \rho(\omega) & \text{якщо } \rho(\omega) \geq 0 \\ -\lambda_l(t)|\rho(\omega)| & \text{якщо } \rho(\omega) < 0 \end{cases}, \quad (12)$$

де $\rho(\omega)$ – очікувана винагорода/втрата від цілі ω.

$$U_s(\omega, t) = \rho(\omega) + \mu_s(t) \cdot k(\omega, t), \quad (13)$$

де $k(\omega, t)$ – кумулятивні невідшкодовані витрати на ціль ω до моменту t.

Алгоритм оновлення параметрів. Модель включає механізм навчання через підкріплення для оновлення когнітивних параметрів:

$$\Phi(t + 1) = \Phi(t) + \eta \cdot \nabla\Phi\, J(\Phi(t)) \cdot \eta(R(t)), \quad (14)$$

де $\eta \in (0,1)$ – швидкість навчання;

J(Φ) – функція якості;

R(t) – вектор винагород за період [t, t+1];

$\eta(R) = \dfrac{1 - e^{-\beta|R|}}{1 + e^{-\beta|R|}}$ – функція чутливості до результатів з параметром $\beta > 0$.

Запропонована у цій роботі АКТМ представляє кілька ключових переваг порівняно з існуючими підходами до моделювання поведінки APT-операторів:

1. На відміну від статичних моделей, АКТМ враховує еволюцію когнітивних упереджень протягом тривалого періоду. Це критично важливо для APT, оскільки оператори можуть змінювати свою поведінку на основі попередніх успіхів, невдач або зміни умов захищеності цільової мережі.

2. Модель не розглядає упередження ізольовано, а моделює їх взаємодію через механізм контекстно-залежних ваг. Це відображає реальність прийняття рішень, де кілька психологічних факторів можуть одночасно впливати на вибір тактики.

3. АКТМ забезпечує можливість прогнозувати майбутню поведінку кіберзлочинців на основі їх когнітивного профілю та історії дій. Це може значно покращити ефективність проактивних захисних стратегій.

4. Параметри моделі можуть бути налаштовані для конкретних APT-груп на основі спостережуваних поведінкових патернів, що дозволяє створювати більш точні моделі загроз.

5. Розуміння когнітивних упереджень дає можливість розробляти захисні механізми, що експлуатують ці упередження. Наприклад, можна створювати

«приманки», що використовують упередження підтвердження для відволікання уваги зловмисників від справжніх цілей.

6. Модель може ідентифікувати моменти, коли когнітивний профіль зловмисника кардинально змінюється, що може сигналізувати про зміну фази атаки або появу нових учасників кібератаки.

Практичне застосування АКТМ потребує калібрування параметрів на основі емпіричних даних про поведінку конкретних APT-груп. Це може бути досягнуто через аналіз журналів безпеки, систем-пасток, які імітують вразливий комп'ютер або мережу для приваблення кіберзлочинців, та інших джерел інформації про тактики зловмисників. Валідація моделі може здійснюватися через порівняння прогнозованих поведінкових траєкторій з реальними спостереженнями використовуючи метрики когнітивної узгодженості.

Запропонована модель відкриває нові перспективи для розвитку адаптивних систем кібербезпеки, що здатні передбачати та протидіяти еволюції тактик APT-операторів через глибоке розуміння їх психологічних мотивацій та когнітивних обмежень.

Висновки. У роботі досліджено феномен когнітивних упереджень (логічних патернів) як критичного фактору формування поведінки кіберзлочинців у контексті APT. Встановлено, що нехтування базовою частотою призводить до переоцінення значущості окремих індикаторів цілей; упередження підтвердження спонукає до селективного аналізу інформації; аверсія до втрат визначає вибір між агресивними та прихованими методами проведення атак; помилка невідшкодованих витрат зумовлює прив'язаність до субоптимальних векторів атаки навіть за умов низької ефективності.

Розроблено математичний апарат для формалізації когнітивних упереджень через параметричні моделі, що дозволяє кількісно оцінювати їх вплив на процеси прийняття рішень зловмисниками. Запропоновано параметри θ_c для упередження підтвердження, λ_l для аверсії до втрат та μ_s для невідшкодованих витрат, які забезпечують можливість прогнозування вибору цілей і тактик кіберзлочинців на основі їх когнітивного профілю. Створено адаптивну когнітивно-темпоральну модель, що представляє принципово новий підхід до моделювання динамічної еволюції поведінки операторів APT. Модель інтегрує множинні когнітивні упередження через механізм softmax-нормалізації та забезпечує адаптивний перерозподіл уваги між різними психологічними факторами залежно від контексту операції. Доведено, що темпоральна компонента моделі дозволяє ідентифікувати критичні точки зміни поведінкових патернів на основі накопиченого досвіду успіхів і невдач зловмисників.

Визначено практичні застосування запропонованої моделі для розробки персоналізованих систем виявлення загроз, оптимізації стратегій активної оборони та створення адаптивних систем-пасток для імітації вразливого комп'ютера чи мережі для введення в оману кіберзлочинців. Обґрунтовано можливість експлуатації когнітивних упереджень для підвищення ефективності захисних механізмів шляхом створення умов, що провокують прогнозовані помилки в рішеннях кіберзлочинців. Міждисциплінарний підхід, який поєднує методи когнітивної психології, теорії ігор та машинного навчання, відкриває нові перспективи для вирішення актуальних проблем кібербезпеки в умовах зростаючої складності та тривалості сучасних кібератак. Результати дослідження створюють теоретичну основу для подальшого розвитку поведінково-орієнтованих систем кібербезпеки.

Список літератури

1. FireEye Mandiant Services. M-Trends. Advanced Persistent Threat Groups Special Report. 2020. URL: https://www.fireeye.com/current-threats/annual-threat-report/m-trends.html.
2. Farwell J.P., Rohozinski R. Stuxnet and the Future of Cyber War. *Survival*. 2011. Vol. 53(1). P. 23–40. DOI: https://doi.org/10.1080/00396338.2011.555586.

3. Nasir F., Sohail R. State, Surveillance, and Cyberspace: An Intelligence Analysis of Operation Aurora. *Social Science Review Archives*. 2025. Vol. 3(2). Article 1668–1675. DOI: https://doi.org/10.70670/sra.v3i2.789.
4. Lyngaas S. FireEye unmasks a new North Korean threat group. Cyberscoop. 2018. https://cyberscoop.com/apt38-north-korea-fire-eye/.
5. Sfetcu N. APT: Definition, History and Features. In book: Advanced Persistent Threats in Cybersecurity – Cyber Warfare. 2024. DOI: 10.58679/mm28378. https://www.telework.ro/en/e-books/advanced-persistent-threats-in-cybersecurity-cyber-warfare/.
6. Aggarwal P., Thakoor O., Jabbari S., Cranford E. A., Lebiere C., Tambe M., Gonzalez C. Designing effective masking strategies for cyberdefense through human experimentation and cognitive models. *Computers & Security*. 2022. Vol. 117. Article 102671. DOI: https://doi.org/10.1016/j.cose.2022.102671.
7. Kovalchuk O., Shevchuk R., Banakh S., Cryptocurrency Crime Risks Modeling: Environment, E-Commerce, and Cybersecurity Issue. *IEEE Accpess*. 2024. Vol. 12. P. 50673–50688. DOI: 10.1109/ACCESS.2024.3386428.
8. Kovalchuk O., Shynkaryk, Masonkova M. Econometric Models for Estimating the Financial Effect of Cybercrimes. *11th International Conference on Advanced Computer Information Technologies (ACIT)*, Deggendorf, Germany. 2021, P. 381–384. DOI: 10.1109/ACIT52158.2021.9548490.
9. Kovalchuk O., Shynkaryk M., Masonkova M., Banakh S. Cybercecurity: Technology vs Safety. *10th International Conference on Advanced Computer Information Technologies (ACIT)*, Deggendorf, Germany. 2020. P. 765–768. DOI: 10.1109/ACIT49673.2020.9208951.
10. Midtgård K, Selart M. Cognitive Biases in Strategic Decision-Making. *Administrative Sciences*. 2025. Vol. 15(6). Article 227. DOI: https://doi.org/10.3390/admsci15060227.
11. Tversky A., Kahneman D. Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*. 1973. Vol. 5 (2). P. 207–232. DOI: https://doi.org/10.1016/0010-0285(73)90033-9.
12. Johnson C.K., Gutzwiller R.S., Gervais J. Ferguson-Walter K. Decision-Making Biases and Cyber Attackers. November. *2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)*, Melbourne, Australia. 2021. P. 140–144. DOI: 10.1109/ASEW52652.2021.00038.
13. Cyberproof. AI Data Security: Key Threats and Protection. 2024. URL: https://www.cyberproof.com/blog/ai-data-security-key-threats-and-protection/?utm_campaign=Data%20Security&utm_source=ppc&utm_medium=Google%20Search%20Ads&campaign_id=220.
14. Mutalib N.H.A., Sabri A.Q.M., Wahab, A.W.A. et al. Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review. *Artif Intell Rev*. 2024. Vol. 57. Article 297. DOI: https://doi.org/10.1007/s10462-024-10890-4.
15. Mat N.I.C., Jamil N., Yusoff Y., Kiah M.L.M. A systematic literature review on advanced persistent threat behaviors and its detection strategy. *Journal of Cybersecurity*. 2024. Vol. 10(1). Article 23. DOI: https://doi.org/10.1093/cybsec/tyad023.
16. Imperva. Advanced persistent threat (APT). 2025. URL: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.
17. Huang S. *et al*. PsybORG+: Modeling and Simulation for Detecting Cognitive Biases in Advanced Persistent Threats. MILCOM 2024. *IEEE Military Communications Conference (MILCOM), Washington, DC, USA,* 2024, P. 1–6. DOI: 10.1109/MILCOM61039.2024.10773763.
18. Schmidt, U., Zank, H. What is Loss Aversion? *J Risk Uncertainty*. 2005. Vol. 30. P. 157–167. DOI:10.1007/s11166-005-6564-6.

19. Kahneman D., Tversky A. Prospect theory – Analysis of decision under risk. *Econometrica*. 1979. Vol. 47. P. 263–291. DOI: 10.2307/1914185.
20. Standen M., Lucas M., Bowman D., Richer T.J., Kim J., Marriott, D. CybORG: A Gym for the Development of Autonomous Cyber Agents. *IJCAI-21 1st International Workshop on Adaptive Cyber Defense*, 2021. DOI: https://doi.org/10.48550/arXiv.2108.09118.
21. Jeon S.-E., Oh Y.-S., Lee Y.-J., Lee I.-G. Suboptimal Feature Selection Techniques for Effective Malicious Traffic Detection on Lightweight Devices. *CMES - Computer Modeling in Engineering and Sciences*. 2024. Vol. 140(2). P. 1669–1687. DOI: https://doi.org/10.32604/cmes.2024.047239.
22. Grinde B. The Evolution of Human Social Behavior. *Encyclopedia*. 2024. Vol. 4(1). P. 430–443. DOI: https://doi.org/10.3390/encyclopedia4010029.
23. Ковальчук О.Я, Банах С.В. Логіка права: стратегія кримінального профілювання. *Актуальні проблеми правознавства*. №3 (31). 2022. С. 70–76. DOI:10.35774/app2022.03.169

MODELING DYNAMICS OF CYBERCRIMINALS' LOGICAL PATTERNS

O. Kovalchuk[1], R. Ivanytskyy[2], L. Babala[1]

[1]West Ukrainian National University
11, Lvivska Str., Ternopil, 46009, Ukraine
[2]Ternopil Volodymyr Hnatiuk National Pedagogical University
2, M. Kryvonosa. Str., Ternopil, 46009, Ukraine
Email: olhakov@gmail.com, romikiv@ukr.net, ludaduma7@gmail.com

The study investigates the impact of cognitive biases on the behavior of cybercriminals in the context of advanced persistent threats (APTs). Four key cognitive biases are analyzed: base-rate neglect, confirmation bias, loss aversion, and the sunk cost fallacy. It is established that base-rate neglect leads to overestimating the significance of specific target indicators; confirmation bias drives selective information analysis; loss aversion determines the choice between aggressive and stealth attack methods; and the sunk cost fallacy results in attachment to suboptimal criminal strategies. A mathematical framework is developed to formalize cognitive biases through parametric models with corresponding coefficients for confirmation bias, loss aversion, and sunk cost fallacy. An adaptive cognitive-temporal model (ACTM) is proposed, integrating multiple biases into a single dynamic system with mechanisms of learning and adaptation. The model accounts for the temporal evolution of the cognitive profile of cybercriminals and enables adaptive redistribution of attention among biases depending on specific cyberattack conditions. Practical applications of the model are identified for developing personalized threat detection systems, optimizing active defense strategies, and designing adaptive honeypot systems for deceptive targeting of adversaries. The study substantiates the possibility of exploiting cognitive biases to enhance the effectiveness of defensive mechanisms by provoking predictable decision-making errors among cybercriminals.

Keywords: mathematical modeling, logical patterns, cognitive profile, cybersecurity, Advanced Persistent Threats (APT), decision-making, cybercrime.

DOI 10.15276/imms.v15.no3.386
УДК 519.6:004.93

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 386-392

СТВОРЕННЯ ТА ТЕСТУВАННЯ КРОСПЛАТФОРМЕНОГО ДОДАТКУ ДЛЯ АВТОМАТИЗАЦІЇ СКЛАДСЬКОГО ОБЛІКУ У СФЕРІ МАЛОГО ПІДПРИЄМНИЦТВА

Ю.Ю. Козіна[1], Д.Р. Горпенко[2], Д.О. Гріднєв

Національний університет «Одеська політехніка»
1, пр. Шевченка, Одеса, 65044, Україна
Emails: yuliyakc21@gmail.com[1], horpenko@op.edu.ua[2]

Розглянуто ключові принципи та переваги застосування WMS-систем в управлінні складськими процесами. Проаналізовано сучасні підходи до організації інвентаризації в роздрібній торгівлі та запропоновано власний кросплатформний застосунок, реалізований з використанням технологій C# та MAUI. Розроблений інструмент підтримує роботу як на мобільних пристроях, так і на стаціонарних комп'ютерах, забезпечує функції додавання, зберігання та пошуку товарів, а також підвищує ефективність управління запасами. У рамках розробки реалізовано функціонал моніторингу товарних залишків у реальному часі, визначення їх розміщення на складі та автоматизації процесів інвентаризації. Представлені результати можуть бути впроваджені в практичну діяльність торгових підприємств для підвищення продуктивності персоналу та зменшення впливу людського фактору.
Ключові слова: WMS-система, моніторинг, інвентаризація, кросплатформність.

Вступ. Раціональне управління складськими запасами відіграє важливу роль у забезпеченні успішної діяльності підприємств, особливо в роздрібній торгівлі, де безперебійна наявність продукції на полицях є критичною. Використання застарілих методів обліку, таких як паперові носії чи електронні таблиці, часто спричиняє помилки та ускладнює процес контролю товарних залишків. Це свідчить про актуальність впровадження сучасних цифрових інструментів, здатних оптимізувати інвентаризацію та підвищити ефективність складських операцій.

Мета роботи. Вимоги практики до розробки кросплатформних додатків, що функціонують як на десктопних, так і на мобільних платформах для підтримки працівників під час інвентаризації товарів у магазині, є досить високими. Метою даної роботи є створення кросплатформного додатку з низьким рівнем ресурсоємності на основі принципів WMS-систем (Warehouse Management System) для ефективного управління запасами та контролю товарних залишків.

Основна частина. Проведений аналіз WMS-систем [1], аналогічних програмних рішень та кросплатформних фреймворків дозволив виявити ключові переваги й недоліки кожного підходу, що варто враховувати при розробці або виборі системи управління складом. Серед WMS-систем спостерігається чіткий розподіл за рівнем адаптивності та складності впровадження. Коробкові рішення є простими у встановленні, проте обмежені в налаштуванні. Адаптовані системи є найкращим вибором для середнього бізнесу, забезпечуючи гнучкість та розширюваність. Замовні системи, попри високу вартість і тривалий цикл впровадження, забезпечують найвищу ефективність для великих підприємств із складними логістичними потребами. Водночас, хмарні рішення забезпечують швидкий старт і зменшення експлуатаційних витрат, однак залежать від сторонніх провайдерів. У рамках порівняльного аналізу існуючих рішень, зокрема Odoo та DNTrade [2], виявлено, що обидва продукти частково задовольняють потреби управління складом, однак мають суттєві обмеження. Odoo пропонує тісну інтеграцію з іншими бізнес-процесами, але не забезпечує детального управління простором складу, а також вимагає додаткових налаштувань і витрат. DNTrade є доступнішим, проте менш функціональним – відсутні звіти та

повноцінне управління персоналом, що обмежує можливості масштабування. Щодо кросплатформних фреймворків, MAUI відзначається високою продуктивністю і стабільністю, проте має обмежену екосистему та велику вагу додатків [3]. React Native забезпечує швидку розробку й активну підтримку спільноти, однак не підходить для складної графіки й потребує додаткових рішень для оптимізації інтерфейсу під iOS. Flutter, хоча й потребує вивчення мови Dart, вирізняється потужними інструментами для створення функціональних інтерфейсів та високою продуктивністю, але має певні технічні обмеження через ще не повністю стабілізовану екосистему.

Таким чином, ефективне впровадження WMS-системи потребує збалансованого вибору між функціональністю, масштабованістю та вартістю. А вибір фреймворку для розробки безпосередньо залежить від складності продукту, строків реалізації та наявних технічних ресурсів.

Для оптимізації інвентаризаційних процесів було вирішено створити кросплатформний застосунок, що поєднує можливості WMS-систем і враховує потреби малого бізнесу. Він дозволить швидко знаходити товари за назвою чи штрих-кодом, переглядати залишки та місцезнаходження продукції. Ключовою особливістю є система акаунтів із розподілом ролей і захищеним зберіганням паролів. Застосунок буде підтримувати базові операції з товарами – додавання, редагування, видалення, а також формування звітів. Адміністратор бути мати повний доступ до керування системою. Завдяки локальній базі даних додаток буде працювати навіть без інтернету, що особливо важливо за умов нестабільного зв’язку.

Для зберігання даних у системі інвентаризації пропонується реляційна база даних, яка містить основні сутності, необхідні для функціонування додатку. Структура бази побудована таким чином, щоб забезпечити ефективне управління користувачами та товарами, а також спростити процеси пошуку, редагування та оновлення інформації.

У базі даних визначено дві основні сутності: User (Користувач) та Product (Товар). Розглянемо схему бази даних та її елементи рис. 1.

Сутність User (Користувач) відповідає за управління обліковими записами співробітників і контроль доступу до функцій додатку. Містить унікальний ID (int, первинний ключ з автоінкрементом), ім’я (Name), унікальний логін (Login), зашифрований пароль (Password) та роль (Role), наприклад, «Адміністратор» або «Працівник». Розподіл ролей забезпечує різні рівні доступу для підвищення безпеки.

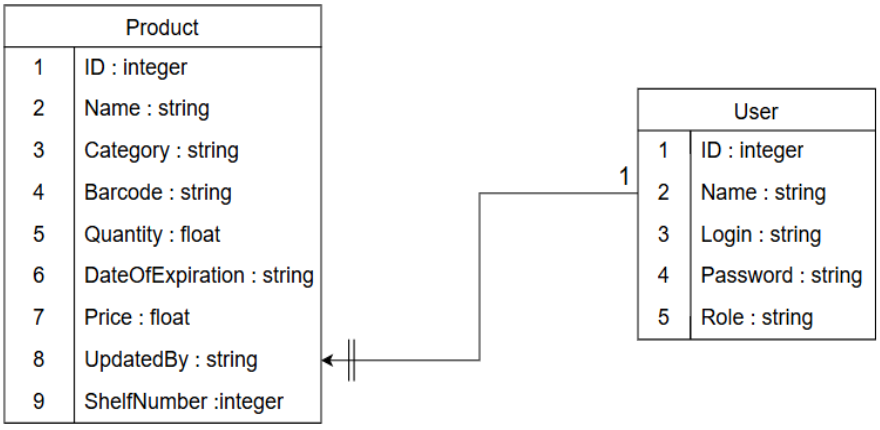


Рис. 1. Схема зв’язку бази даних та її елементи

Сутність Product (Товар) зберігає інформацію про товари на складі та в магазині: унікальний ID, назву (Name), категорію (Category), штрих-код (Barcode), кількість (Quantity), термін придатності (DateOfExpiration), ціну (Price), логін останнього, хто оновлював товар (UpdatedBy) та номер полиці (ShelfNumber). Така структура дозволяє швидко шукати товари, контролювати залишки та оновлювати дані. База даних працює локально, що забезпечує доступ до інформації навіть без інтернету.

Запропоновано зберігати у зашифрованому вигляді за допомогою алгоритму BCrypt, що підвищує безпеку системи. Унікальність логінів виключає дублювання облікових записів. Наявність даних про термін придатності товарів дозволяє автоматизувати контроль прострочених позицій. Алгоритм BCrypt використовує сольове хешування та регульований фактор складності, що ускладнює атаки методом перебору (brute-force) і захищає від відомих вразливостей стандартних хеш-функцій (SHA-256, MD5). Завдяки цьому паролі надійно захищені навіть при зломі бази даних. База даних запроєктована для швидкої обробки запитів, ефективного збереження інформації і можливості подальшого розширення функціоналу системи.Загальна блок-схема функції хешування показана на рис. 2.Під час генерації ключа BCrypt застосовує функцію розширення ключа (key expansion), що приймає сіль і пароль як вхідні дані та виконує велику кількість ітерацій для уповільнення процесу ця система ітерацій є основною захисною рисою алгоритму. Далі відбувається інтенсивне ключове розтягнення (key stretching): алгоритм виконує 2^cost раундів (де cost це налаштовуваний параметр складності), і чим вищий цей параметр, тим довше формується хеш, що значно ускладнює brute-force атаки.

Готовий хеш кодується у спеціальному форматі, яке містить ідентифікатор алгоритму (наприклад, $2a$), сіль, рівень складності (cost) і власне *фінальний* хеш пароля [4].

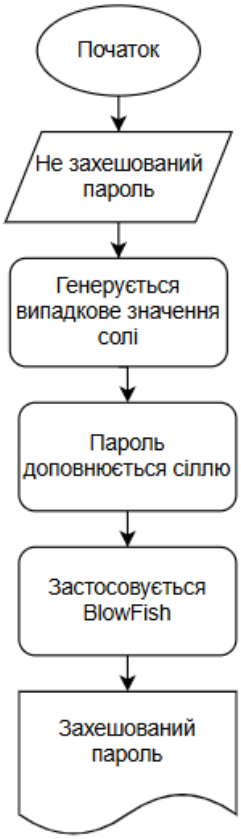


Рис.2. Алгоритм хешування

Ключові функції системи охоплюють основні процеси, зокрема управління товарами, роботу з обліковими записами, перевірку паролів і створення звітів. Розробка функцій орієнтована на зручність використання, безпеку та продуктивність.

Основні з них:

– реєстрація, видалення та вхід користувачів із перевіркою пароля за допомогою Bcrypt;

– додавання, редагування й пошук товарів у базі даних;

– моніторинг термінів придатності та залишків під час формування звітів;

– контроль доступу до функцій залежно від ролі користувача.

Функції системи поділено за призначенням. Зокрема, функції, що стосуються користувачів, згруповані в категорії "Акаунт" і реалізовані з використанням моделі User та запитів до бази даних. Функція входу (аутентифікації) забезпечує доступ до системи лише авторизованим користувачам відповідно до їхніх прав доступу.

У роботі було використано запропонований в [5] алгоритм, що базується на парадоксу днів народжень. При розробці системи, нам треба генерувати унікальні ідентифікатори, які використовуються для аутентифікації користувачів.

Так як ідентифікатор, по суті, дає повний доступ до аккаунту користувача, до його генерації слід підійти серйозно, головна вимога до гарантії його унікальності, так як при співпаданні ідентифікаторів у різних користувачів, один з користувачів отримає доступ до чужого аккаунту. Виходячи з цього ймовірність дворазового генерування одного і того ж ідентифікатора – виникнення колізії – повинна бути вкрай мала.

Так само ідентифікатор по можливості не повинен бути сильно довгим в цілях економії трафіку. На ймовірність виникнення колізії впливають два фактори:

1) розмір ідентифікаційного простору – кількість можливих унікальних ідентифікаторів;

2) метод генерування ідентифікаторів – яким чином ідентифікатор вибирається із загального простору. В ідеалі нам потрібно великий простір (щодо наших потреб), з якого випадково обираються рівномірно розподілені ідентифікатори. Тому для генерації випадкових рівномірно розподілених ідентифікаторів ми будемо конвертувати результат функції crypto.randomBytes(*N*), де *N* кількість повернених випадкових байт, у шістнадцятирічну строку. Ця функція, із пакету інструментів OpenSSL, є реалізацією криптографічно стійкого псевдовипадкового алгоритму який базується на “Вихрі Мерсена” [6]. Залишилося підрахувати скільки випадкових байт нас, влаштує, щоб ймовірність колізії була вкрай мала. Представимо нашу задачу в наступному абстрактному вигляді: Дано n випадкових чисел з дискретного рівномірного розподілу з діапазоном $[1, H]$. Яка ймовірність $p(n, H)$, що, принаймні два числа збігаються?

Дана задача є узагальненням парадоксу днів народжень. Знайдемо зворотну ймовірність $\overline{p}(n, H)$ при $n < H$, таку що всі числа будуть різними:

$$\overline{p}(n, H) = 1 \times \left(1 - \frac{1}{H}\right) \times \left(1 - \frac{2}{H}\right) \times \ldots \times \left(1 - \frac{n-1}{H}\right). \quad (1)$$

H – буде позначати розмір ідентифікаційного простору, P –ймовірність колізії, n – кількість згенерованих ідентифікаторів. Розмір ідентифікаційного простору обчислюється таким чином:

$$H = 2^{8N}, \quad (2)$$

де N – довжина ідентифікатора в байтах.

Виходячи з досліджень, зроблених на базі цього підходу, можна прийняти довжину ідентифікатора рівну 8 байтам, що гарантує, що ми досягнемо ймовірності колізії в 0,1%.

Проведено тестування розробленої системи. На головній сторінці розташовані елементи для пошуку товарів зі списку, список товарів, та навігаційна панель на якій розташовані кнопки для переходу до інших сторінок. На рис. 3 зображено вигляд інтерфейсу сторінки складу. У додатку можна здійснити пошук за назвою товару або ж його штрих кодом. Для цього потрібно ввести в поле пошуку назву або номер штрих коду та натиснути кнопку “Пошук”. Реалізована можливість додати товар.

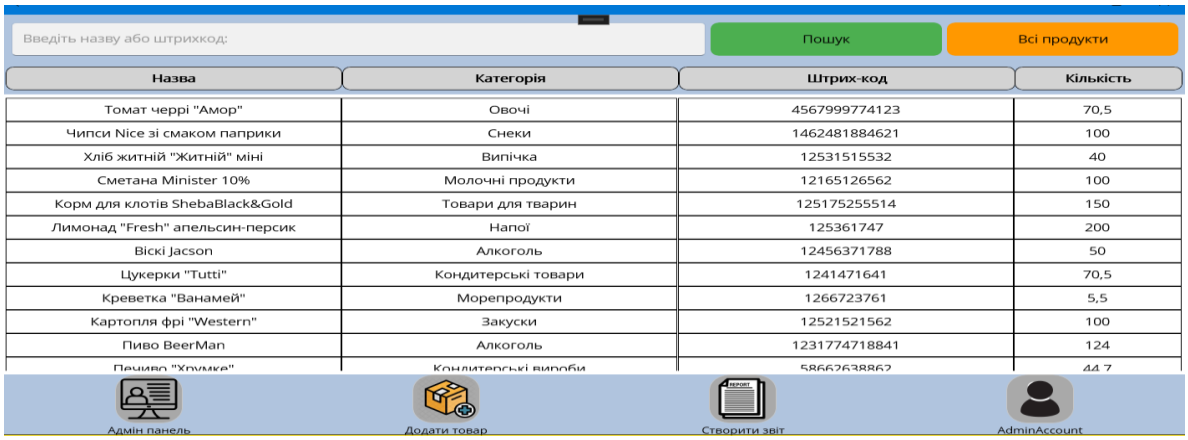


Рис.3. Вигляд інтерфейсу сторінки складу

В полях для інформації можна вписати деталі про товар такі як: назва, категорія, штрих-код, кількість, ціну, дату закінчення терміну придатності та номер полиці (Рис. 4)

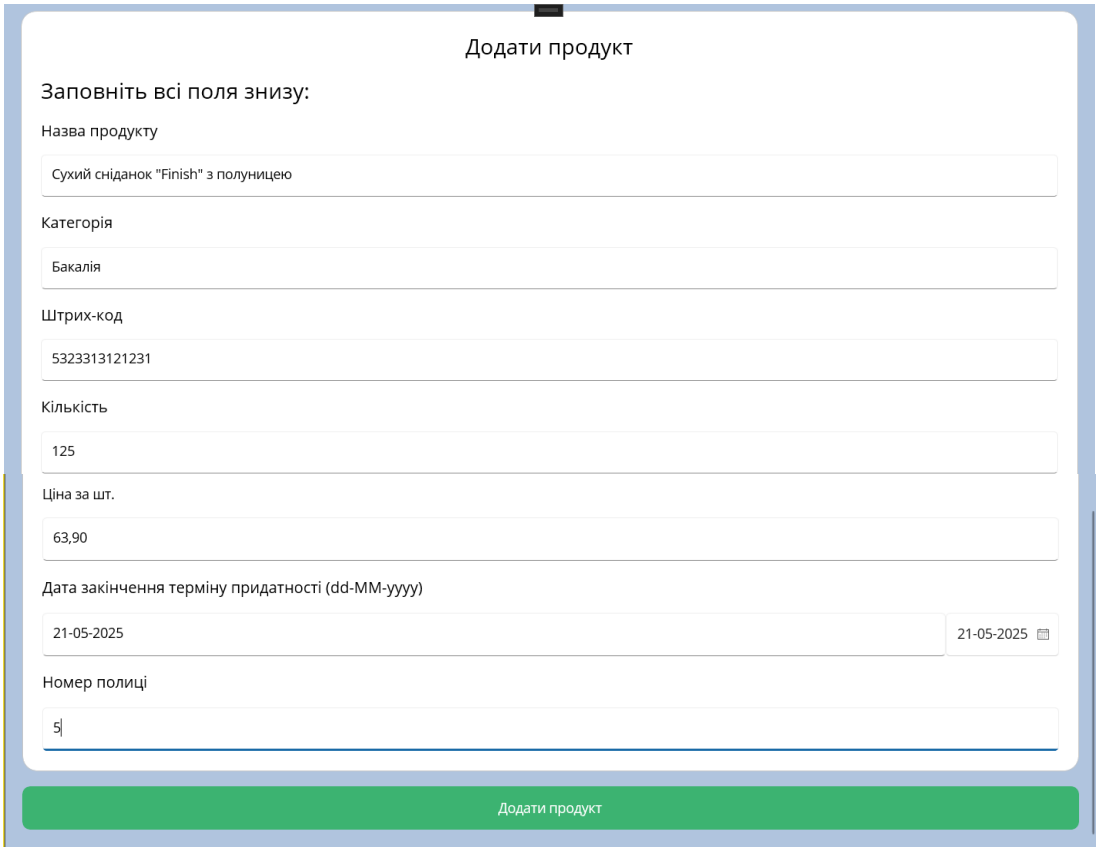


Рис. 4. Вигляд інтерфейсу сторінки додавання товару

Можна сформувати звіт по терміну придатності. Для цього потрібно обрати діапазон дат в яких закінчиться термін придатності товару. На рис. 5 зображено приклад створеного звіту по терміну придатності.

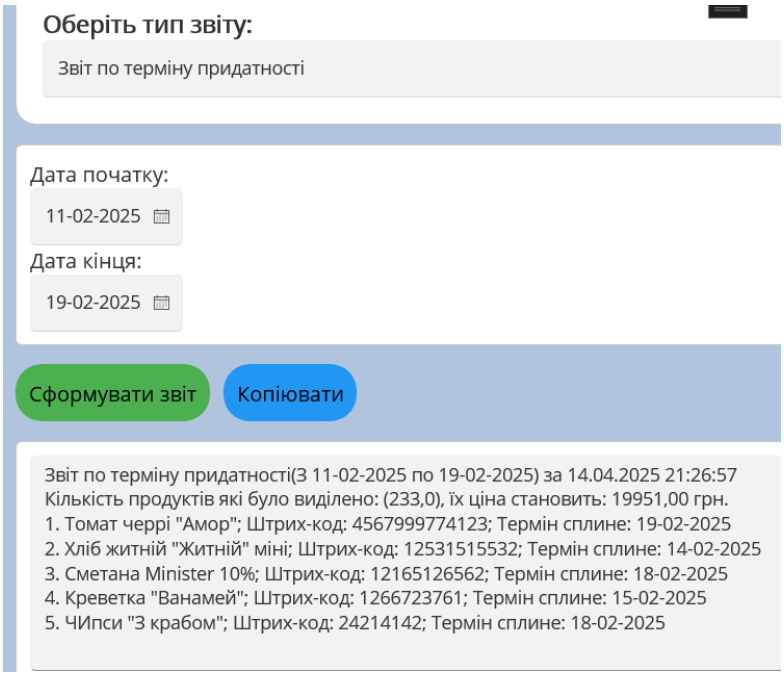


Рис. 5. Приклад створеного звіту по терміну придатності

Після завершення функціонального тестування розроблений застосунок, який ґрунтується на принципах WMS-систем, було порівняно з DNTrade за такими ключовими параметрами: адаптивність інтерфейсу, точність введення та обробки даних, розширені функції інвентаризації, рівень безпеки доступу, стійкість до нестабільного інтернет-з'єднання та модель розповсюдження з економічної точки зору.

Розроблений додаток вирізняється справжньою кросплатформенністю – інтерфейс автоматично оптимізується під будь-який тип пристрою, зберігаючи зручність користування та чіткість відображення. У випадку з DNTrade, який переважно орієнтований на використання з десктопів, перехід на мобільні пристрої призводить до зменшення елементів інтерфейсу або їх згортання в списки, що ускладнює доступ до потрібної інформації та уповільнює процес вибору товарів.

Висновки. Запропонований кросплатформений додаток, розроблений за принципами WMS-систем не лише покращує деякі функції у DNTrade такі як адаптивність, точність обліку, безпека паролів та стабільність роботи без інтернету, а й надає бізнесу додаткову економію завдяки безкоштовному розповсюдженню. Результати його функціонування мають прикладне значення та відкривають перспективи подальшого вдосконалення через інтеграцію з іншими системами й використання розширених аналітичних інструментів.

Список літератури

1. Implementing Warehouse Management Systems (WMS) in Logistics URL: https://www.researchgate.net/publication/330293478
2. Oddo ERP and CR. URL: https://www.odoo.com
3. Roger Y. .NET MAUI Cross-Platform Application Development: навчальний посібник. Birmingham: Packt Publishing Ltd., 2023. 400 p.
4. Fast Software Encryption, Description of a New Variable-Length Key, 64-Bit Block Cipher URL: https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html
5. Birthday problem URL: https://en.wikipedia.org/wiki/Birthday_problem
6. Mersenne Twister Home Page URL: http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html

DEVELOPMENT AND TESTING OF A CROSS-PLATFORM APPLICATION FOR WAREHOUSE MANAGEMENT AUTOMATION IN THE FIELD OF SMALL BUSINESS

Yu.Yu. Kozina[1], D.R. Gorpenko[2], D.O. Gridnev

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: yuliyakc21@gmail.com[1], horpenko@op.edu.ua[2]

The key principles and advantages of using WMS systems in warehouse process management have been examined. Modern approaches to inventory organization in retail have been analyzed, and a custom cross-platform application developed using C# and MAUI technologies has been proposed. The developed tool supports operation on both mobile devices and desktop computers, providing functionality for adding, storing, and searching for products, while also improving inventory management efficiency. The application includes features for real-time stock level monitoring, determining product placement within the warehouse, and automating inventory processes. The presented results can be applied in the practical operations of retail businesses to increase staff productivity and reduce the impact of human error.
Keywords: WMS system, monitoring, inventory, cross-platform.

DOI 10.15276/imms.v15.no3.393
УДК 681.51

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 393-401

ІНТЕЛЕКТУАЛЬНИЙ МЕТОД УПРАВЛІННЯ АВТОНОМНИМИ СУДНАМИ НА ВНУТРІШНІХ ВОДНИХ МАГІСТРАЛЯХ

М.М. Масьонкова

Херсонська державна морська академія
20, Ушакова пр., Херсон, 73000, Україна
Email: masyonkova@gmail.com

Запропоновано метод автономної навігації для внутрішніх водних шляхів із притоками, спрямований на зниження ризику зіткнень суден у складних навігаційних умовах. Проаналізовано особливості маневрування суден у вузьких притоках, де невизначеність дій інших суден і складні гідродинамічні фактори значно підвищують аварійні ризики. Представлена методика поєднує цифрове моделювання річкового середовища, удосконалений алгоритм трасування маршруту, тривимірну динамічну модель руху судна, алгоритм ухвалення рішень відповідно до «Правил для уникнення зіткнень на внутрішніх річках» та належну морську практику. Вперше запропоновано фазову модель зближення суден для шляхів водних приток. Це забезпечило можливість відокремлювати безконфліктну та конфліктну фази взаємодії і своєчасно ініціювати маневр ухилення. Результати моделювання підтвердили ефективність запропонованого підходу: алгоритм забезпечує своєчасне виявлення ризику, вибір оптимальної стратегії ухилення та збереження курсової стійкості судна. Практична значущість дослідження полягає у створенні основи для впровадження автономних систем підтримки прийняття рішень на внутрішніх водних шляхах, що може суттєво підвищити безпеку судноплавства в районах злиття річок.

Ключові слова: моделювання, інтелектуальні методи, притокові водні шляхи; автономне прийняття рішень, навігація, ідентифікація ризику зіткнення, уникнення зіткнень, ефективність

Вступ. Сучасний розвиток технологій автономного судноводіння відкриває нові горизонти для забезпечення безпеки та ефективності на внутрішніх водних шляхах. Зростання інтенсивності судноплавства на річках і каналах, зокрема у районах злиття основних русел та їхніх приток, супроводжується підвищенням ризиків аварійних ситуацій. Згідно зі статистичними даними, переважна більшість зіткнень на внутрішніх водах зумовлена людським фактором – помилками під час оцінювання навігаційної обстановки, неправильним тлумаченням правил плавання чи запізнілими маневрами ухилення [1]. З цієї перспективи автономні навігаційні системи розглядаються як перспективний інструмент для мінімізації впливу людських помилок та підвищення рівня безпеки судноплавства [2, 3]. Використання автономних рішень дає можливість своєчасно виявляти потенційні небезпеки та оперативно формувати рекомендації для екіпажу або безпосередньо для суднової автоматизованої системи управління. Такі системи здатні прогнозувати траєкторії руху цільових суден, оцінювати ступінь ризику зближення, визначати оптимальний момент для маневрування ухилення та пропонувати безпечні параметри руху – курс і швидкість [4]. Це надзвичайно важливо для судноплавства у вузьких та складних умовах притокових русел, де невизначеність дій інших учасників руху поєднується з природними та технічними обмеженнями: звуженим фарватером, обмеженою видимістю, підвищеним впливом течії та низькою маневровістю річкових суден [5].

Попри значні досягнення у сфері автономної навігації для морських і прибережних суден, питання безпечного руху у внутрішніх водних системах залишається недостатньо вивченим. Більшість існуючих підходів орієнтовані на відкриті

акваторії, де умови відносно передбачувані, а простір для маневра значно більший. Натомість притокові ділянки річок відзначаються високою динамічністю навігаційної ситуації: раптовою появою суден з обмеженою можливістю маневрування, складною геометрією фарватеру та необхідністю дотримання спеціальних регуляторних правил, що визначають пріоритети руху у місцях злиття [6, 7].

Актуальність даного дослідження зумовлена потребою у створенні спеціалізованих методів автономного управління судном саме в умовах внутрішніх притокових шляхів. Такі методи мають інтегрувати сучасні алгоритми оцінки ризику зіткнень, динамічні моделі руху суден, адаптивні методики трасування маршруту та чинні навігаційні правила. Лише комплексний підхід, що поєднує технічні, регуляторні та практичні аспекти, здатен забезпечити високу надійність системи автономної навігації та сприяти підвищенню рівня безпеки і ефективності внутрішнього судноплавства.

Огляд літератури. Останнім часом увагу наукової спільноти все частіше привертає проблема ефективності використання як простих, так і комбінованих індексів ризику, які оцінюють безпеку навігації суден. Такі індекси поєднують автоматичну ідентифікаційну систему (AIS) із візуальними або радарними джерелами та враховують специфіку вузьких і мілких акваторій. Так, у [8] автори запропонували методику робастної оцінки ризику з використанням ф'юзії AIS та зображення, що підвищило стійкість до пропусків/збоїв у даних і забезпечило покращення складних конфігурацій руху судна в каналах і на злиттях річок. Паралельно з технічним прогресом зростає увага до відповідності навігаційним правилам (міжнародним та національним/внутрішнім регламентам). Дотримання загальноприйнятих правил є ключовою вимогою для автономного управління судном, обмеження та логіки прийняття рішень [9]. Для внутрішніх водних шляхів актуальні також міжнародні навігаційні правила, які деталізують пріоритети в обмежених водах. Новітні дослідження у цій сфері пропонують формалізовані зони безпеки/дистанції та механізми ролей на зразок "дати дорогу/йти прямим курсом" [10]. Низка сучасних досліджень орієнтовані на оцінювання ризику навігації суден у внутрішніх водах, включно з вузькими каналами й ситуаціями перетину/злиття [4]. За 2023–2025 рр. з'явилися спеціальні огляди автономного судноплавства, які, зокрема, розглядають питаннями юридичної відповідальності, інтеграції з береговою інфраструктурою, стандартів датчиків і сертифікації [11]. Публікації з питань підвищення рівня морської безпеки та ефективного управління ризиками все частіше розглядають проблематику використання штучного інтелекту та його застосування у сфері прогнозного технічного обслуговування, навігації, аналізу ризиків, управління екіпажем та контролю небезпечних матеріалів демонструє значний потенціал для зниження загроз і оптимізації процесів [12, 13].

Однак фрагментарність наукових розробок у сфері автономного судноплавства на внутрішніх водних шляхах, недостатня інтеграція існуючих підходів до оцінки ризиків і управління безпекою навігації обумовлюють необхідність подальших комплексних досліджень інтелектуальних методів управління автономними суднами на внутрішніх водних магістралях.

Мета роботи. Метою даного дослідження є створення комплексного методу автономної навігації суден у внутрішніх водних шляхах з притоками, який здатен забезпечити безпечне та ефективне керування рухом у складних і динамічних умовах.

Для досягнення цієї мети в роботі вирішуються наступні завдання:

- розробити математичну модель оцінювання ризику зіткнень, яка враховує багатосуднові сценарії та специфіку вузьких фарватерів;
- інтегрувати динамічні моделі маневрових характеристик судна (з урахуванням ефектів мілководдя та обмеженості маневрування) у процес планування траєкторій;

- поєднати алгоритми прогнозування руху та ухвалення рішень з чинними міжнародними та національними правилами судноплавства;
- сформувати стратегію адаптивного маневру ухилення, здатну своєчасно переходити від безконфліктної до конфліктної фази взаємодії суден і мінімізувати ризик аварійної ситуації;
- провести моделювання та імітаційні експерименти для перевірки ефективності та стійкості запропонованого методу в реалістичних умовах річкових злиттів.

Ключові проблеми та напрямки досліджень для автономної навігації на притокових шляхах. Специфічні особливості навігації у внутрішніх притоках ускладнюють дослідження автономної навігації на притокових шляхах. Ми визначили три ключові проблеми та напрями у цій сфері.

1. Відсутність методики оцінки ризику зіткнення, що враховує правила навігації.
2. Недостатній розвиток адаптивних методів оптимізації рішень.
3. Неврахування взаємодії динаміки маневру судна та довкілля.

Удосконалений метод автономної навігації для внутрішніх приток. У відповідь на ці виклики у роботі запропоновано удосконалений метод автономної навігації для внутрішніх приток. Він призначений для виявлення потенційних ризиків зіткнення та надання судноводію рекомендацій щодо того, коли і який саме маневр ухилення виконати. Метод базується на «Правилах щодо запобігання зіткненням на внутрішніх водних шляхах» та принципів належної морської практики [15]. На основі прогнозованої траєкторії цільового судна визначаються оптимальні принципи ухилення та момент для маневра відповідно до поточної ситуації зближення суден. Далі, поєднується маневрова математична модель руху судна та метод керування курсом із технікою трасування маршруту. На основі цієї консолідації формується модель ухвалення рішення щодо уникнення зіткнення, яка обирає оптимальну стратегію для кожної ситуації. Метод враховує маневрові характеристики судна і забезпечує дотримання правил «Правил для уникнення зіткнень на внутрішніх річках» та належної морської практики. Цей метод може бути використаний для автономної навігації у складних умовах внутрішніх притокових водних мереж.

Фази взаємодії двох суден. На основі аналізу динаміки зближення суден у вузьких внутрішніх водних шляхах ми виокремили дві фази взаємодії двох суден: фаза без конфлікту (нормального розходження) і фаза конфлікту (небезпечного зближення). У фазі без конфлікту обидва судна можуть вільно рухатися запланованим курсом без спеціальних маневрів ухилення, оскільки на цьому етапі відсутній ризик зіткнення. Коли система виявляє потенційний ризик, відбувається перехід до фази конфлікту. Цей момент ініціює початок маневру ухилення (точка А). Після того, як небезпека минає і ризик зіткнення зникає, фіксується завершення маневру ухилення (точка В). З цього моменту подальші екстрені маневри вже не потрібні (Рис. 1). Після точки В судно переходить у фазу відновлення курсу. Такий поділ процесу зближення на етапи допомагає чітко визначити критичні моменти для ухвалення рішень у сценаріях уникнення зіткнень на річці.

Рис. 1 Динаміка зближення суден та дії з запобігання їх зіткнення

Загальний підхід. Запропонована методологія передбачає виконання кількох етапів. Спочатку формується цифрова модель навігаційного середовища для внутрішньої водної системи з притоками. Навколишня обстановка (береги, межі фарватеру, рекомендований курс, роздільні смуги, якірні стоянки тощо) представлена у вигляді математичних об'єктів (точок, ліній, багатокутників), щоб судно могло «розуміти» межі і структуру водного шляху [16]. Непрямолінійний маршрут судна було розділено на серію коротких прямих відрізків – умовних прямокутних ділянок, кожна задана чотирма координатами вершин. Такий підхід до дискретизації фарватеру забезпечив опис кривого каналу набором прямолінійних відрізків та спростив розрахунки траєкторії судна. Серединою кожного прямого сегмента проходить рекомендований маршрут – ламана лінія, що з'єднує середини послідовних відрізків каналу. Цифрова модель водної ділянки з притоками створює основу для навігаційних обчислень і рішень.

Модель руху судна. При моделюванні руху судна було враховано тільки горизонтальні плоскі рухи – розкачку (свай), дрейф (знос) і поворот (ріса, або рискання). Вертикальні коливання (диферент, крен, килювання) не взято до уваги, оскільки вони мало впливають на маневрування у сенсі зіткнень. Для точного відтворення динаміки руху застосовано трьохступеневу модель з урахуванням сил опору води, вітру, течії та дії рушія і стерна. Рівняння руху судна у горизонтальній площині записано у вигляді системи (1) для трьох ступенів вільності (курсу, поздовжнього і поперечного руху):

$$\begin{cases} \left(m+m_x\right)\cdot\dot{u}+\left(m+m_x\right)\cdot r\cdot v = X_H + X_P + X_R + X_E \\ \left(m+m_y\right)\cdot\dot{v}-\left(m+m_y\right)\cdot\dot{u}\cdot v = Y_H + Y_P + Y_R + X_E \\ \left(I_{zz}+J_{zz}\right)\cdot\dot{r} = N_H + N_P + N_R + N_E \end{cases} \quad (1)$$

де m – маса судна, m_x та m_y – додаткова маса (коефіцієнти інерції води) відповідно по осі x (поздовжній) та y (поперечний), u, v, r – прискорення поступального руху (вперед u, бічного v) та кутове прискорення повороту r, X, Y, N – сили та моменти, що діють на корпус (H – гідродинамічні сили корпусу), гребний гвинт (P), стерно (R) та сили довкілля (E, зумовлені вітром, течією, мілководдям тощо). Таким чином, перше рівняння описує баланс сил уздовж курсу (тяга рушія та опір води), друге – поперечних сил (бічний дрейф і відповідні опори), а третє – баланс обертальних моментів навколо вертикальної осі судна. Окремо враховано роботу гребного гвинта: ефективна тяга гвинта T визначається з урахуванням коефіцієнта відбору потужності на гвинт t_p. В статті наводиться формула (2) для розрахунку тяги T та пов'язані залежності, які враховують характеристики гвинта і корпусу.

$$Y_P = \left(1-t_p\right)T \quad (2)$$

Враховано емпіричні формули для коефіцієнтів, що відображають ефект мілководдя, індукованої течії за кормою та інших гідродинамічних факторів (формула (3)). Модель включає коригувальні коефіцієнти для врахування складних ефектів (мілководдя, потік води від гвинта до корпуса, відхил стерна тощо).

$$\begin{cases} f = k_t \beta_R \\ k_t = 0.00023(\gamma_A \cdot L / D_P) - 0.028 \\ \gamma_A = (B/d)\{1.3(1-C_b) - 3.1 l_{cb}\} \\ l_{cb} = x_c / L \cdot 100 \\ \beta_R = \beta - l_R \dfrac{r}{V} \end{cases} \quad (3)$$

де β_R – кут дрейфу керма, B – ширина, d – осадка, L – довжина, D_p – діаметр гвинта, x_c – поздовжня координата центра плавучості; k_t – поправковий коефіцієнт тяги, γ_A – поправковий коефіцієнт індукованої швидкості обтікання корпусу, C_b – коефіцієнт повноти корпусу, l_{cb} – поздовжній центр плавучості), l_R – коефіцієнт кута дрейфу керма; r – кутова швидкість хитавиці навколо вертикальної осі, V – поздовжня швидкість.

Модель відстеження маршруту. Для забезпечення руху судна по заданому фарватеру використано покращений алгоритм наведення по лінії видимості (Line-of-Sight, LOS). У кожний момент обирається цільова точка маршруту попереду судна на деякій фіксованій відстані вздовж курсу (ця відстань – попереджувальна дистанція вздовж маршруту). Кут напрямку на цю цільову точку визначає бажаний курс ψ_{LOS} для судна. На рис. 2 статті схематично показано принцип LOS: поточна позиція судна проектується на рекомендований маршрут, від неї відкладається наперед задана відстань Δ вздовж маршруту – отримана точка і є ціллю для наведення.

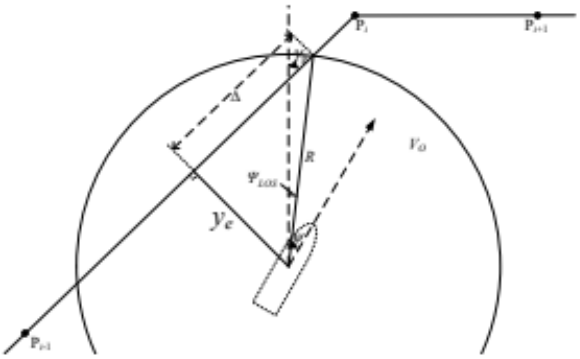


Рис. 2. Наведення по лінії видимості

Позначимо бічне відхилення судна від маршруту як $y_e(t)$, а курс самого маршруту в цій точці як γ_p. Тоді бажаний курс на цільову точку розраховують за формулою (4):

$$\psi_{LOS}\ \gamma_P - \tan^{-1}\left(\frac{y_e(t)}{\Delta}\right) \quad (4)$$

Носова частина суднаспрямована у бік маршруту, пропорційно відхиленню y_e. Однак вибір надто великої Δ призводить до повільного повернення на курс, а надто малої – до перерегулювання. Зважаючи на значну інерцію та обмежену керованість річкових суден, запропоновано відмовитися використовувати адаптивне визначення попереджувальної дистанції залежно від величини відхилення. Введено функцію (5)–(6), яка збільшує Δ при великих відхиленнях і зменшує при малих, використовуючи згладжену косинусоїдальну залежність (це забезпечує швидке, але плавне повернення на курс без перерегулювання).

$$f(x)=\begin{cases}0, x \le x_{\min}\\ \frac{1}{2}\left(1-\cos\frac{\pi(x-x_{\min})}{x_{\max}-x_{\min}}\right), x_{\min} \le x \le x_{\max}\\ 1, x \ge x_{\max}\end{cases} \quad (5)$$

$$\Delta = \Delta_{\min} + (\Delta_{\max} - \Delta_{\min})\left[1 - f(y_e(t))\right] \quad (6)$$

У результаті судно ефективно утримується на фарватері навіть за наявності збурень.

Модель оцінювання ризику зіткнення. У притокових водах судна можуть рухатися як по каналу (вздовж рекомендованого маршруту), так і поза фарватером (підходячи під різними кутами, наприклад, при виході з притоку). Пропонується класифікація інших суден за їхнім курсом: якщо курс іншого судна приблизно збігається з напрямком каналу, його вважають «тим, що слідує фарватером»; якщо інше судно йде під значним кутом або взагалі поза межами каналу, воно належить до «нефарватерних» об'єктів. На основі експертних оцінок (досвіду капітанів) встановлено граничне значення 5° для різниці курсу судна і напряму каналу: якщо відхилення курсу іншого судна від осі каналу перевищує 5°, його вважають таким, що не дотримується фарватеру.

В залежності від категорії іншого судна, застосовуються різні методи прогнозування його траєкторії.

1. Для суден на фарватері: вважається, що вони до чергового повороту рухатимуться вздовж осі каналу, а в точці повороту здійснять маневр зміни курсу на наступний сегмент каналу.
2. Для суден поза фарватером: застосовується проєкція швидкісного вектора – проста інерційна модель, що припускає збереження поточних параметрів руху (курсу і швидкості). Такий метод (відомий як метод кінематичного прогнозування) обчислює майбутню позицію $P_{TS}(t_2|t_1)$ цільового судна в момент t_2 за його положенням $P_{TS}(t_1)$ на час t_1, курсом C_{TS} та швидкістю v_{TS}.

Окремо розглядається перехідна зона на стику притоку і головного русла. В межах цієї зони (її вводять штучно у моделі) вважається, що судно, яке виходить з притоку, встигає завершити маневр повороту перед виходом до головного русла і входить у нього вже з постійним курсом (швидкість стабілізувалась). Від моменту перетину кордону зоні злиття майбутня поведінка іншого судна оцінюється за його останнім курсом і швидкістю.

У цій зоні для іншого судна запропоновано спеціальну модель уникнення зіткнення: по-перше, вважається, що уникнення виконується тільки поворотом (без зміни швидкості в самій зоні злиття). Кут повороту фіксований (швидкість стала). Швидкість обчислюється на основі послідовних курсів судна, а подальша траєкторія прогнозується обчисленням нових компонента швидкості та координат. Така модель враховує плавний перехід маневру в притоку до руху в головному руслі, що підвищує точність оцінки ризику зіткнення і відповідає реальним практикам управління суднами.

Алгоритм ухвалення рішення про маневр ухилення базується на поєднанні навігаційних правил і динамічних моделей. Спочатку система на основі даних сенсорів виявляє конфлікт: об'єднує дані про рух власного судна, усіх цільових суден та навколишнього середовища, після чого за допомогою моделі прогнозу ідентифікує потенційні конфлікти протягом заданого горизонту часу. Далі, відповідно до «Правил для уникнення зіткнень на внутрішніх річках» і принципів уникнення зіткнень, система визначає роль власного судна у кожному конфлікті – поступається судно дорогою чи має право прямувати своїм курсом:

- якщо власне судно повинно дати дорогу, то воно негайно виконує необхідний маневр ухилення згідно з правилами (наприклад, зміну курсу або гальмування);
- якщо власне судно виступає як судно з переважним правом проходу, то воно контролює ситуацію: відстежує дії іншого судна і оцінює їхню достатність;
- якщо інше судно здійснює належний маневр вчасно і правильно, власне судно зберігає свій курс і швидкість (дотримуючись права руху прямим курсом);
- якщо дії іншого судна недостатні або запізнілі, власне судно зобов'язане втрутитися – виконати коригувальний маневр, щоб забезпечити розходження (зазвичай, дозволити іншому судну пройти поза доменом безпеки власного судна).

Реалізований алгоритм повністю відповідає чинним правилам судноплавства для внутрішніх водних шляхів Китаю. Зокрема, враховано Правило 15 «Правил для уникнення зіткнень на внутрішніх річках», яке спеціально регулює рух у місцях злиття річкового русла з притокою [11]. Це правило визначає пріоритети проходу для суден з основного русла і з притоку залежно від напрямків їх руху:

- якщо судно в головному руслі і судно з притоку рухаються в одному напрямку, то судно на головній річці зобов'язане дати дорогу судну, що виходить з притоки;
- якщо судна в руслі і притоку йдуть у зустрічних напрямках, то пріоритет визначається за течією: судно, що рухається проти течії (вгору за течією), повинно поступитися дорогою судну, що йде за течією (вниз).

У загальному випадку судно в притоку має перевагу при вході в основне русло, якщо обидва йдуть в одному напрямку, а судно, що йде вниз за течією, має перевагу перед тим, що йде вгору, при зустрічному курсі. Алгоритм ухвалення рішень використовує цю логіку для призначення ролей власне судно/інше судно у кожній конкретній ситуації зближення суден.

Аналіз ефективності. Поєднання динамічної моделі руху та методу повного перебору маневрів дає можливість успішно вирішувати завдання навігації в складних ситуаціях зустрічі суден. Метод забезпечує одночасно і ефективне уникнення зіткнення, і продовження плавання за курсом (операційна ефективність): судно не просто ухиляється, а робить це оптимально, не втрачаючи більше шляху, ніж потрібно.

Переваги та унікальність підходу. Розроблений метод демонструє цілісність підходу: він поєднав багато компонентів (цифрове середовище, правила плавання, динаміку судна, стратегія ухилення) у єдину систему. Алгоритм враховує формальні навігаційні правила і належну морську практику при виборі маневрів, а не оптимізує суто математичний критерій. Це наближає його до реального використання, оскільки гарантує, що запропоновані дії будуть зрозумілі й очікувані для живого капітана та інших учасників руху.

Висновки. У статті розроблено модель автономної навігації для внутрішніх водних шляхів із притоками шляхом об'єднання двох компонент: моделі уникнення зіткнень та моделі трасування маршруту з використанням математичного опису руху судна. Запропоновано методику, що забезпечує ефективну ідентифікацію ризику зіткнення та генерує конкретні рекомендації щодо маневру ухилення, пристосовані до маневрових характеристик судна. Реалізовано динамічне відстеження змін: система постійно фіксує відхилення курсу та швидкості цільових суден, інтерпретує їхні наміри (наприклад, зрозуміти, чи інше судно планує повернути чи продовжує прямий шлях) і адаптивно переналаштовує власне рішення. Завдяки цьому кожна дія власного судна актуальна до поточної ситуації, а не до застарілої інформації. Усі маневри (зміни курсу і швидкості), які виконує система, прораховуються в єдиному інтегрованому контурі, що враховує обмеження навколишнього середовища (береги, глибини), дотримання правил

(регуляторні обмеження «Правил для уникнення зіткнень на внутрішніх річках») та можливості судна (максимальні кути повороту, прискорення тощо). Такий всеосяжний підхід забезпечує надійність і безпеку маневру навіть у багатосуднових сценаріях у складній обстановці.

Практична значущість роботи полягає в тому, що вперше детально опрацьовано автономну навігацію саме для вузьких внутрішніх притокових шляхів – сфери, що раніше отримувала менше уваги дослідників. Метод потенційно може бути впроваджений у системи підтримки рішення для екіпажів річкових суден або безпосередньо в автономні судна, підвищуючи безпеку на небезпечних ділянках. У подальшому планується розширити модель динаміки, включивши ефекти мілководдя, близькості берегів та взаємодії суден між собою, щоби підвищити адекватність симуляції реальних умов.

Список літератури

1. Dong C., Guo X., Gong Y. Research on Coupling Mechanisms of Risk Factors for Collision Accidents Between Merchant Ships and Fishing Vessels Based on the N-K Model. *Journal of Marine Science and Engineering*, 2025. V.13(3). P. 466. URL: https://doi.org/10.3390/jmse13030466
2. Durlik I., Miller, T. Kostecka, E. Kozlovska, Ślączka W. Enhancing Safety in Autonomous Maritime Transportation Systems with Real-Time AI Agents. *Applied Sciences*. 2025. V. 15(9). P. 4986. URL: https://doi.org/10.3390/app15094986
3. Liu C., Mao W., Liu J., & Chu, X. (). Intelligent Ships and Waterways: Design, Operation and Advanced Technology. *Journal of Marine Science and Engineering*. 2024. V.12(9), P. 1614. URL: https://doi.org/10.3390/jmse12091614
4. Alamoush A.S., Ölçer A.I. Maritime Autonomous Surface Ships: Architecture for Autonomous Navigation Systems. *Journal of Marine Science and Engineering*, 2025. V.13(1), P. 122. URL: https://doi.org/10.3390/jmse13010122
5. Масьонкова М. М. Інтелектуальна система аналізу ризиків для підтримки прийняття рішень при евакуації корабля. *Інформатика та математичні методи в моделюванні*. 2025. Том 15, №2. С. 107–114. https://doi.org/10.15276/imms.v15.no1.107
6. Carvalho D.M., Dias J.M., de Abreu J.F. Sensing in Inland Waters to Promote Safe Navigation: A Case Study in the Aveiro's Lagoon. *Sensors*. 2024. Vol. 24(23). P. 7677. URL: https://doi.org/10.3390/s24237677
7. Huang L., Chen J., Xu L., Li H., Hao G., He Y. Research on Decision-Making Methods for Autonomous Navigation in Inland Tributary Waterways. *Applied Sciences*. 2025. V.15(7). P. 3823. URL: https://doi.org/10.3390/app15073823
8. Zhang H., Cao Y., Shan Q., Sun Y. Collision Avoidance for Maritime Autonomous Surface Ships Based on Model Predictive Control Using Intention Data and Quaterp.nion Ship Domain. *Journal of Marine Science and Engineering*, V. 202513, 124. URL: https://doi.org/10.3390/jmse13010124
9. Ding H., Weng J. A robust assessment of inland waterway collision risk based on AIS and visual data fusion. *Ocean Engineering*. 2024. V.2024*307*. P. 118242. URL: https://doi.org/10.1016/j.oceaneng.2024.118242
10. Hannaford E., Maes P., Van Hassel E. (). Autonomous ships and the collision avoidance regulations: a licensed deck officer survey. *WMU Journal of Maritime Affairs*. 2022. V.*21*. P.233–266. URL: https://doi.org/10.1007/s13437-022-00269-z
11. Potočnik, P. (). Model Predictive Control for Autonomous Ship Navigation with COLREG Compliance and Chart-Based Path Planning. *Journal of Marine Science and Engineering*. 2025. V.13. P. 1246. URL: https://doi.org/10.3390/jmse13071246

12. Durlik I., Miller T., Kostecka E., Tuński T. Artificial Intelligence in Maritime Transportation: A Comprehensive Review of Safety and Risk Management Applications. *Applied Sciences*. 2024. V.14(18). P.8420. URL: https://doi.org/10.3390/app14188420
13. Pang Y., Huang T., Wang Q. AI and Data-Driven Advancements in Industry 4.0. *Sensors*. 2025. V.*25*(7). P. 2249. URL: https://doi.org/10.3390/s25072249
14. Regulations of the People's Republic of China on Administration of Traffic Safety in Inland Waters. 2025. URL: https://faolex.fao.org/docs/pdf/chn149783.pdf
15. Understanding on Common Shipping OECD Legal Instruments Principles. OECD. 2025. URL: https://legalinstruments.oecd.org/public/doc/165/165.en.pdf
16. Miličević M., Vujović I., Petković M., Kuzmanić-Skelin A. Toward an Augmented Reality Representation of Collision Risks in Harbors. *Applied Sciences*. 2025. V.15, P.9260. URL: https://doi.org/10.3390/app15179260

INTELLIGENT METHOD OF CONTROLLING AUTONOMOUS VESSELS ON TRIBUTARY WATERWAYS

M. Masonkova

Kherson State Maritime Academy
20, Ushakov ave., Kherson, 73000, Ukraine
Email: masyonkova@gmail.com

The article proposes a method of autonomous navigation for inland waterways with tributaries, aimed at reducing the risk of vessel collisions under complex navigation conditions. The peculiarities of vessel maneuvering in narrow tributaries are analyzed, where the uncertainty of other vessels' actions and complex hydrodynamic factors significantly increase accident risks. The presented methodology combines digital modeling of the river environment, an advanced route-tracing algorithm, a three-dimensional dynamic model of vessel motion, a decision-making algorithm based on the "Inland Waterways Collision Avoidance Rules" and good seamanship practice. For the first time, a phase model of vessel encounter for tributary waterways is proposed. This made it possible to distinguish between conflict-free and conflict phases of interaction and to timely initiate an avoidance maneuver. Simulation results confirmed the effectiveness of the proposed approach: the algorithm ensures timely risk detection, optimal avoidance strategy selection, and preservation of vessel course stability. The practical significance of the study lies in establishing a foundation for the implementation of autonomous decision-support systems on inland waterways, which can substantially improve navigation safety in river confluence areas.
Keywords: modeling, intelligent methods, tributary waterways, autonomous decision-making, navigation, collision risk identification, collision avoidance, efficiency.

DOI 10.15276/imms.v15.no3.402
УДК 004.61

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 402-418

ДІАГНОСТУВАННЯ ЕЛЕКТРОТЕХНІЧНИХ ПІДСИСТЕМ ЗА УМОВ НЕЗАЛЕЖНОСТІ ЇХ СПОСТЕРЕЖЕННЯ ТА УПРАВЛІННЯ

А. А. Савєльєв[1], Л. Л. Прокофьєва[2], М.А. Котолуп[3]

[1,2] Національній університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
[3] Фаховий коледж морського транспорту Національного університету
«Одеська морська академія»
40/42, Маразліївська, 65014, Україна
Emails: savieliev.a.a@op.edu.ua [1], prokofieva@op.edu.ua[2], marinakstvdi@gmail.com[3]

Сучасна практика розробки технічних систем, і електротехнічних зокрема, показує, що їх надійність закладається на стадії проектування та забезпечується на стадії виробництва. Недосконаліть технології виробництва та порушення режимів експлуатації можуть спричинити появу різного роду дефектів у готових системах. Таким чином, діагностування технічного об'єкта (системи) обов'язково має бути присутнім на всіх етапах його життєвого циклу. Тому, різноманітні роботи щодо забезпечення процесу діагностування технічної системи проводяться при її розробці, виготовленні, випробовуваннях та експлуатації. При цьому мета діагностування полягає у підтриманні необхідного рівня показників технічного стану системи. На стадії проектування основною задачею діагностування є забезпечення можливості потенціального діагностування системи, що проектується, а на стадії виробництва та експлуатації — поточний контроль її працездатності. Постійне зростання складності технічних систем, пов'язане зі збільшенням та ускладненням виконуваних функцій, удосконаленням технології виробництва, підвищенням вимог до показників якості тощо, призводить до ускладнення методів та засобів діагностування, які забезпечують необхідні властивості систем. Для діагностування електротехнічних пристроїв використовуються такі методи як: периферійне сканування, технологія автоматичної генерації зразків, вбудоване само сканування, а також методи параметричної ідентифікації, методи контролю несправностей, методи оцінювання тощо. Багатьом з цих методів притаманні наступні недоліки: значний обсяг обчислень, необхідність доступу до всіх вузлів електричної схеми, чутливість до похибок обчислень, і, як наслідок — складність практичної реалізації. Крім того, значне поширення при діагностуванні електротехнічних пристроїв набув метод довідників, заснований на віднаходженні з множини значень напруг або струмів в контрольних точках тих з них, які ближчі за все до значень, отриманих при вимірюванні в пристрої, що діагностується. Незважаючи на значні досягнення в області діагностування технічного стану систем, на теперішній час визначальною залишається актуальність теоретичних досліджень та практичного застосування методів діагностування як основи щодо забезпечення необхідних показників якості систем (і електротехнічних, зокрема) та підвищення достовірності оцінок технічного стану останніх. Розглянуто та досліджено умови незалежних спостереження та управління, які забезпечують можливість проведення діагностичного експерименту без виведення контрольованої системи з експлуатації.

Ключові слова. Діагностування, діагностичний експеримент, методи діагностики, умови працездатності, незалежне спостереження, незалежне управління, технічна система.

Вступ. Діагностування працездатного стану технічних, зокрема електротехнічних пристроїв (ЕП) різного призначення являє собою важливу наукову та прикладну задачу. В постановочному плані і в процесі реалізації дана задача суттєво ускладнюється необхідністю отримання оцінок стану об'єкта, що діагностується, безпосередньо в робочих режимах роботи. Особливо актуально вказаний аспект рішення задачі діагностування полягає для пристроїв, які не підлягають виведенню з експлуатації. Наприклад, це стосується елементів аварійної сигналізації; компонентів

диспетчерського управління, що не мають резервування, а також пристроїв, які працюють у автономному режимі (зокрема, зонди атмосферного та водного простору) тощо.

Відомі на поточний час методи функціонування та тестового діагностування характеризуються низкою суттєвих недоліків. Так, методи функціонального діагностування [1— 8] обмежені можливістю проведення діагностичного експерименту (наприклад, через необхідність формування на вході об'єкта довільного тестового сигналу), що суттєво знижує ефективність діагностування. Методи тестового діагностування [9, 10], в свою чергу, потребують виведення з експлуатації об'єкт, який діагностується, що не дозволяє використовувати дані методи безпосередньо в ході робочого циклу. Зазначені недоліки призводять до необхідності розвитку методів діагностування, які забезпечують, з одного боку — максимальну повноту отримуваної оцінки результату діагностування, а з іншого боку — проведення діагностичного експерименту безпосередньо в процесі експлуатації об'єкта, в якості якого може розглядатися широкий клас ЕП.

Мета роботи. Визначення умов незалежних спостереження та управління при проведенні діагностичного експерименту для ЕП, які являють собою безінерційні системи (підсистеми) або системи, опис яких формалізовано у вигляді передаточних функцій.

Основна частина. При розв'язуванні задач діагностування за звичай [11, 12] розглядаються окремо об'єкти діагностування зі *спрямованим* (системи) та *не спрямованим* (ланцюги) розповсюдженням сигналів. До перших відносяться, наприклад, неперервні системи управління, а до других — електричні ланцюги. В практичних додатках значне поширення набули безінерційні системи, час перехідних процесів в яких $\tau_{\text{пп}} \to 0$. Саме поширеність безінерційних систем зумовлює інтерес до їх діагностування.

1. Діагностування підсистем в безінерційних системах, які мають властивість незалежного спостереження. Розглянемо безінерційні системи, у яких залежність вихідного сигналу системи від вихідних сигналів підсистем, що перевіряються (діагностуються) лінійна. В цьому випадку опис систем зі справною підсистемою S_j можна представити наступним чином:

$$\mathbf{y} = A(\mathbf{u}) + \mathbf{L}_j(\mathbf{u})\,\Delta\mathbf{Z}_j, \tag{1}$$

де $\mathbf{y}$ — сигнал на виході несправної системи; $\mathbf{u}$ — сигнал на вході несправної системи; A — оператор, який описує справну систему; $\mathbf{L}_j(\mathbf{u}) = \partial\mathbf{y}/\partial\mathbf{Z}_j$ — матриця функцій чутливості; $\Delta Z_j = \mathbf{Z}_j - \mathbf{Z}_j^*$ — зміна сигналу на виході несправної підсистеми у порівнянні з її справним станом при одному й тому ж сигналі на вході.

З викладеного вище можна записати

$$\Delta y = \mathbf{L}_j(\mathbf{u})\,\Delta Z_j. \tag{2}$$

Несправна система є спостережною тоді і тільки тоді, коли існує таке $\mathbf{u}$, що

$$\text{rang}\mathbf{L}_j(\mathbf{u}) = n_j,$$

де n_j — розмірність вектора $\mathbf{Z}_j$.

Пошук несправної підсистеми здійснюється послідовною перевіркою гіпотез H_i:

$$\Delta y = \mathbf{L}_i(\mathbf{u})\,\Delta Z_i;\ i = \overline{1,N}, \tag{3}$$

де N — число підсхем, які перевіряються.

Рівняння (3) являє собою діагностичне рівняння при перевірці гіпотези H_i. Перевірка гіпотези H_i полягає у перевірці спільності рівнянь (3). Якщо рівняння (3)

спільні, то гіпотеза H_i приймається, і підсистема S_i вважається несправною. Якщо рівняння (3) неспільні, то гіпотеза H_i не приймається та перевіряється чергова гіпотеза.

Підсистеми S_i, S_j не є такими, що розрізняються, в тому і тільки тому випадку, якщо при несправній підсистемі S_j існує таке значення ΔZ_i, що

$$\mathbf{L}_i(\mathbf{u})\,\Delta\mathbf{Z}_i = \mathbf{L}_j(\mathbf{u})\,\Delta\mathbf{Z}_j, \tag{4}$$

тобто для $\forall\mathbf{u}$ та $\forall\Delta\mathbf{Z}_j$ $\exists\Delta\mathbf{Z}_i$ таке, що $\mathbf{L}_i(\mathbf{u})\,\Delta\mathbf{Z}_i = \mathbf{L}_j(\mathbf{u})\,\Delta\mathbf{Z}_j$.

Аналіз умов, при яких не виконується рівність (4) дозволяє встановити критерії, за якими підсистеми не розрізняються.

Визначення 1.1. Підсистеми S_i, S_j називаються підсистемами з *незалежним спостереженням* при гіпотезі H_i, якщо підсистема S_i є спостережною та існує таке $\mathbf{u}$, що умова (4) не виконується для всіх ΔZ_i та ΔZ_j, тобто

$$\exists\mathbf{u},\ \forall\Delta Z_i\ \ \forall\Delta Z_j\ \ \mathbf{L}_i(\mathbf{u})\,\Delta Z_i \neq \mathbf{L}_j(\mathbf{u})\,\Delta Z_j.$$

Підсистеми S_i, S_j мають незалежні спостереження при гіпотезі H_i в тому і лише в тому випадку, якщо існує таке значення $\mathbf{u}$, що

$$\operatorname{rang}\left[\mathbf{L}_i(\mathbf{u}) \vdots \mathbf{L}_j(\mathbf{u})\right] = n + \operatorname{rang}\left[\mathbf{L}_j(\mathbf{u})\right]. \tag{5}$$

Доведення. Розглянемо наступні лінійні простори

$$P_i = \{\Delta Z_i\},\ P_j = \{\Delta Z_j\},$$

які за допомогою операторів $\mathbf{L}_i(\mathbf{u})$ та $\mathbf{L}_j(\mathbf{u})$ відображуються в просторах Q_i та Q_j

$$\mathbf{L}_i(\mathbf{u}):\ P_i \to Q_i,\ \ \mathbf{L}_j(\mathbf{u}):\ P_j \to Q_j.$$

Очевидно, виходячи з властивостей лінійних операторів, можна стверджувати, що

$$\dim P_i = n_i;\ \dim P_j = n_j,$$

$$\dim Q_i = \operatorname{rang}\left[\mathbf{L}_i(\mathbf{u})\right];\ \dim Q_j = \operatorname{rang}\left[\mathbf{L}_j(\mathbf{u})\right].$$

Розглянемо простір P векторів $\left[\Delta\mathbf{Z}_i^T \vdots \Delta\mathbf{Z}_j^T\right]^T$ та оператор $\mathbf{L}(\mathbf{u}) = \left[\mathbf{L}_i(\mathbf{u}) \vdots \mathbf{L}_j(\mathbf{u})\right]$, який здійснює відображення

$$\mathbf{L}(\mathbf{u}):\ P \to Q,$$

звідки маємо

$$\dim Q = \operatorname{rang}\left[\mathbf{L}(\mathbf{u})\right].$$

Легко можна показати, що

$$Q_i \subset Q \text{ та } Q_j \subset Q.$$

Таким чином, маємо

$$\dim Q \le \dim Q_i + \dim Q_j.$$

Нехай

$$\forall\Delta Z_i\ \ \forall\Delta Z_j\ \ \mathbf{L}_i(\mathbf{u})\,\Delta Z_i = \mathbf{L}_j(\mathbf{u})\,\Delta Z_j.$$

тобто підсистеми S_i, S_j є такими, що спостерігаються незалежно.

Тоді $Q_i \bigcap Q_j = \{0\}$.

Тобто, справедливо сувора рівність

$$\dim Q = \dim Q_i + \dim Q_j,$$

а це означає, що

$$\operatorname{rang}\left[\mathbf{L}(\mathbf{u})\right] = \operatorname{rang}\left[\mathbf{L}_i(\mathbf{u})\right] + \operatorname{rang}\left[\mathbf{L}_j(\mathbf{u})\right].$$

Враховуючи, що $\text{rang}\left[\mathbf{L}_i(\mathbf{u})\right]=n_i$ отримаємо

$$\mathbf{L}(\mathbf{u})=n_i+\text{rang}\left[\mathbf{L}_j(\mathbf{u})\right]$$

і навпаки, якщо

$$\text{rang}\left[\mathbf{L}(\mathbf{u})\right]=\text{rang}\left[\mathbf{L}_i(\mathbf{u})\right]+\text{rang}\left[\mathbf{L}_j(\mathbf{u})\right],$$
$$\dim Q=\dim Q_i+\dim Q_j$$

то, відповідно

$$Q_i\bigcap Q_j=\{0\},$$

а, значить, виконується нерівність

$$\forall\Delta Z_i\ \ \forall\Delta Z_j\ \ \mathbf{L}_i(\mathbf{u})\Delta Z_i\neq\mathbf{L}_j(\mathbf{u})\Delta Z_j.$$

Для забезпечення властивості незалежного спостереження підсистем S_i, S_j в загальному випадку необхідно n_i+n_j контрольних точок. Одначе вектори ΔZ_i та ΔZ_j можуть бути лінійно незалежними (з урахуванням конкретного значення ΔZ_j) при $n+1$ в контрольній точці, якщо виконується умова [13]

$$\text{rang}\left[\mathbf{L}_i(\mathbf{u}_k)\ \vdots\ \mathbf{l}_{j,k}(\mathbf{u}_k)\right]=n_i+1;\ \ k=\overline{1,n_j},\ (6)$$

де $\mathbf{l}_{j,k}$ — k-й стовпчик матриці $\mathbf{L}_j(\mathbf{u})$.

Якщо матриці $\mathbf{L}_i(\mathbf{u})$, $\mathbf{L}_j(\mathbf{u})$ є функціями сигналів на виході системи і можуть змінюватися в процесі діагностичного експерименту, то вірогідність появи для різних значень $\mathbf{u}$ таких значень ΔZ_j, що за умови (6) вектор $\mathbf{L}_j(\mathbf{u})\Delta Z_j$ є лінійно залежним з матрицею $\mathbf{L}_i(\mathbf{u})$ мала. Якщо цією вірогідністю можна знехтувати (що на практиці часто має місце), то умову (6) можна прийняти в якості критерію незалежності спостережень підсистем.

Справедливим можна вважати наступне твердження [12]: якщо підсистеми S_i, S_j мають незалежні спостереження, то вони є такими, що розрізняються.

Процедура діагностування підсистем, що спостерігаються незалежно, полягає у перевірці спільності систем діагностичних рівнянь, що відповідають гіпотезам, які перевіряються. Якщо система діагностичних рівнянь спільна, то відповідна їй гіпотеза приймається, якщо не спільна — відкидається.

2. Діагностування систем, які задано передаточними функціями. При описі систем широко застосовується апарат передаточних функцій. Щодо задач діагностування будемо мати на увазі наступне.

Нехай справну систему задано у вигляді структурної схеми. Будемо розглядати підсистеми, які мають скалярними входом та виходом, залежність між якими описується відомою передаточною функцією виду $W(p)=Z_i(p)/V_i(p)$, де $Z_i(p)$, $V_i(p)$ — зображення за Лапласом сигналу $Z_i(t)$ на виході та сигналу $V_i(t)$ на вході підсистеми.

Будемо вважати, що несправності можливі лише тільки в одній підсистемі, несправність змінює передаточну функцію підсистеми на невідому залежність між її входом та виходом. В частковому випадку несправна підсистема може описуватися невідомою передаточною функцією. Тоді несправності не виводять систему, що діагностується, з класу лінійних систем.

Задача полягає в тому, щоб маючи опис справної системи та наявними реалізаціями вхідних та вихідних сигналів системи, що діагностується, визначити несправну підсистему.

Підсистеми у лінійній системі при структурних несправностях можуть мати тільки дві з трьох діагностичних властивостей: *незалежними спостереженнями* та

незалежними управліннями. Тому аналіз властивість бути діагностованою для підсистеми зводиться до визначення цих властивостей у різноманітних пар підсистем. Для підсистем, які володіють якоюсь властивістю, використовується відповідний метод діагностування.

Спочатку розглянемо підсистеми з *незалежним спостереженням*. Передаточну функцію від виходу $Z_i(p)$ несправної підсистеми S_i до виходу всієї системи y_k (як і раніше — скалярної величини) позначимо як $W_{i,к}$ (для спрощення запису тут, і у подальшому, крім обумовлених випадків, символом p, що позначає зображення при запису передаточних функцій, будемо нехтувати).

Залежність вихідного сигналу всієї системи від вихідного сигналу підсистеми S_i має вигляд

$$y_к(p) = W_{i,к}\, Z_i(p),\ \ k = \overline{1,n}.$$

Несправна підсистема S_i є такою, що спостерігається, в тому і лише в тому випадку, якщо існує вихід системи y_k, відносно якого передаточна функція $W_{i,к}$ має зворотну $W_{i,к}^{-1}$. Підсистеми S_i та S_j є такими, що не розрізняються при гіпотезі H_i, лише в тому випадку, якщо при несправній підсистемі S_j існує таке значення ΔZ_i, що

$$L_i(u)\Delta Z_i = L_j(u)\Delta Z_j,\ \ u \in D_u,$$

де оператори L_i та L_j задають класи несправностей в підсистемах S_i та S_j, відповідно.

Останнє рівняння для випадку опису підсистеми у вигляді передаточних функцій записується наступним чином:

$$\begin{bmatrix} W_{i,1} \\ \vdots \\ W_{i,n} \end{bmatrix} \mathrm{Z}_i(p) = \begin{bmatrix} W_{j,1} \\ \vdots \\ W_{j,n} \end{bmatrix} \mathrm{Z}_j(p). \qquad (7)$$

Твердження 2.1. Підсистеми S_i та S_j мають незалежні спостереження відносно деяких виходів системи Z_a, Z_δ при гіпотезі H_i, якщо підсистема S_i є такою, що спостерігається та

$$W_{i,\mathrm{a}}\, W_{j,\delta} \neq W_{j,\mathrm{a}}\, W_{i,\delta}. \qquad (8)$$

Доведення. Слід довести, що при заданому $Z_j(p)$ не існує $Z_i(p)$, яке задовольняє рівності (7).

Оскільки S_i є такою, що спостерігається, то хоча б для однієї передаточної функції $W_{i,\mathrm{a}}$, $W_{i,\delta}$ існує зворотна функція. Нехай існує $W_{i,\mathrm{a}}^{-1}$. Тоді з (8) отримаємо

$$Z_i(p) = W_{i,\mathrm{a}}^{-1}\, W_{j,\mathrm{a}}\, Z_j(p). \qquad (9)$$

Очевидно, що значення $Z_i(p)$, яке отримано відносно виходу Z_a, повинно задовольняти і рівнянню, яке відповідає виходу системи Z_δ (δ-й рядок системи рівнянь (7)). Підставимо (9) в δ-й рядок (7), тоді

$$W_{i,\delta}\, W_{i,\mathrm{a}}^{-1}\, W_{j,\mathrm{a}}\, Z_j(p) = W_{j,\delta}\, Z_j(p). \qquad (10)$$

Рівність (10) існує тільки у тому випадку, якщо $W_{i,\delta}\, W_{i,\mathrm{a}}^{-1}\, W_{j,\mathrm{a}} = W_{j,\delta}$ або $W_{i,\delta}\, W_{j,\mathrm{a}} = W_{i,\mathrm{a}}\, W_{j,\delta}$. Але ця рівність відповідно до умови (8) не існує, тобто, не виконується і рівність (10), тобто при заданому $Z_j(p)$ не існує значення $Z_i(p)$, яке задовольняє виразу (7).

Незалежність спостережень підсистем зумовлюється структурою та параметрами системи. Для систем, заданих передаточними функціями, зручно спочатку

провести аналіз системи в символьному вигляді. При цьому передаточні функції виразу (8) визначаються у загальному вигляді відповідно до алгебри структурних схем по передаточних функціях, заданих символами $W_1,\ldots,W_n$. Аналіз в символьному вигляді дозволяє поставити необхідні умови лінійної незалежності спостережень підсистем та достатні умови їх залежності.

Якщо встановлено, що умова (8) при символьному аналізі виконується, то слід цю умову перевірити для конкретних моделей підсистем, що дозволяє остаточно встановити незалежність спостережень підсистем.

Якщо при символьному аналізі умова (8) не виконується, то підсистеми S_i та S_j мають незалежні спостереження і подальший аналіз не проводиться.

Очевидно, що підсистеми с незалежним спостереженням є такими, що розрізняються для широкого класу несправностей, причому, метод діагностування підсистем с незалежним спостереженням полягає у перевірці сумісності системи діагностичних рівнянь, складеної для кожної з гіпотез.

Далі розглянемо підсистеми з *незалежним управлінням*. Нехай система, що діагностується, має m входів та один вихід. Як і раніше, будемо розглядати підсистеми зі скалярними входом та виходом.

Передаточну функцію від входу системи $u_к(p)$ до входу $V_i(p)$ несправної підсистеми S_i позначимо через $V_{i,к}(p)$ (далі використовується позначення $V_{i,к}$, в силу зробленого вище зауваження), для якої приймемо $V_{i,k}=(V_{i,1},\ldots,V_{i,m})$. В справній частині системи виділимо, в свою чергу, підсистему S_j. Передаточну функцію від входу системи $u_к(p)$ до входу цієї підсистеми $V_j(p)$ позначимо через $V^i_{j,к}$, де $V^i_{j,k}=(V^i_{j,1},\ldots,V^i_{j,m})$.

Варіацію вхідних сигналів системи $\Delta u(p)$, що забезпечує варіацію вхідного сигналу підсистеми S_i при незмінному вхідному сигналі підсистеми S_j при гіпотезі H_i, отримаємо з системи рівнянь

$$\begin{bmatrix}\Delta V_i(p)=0\\ \Delta V_j(p)\neq 0\end{bmatrix}=\begin{bmatrix}V_i\\ V^i_j\end{bmatrix}\Delta u(p) \tag{11}$$

при умові, що

$$\text{ранг}\begin{bmatrix}V_i\\ V^i_j\end{bmatrix}=2. \tag{12}$$

Для проведення подальших розмірковувань, зазначимо, що дієвим шляхом локалізації несправних підсистем може розглядатися метод *навчаючих* та *перевірочних* характеристик (метод НПХ) [13 — 16]. Пошук несправної підсистеми за допомогою методу НПХ зводиться до почергового розгляду гіпотез H_i щодо несправності підсистеми S_i. Якщо деяка гіпотеза H_i приймається, то підсистема S_i вважається несправною.

Для перевірки гіпотези H_i виділяються *навчаючі* $N_{\text{навч}}$ та *перевірочні* $N_{\text{пер}}$ множини контрольованих сигналів, що задовольняють умові:

$$N_{\text{навч}}\bigcap N_{\text{пер}}\neq N_{\text{пер}}.$$

Надалі скористаємося застосуванням методу НПХ щодо розгляду властивостей незалежних спостереження та управління при діагностуванні підсистем ЕП.

Тоді, перед перевіркою гіпотези H_i запишемо $u^{\text{пер}}(p)=u^{\text{навч}}(p)+\Delta u(p)$. Значення $\Delta u(p)$ визначається з системи рівнянь (2.21) для заданого значення $\Delta V_{\text{j}}(p)$.

Процедура перевірки гіпотези H_i наступна.

1. При $u^{\text{навч}}(p)$ визначається $\Delta y^{\text{навч}}(p)$.

2. Система встановлюється у вихідний початковий стан і при $u^{\text{пер}}(p)$ визначається $y^{\text{пер}}(p)$.

3. Якщо $\Delta y^{\text{пер}}(p) = \Delta y^{\text{навч}}(p)$, то гіпотеза H_i приймається і підсистема S_i вважається несправною.

Приклад 2.1. Нехай підсистеми $S_1,\ldots,\ S_4$ деякої системи, що діагностується, описуються передаточними функціями:

$$W_1 = 1/p,\ W_2 = 2/p^2,\ W_3 = 2,\ W_4 = 3.$$

Несправною може бути одна з підсистем, опис якої змінюється непередбачуваним чином. Вважаємо, що є можливість встановлення несправної підсистеми в деякий початковий стан. В даному випадку початковий стан справних підсистем — нульовий, несправної підсистеми — довільний. постійний. Слід, маючи вхідні та вихідні сигнали системи, визначити несправну підсистему в режимі тестового діагностування.

Дослідимо незалежність управлінь (властивість розрізнювання) підсистем $S_1,\ \ldots,\ S_4$. Властивість розрізнювання при гіпотезі H_i встановлюється шляхом аналізу залежності вхідних сигналів підсистем при віддаленій підсистемі S_i. Аналіз незалежності управлінь підсистем проведемо в символьному вигляді. Таке дослідження дозволяє встановити достатні умови залежності управлінь підсистем та необхідні умови їх незалежності. Остаточно незалежність управлінь встановлюється заміною позначень передаточних функцій конкретними залежностями.

При гіпотезі H_1 (видаляється підсистема S_1)

$$V_{1,1} = 1,\ V_{1,2} = 0,\ V^1_{2,1} = 0,\ V^1_{2,2} = \frac{1}{1 - W_2\, W_3\, W_4},$$

$$V^1_{3,1} = 0,\ V^1_{3,2} = \frac{W_2}{1 - W_2 W_3 W_4},\ V^1_{4,1} = 0,\ V^1_{4,2} = \frac{W_2 W_3}{1 - W_2\, W_3\, W_4}.$$

Маємо $V_{1,1} V^1_{k,2} \neq V_{1,2}\, V^1_{k,1},\ k = \overline{2,4}$, тобто, виконується (12) і підсистеми в парах $S_1 - S_k$, $k = \overline{2,4}$ мають незалежні управління. Оскільки в матрицях $\begin{bmatrix} V_{1,1} & V_{1,2} \\ V^1_{k,1} & V^1_{k,2} \end{bmatrix}$, $k = \overline{2,4}$ є нульові елементи $\left(V_{1,2} = V^1_{2,1} = V^1_{3,1} = V^1_{4,1} = 0\right)$, то незалежність управлінь зумовлюється структурою схеми і зберігається при будь-якому описі підсистем. Таким чином, якщо гіпотеза H_1 приймається, то несправна підсистема S_1, якщо не приймається $(\overline{H}_1)$, то слід перевірити підсистеми S_2, S_3, S_4.

Аналогічним чином при гіпотезі H_2 отримуємо:

$V^2_{1,1} = 1, V^2_{1,2} = 0$: $V^2_{3,1} = W_1,\ V^2_{3,4} = V^2_{4,2} = 0,\ V^2_{4,1} = W_1 W_3.$

$V_{2,1} = W_1\ W_2\ W_3,\ V_{2,2} = 1,$

Маємо $V_{2,1} V^2_{k,2} \neq V_{2,2} V^2_{k,1},\ k = 1,3,4$. Тобто, при перевірці гіпотези H_2 множина підсистем розбивається на дві підмножини: $\{S_2\}$ — якщо гіпотеза H_2 приймається, $\{S_1, S_3, S_4\}$ — якщо не приймається.

При гіпотезі H_3 отримуємо $V^3_{1,1} = 1$, $V^3_{1,2} = V^3_{2,1} = V^3_{4,1} = V^3_{4,2} = 0$, $V^3_{2,2} = 1, V_{3,1} = W_1$, $V_{3,2} = W_2$. Оскільки $V^3_{4,1} = V^3_{4,2} = 0$, то підсистема S_4 при гіпотезі H_3 не має управлінь, а

підсистеми S_3, S_4 — є такими, що не розрізняються. Цей же висновок витікає з рівності $V_{3,1}V_{4,2}^3 = V_{3,2}V_{4,1}^3$. Підсистеми в парах $S_3 - S_1$, $S_3 - S_2$ мають незалежні управління і, таким чином, їх можна розрізнити, оскільки $V_{3,1}V_{1,2}^3 \neq V_{3,2}V_{4,1}^3$, $V_{3,1}V_{2,2}^3 \neq V_{3,2}V_{2,1}^3$. При перевірці гіпотези отримаємо наступне розбиття множини підсистем: $\{S_3, S_4\}$ — якщо гіпотеза H_3 приймається, $\{S_1, S_2\}$ — якщо не приймається.

Модель справної системи

$$y^*(p) = \frac{W_1 W_3}{1 - W_2 W_3 W_4} u_1(\rho) + \frac{W_2 W_3}{1 - W_2 W_3 W_4};$$

$$u_2(p) = \frac{2p}{p^2 - 12} u_1(p) + \frac{4}{p^2 - 12} u_2(p).$$

Несправна система описується залежністю (нам невідомою)

$$y(p) = \frac{W_1 W_3}{1 - \widetilde{W}_2 W_3 W_4} u_1(p) + \frac{\widetilde{W}_2 W_3}{1 - \widetilde{W}_2 W_3 W_4};$$

$$u_2(p) = \frac{2p^2}{p^2 - 6} u_1(p) + \frac{2}{p^3 - 6} u_2(p).$$

$$\Delta y(p) =$$

$$= y(p) - y^*(p) = \frac{2p}{p^5 - 12p^3 - 6p^2 + 72} \times \times \left[(-12p + 6)u_1(p) + (-2p^2 + p)u_2(p)\right].$$

Перевіримо гіпотезу H_3. Всі розрахунки будемо перевіряти в просторі зображень перетворень по Лапласу.

Варіацію вхідних сигналів системи, які забезпечують незмінність вхідних сигналів підсистеми S_3 і варіацію вхідних сигналів підсистеми S_1, отримаємо з системи рівнянь

$$\begin{bmatrix} \Delta V_3(p) = 0 \\ \Delta V_1(p) = \dfrac{2}{p^2} \end{bmatrix} = \begin{bmatrix} V_{3,1} & V_{3,2} \\ V_{1,1}^3 & V_{1,2}^3 \end{bmatrix} \times \begin{bmatrix} \Delta u_1(p) \\ \Delta u_2(p) \end{bmatrix} = = \begin{bmatrix} \dfrac{1}{p} & \dfrac{2}{p^2} \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} \Delta u_1(p) \\ \Delta u_2(p) \end{bmatrix}.$$

Маємо $\Delta u_1(p) = \dfrac{2}{p^2}$, $\Delta u_2(p) = -\dfrac{1}{p}$.

Задавши $u_1^{\text{навч}}(p) = 1/\rho$, $u_2^{\text{навч}}(\rho) = 2/\rho$, отримаємо

$$u_1^{\text{пер}}(p) = u_1^{\text{навч}}(p) + \Delta u_1(p) = (p + 2)/p, \quad u_2^{\text{пер}} = 1/\rho.$$

Процедура перевірки гіпотези H_3 наступна.

1. При $u^{\text{навч}}(p)$ отримаємо $\Delta y^{\text{навч}}(p) = = \dfrac{-8p^4 - 20p^3 + 12}{p^5 - 12p^3 - 6p^2 + 72}$.

2. Встановивши систему в вихідний початковий стан, при $u^{\text{пер}}(p)$ отримаємо

$$\Delta y^{\text{пер}}(p) = \frac{-4p^3 - 22p^2 - 36p + 24}{p^6 - 12p^4 - 6p^3 + 72p}.$$

3. Оскільки $\Delta y^{\text{пер}}(p) \neq \Delta y^{\text{навч}}(p)$, то гіпотеза H_3 не приймається, і на несправність підозрюються підсистеми S_1, ,S_2.

Аналогічним чином перевіряються гіпотези H_1, H_2. З них приймається тільки гіпотеза H_2 і підсистема S_2 вважається несправною.

Якщо в підсистемах допускаються лише параметричні несправності, то процедура діагностування полягає в перевірці сумісності перевизначеної системи діагностичних рівнянь, які складено відносно параметрів підсистеми. Яка перевіряється. Перевизначена система діагностичних рівнянь формується відповідним вибором контрольних точок або вхідних сигналів системи. Якщо підсхеми мають незалежні спостереження або управління, то можна спочатку визначити несправну підсистему, а потім оцінити значення її параметрів.

3. Діагностування лінійних систем в просторі станів. Представлення динамічних систем в просторі станів з дискретними змінними дозволяє провести формалізацію процедур аналізу та діагностування складних багатовимірних замкнутих систем, зручну для числової реалізації засобами обчислювальної техніки та, крім того, дозволяє з єдиних позицій розглядати лінійні та нелінійні системи, а також стаціонарні та нестаціонарні системи.

Проблема, яка виникає при числовому аналізі та діагностуванні динамічних систем, полягає в урахуванні затримок сигналів від виходів підсистеми до виходів системи в цілому. Вона (проблема) вирішується виділенням шляхів проходження сигналів від виходів підсистеми, яка діагностується, та виходом системи на кожному такті реалізації рівнянь, що описують систему.

3.1. Підсистеми з незалежним спостереженням. Дамо спочатку постановку задачі діагностування систем з *незалежним спостереженням* при її формалізації у просторі станів.

Постановка задачі. Справна система, що діагностується, описується рівняннями

$$\mathbf{X}^*(k+1) = \mathbf{A}\,\mathbf{X}^*(k) + \mathbf{B}\,\mathbf{u}(k),$$

$$\mathbf{X}^*(0) = \mathbf{X}_0^*, \tag{13}$$

$$\mathbf{y}^*(k) = \mathbf{C}\,\mathbf{X}^*(k), \tag{14}$$

де $\mathbf{X}^*$ — вектор стану системи розмірності n; $\mathbf{u}$, $\mathbf{y}^*$ — вектори вхідних та вихідних сигналів, що вимірюються, відповідно; $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ — відомі матриці відповідно розмірностей $n\times n$, $n\times q$, $r\times n$; k — номер рівняння в системі (13).

В системі, що діагностується, може бути виділено підсистеми, кожна з яких описується певною сукупністю рівнянь з системи рівнянь (13).

Одна з підсистем може бути несправною. В результаті несправностей підсистема може стати нелінійною, нестаціонарною, змінити свій порядок та початковий стан. Необхідно, маючи за наявні моделі (13) та (14), сигнали на вході та виході системи, що діагностується, визначити несправну підсистему.

Модель несправної системи. Несправну систему представимо такою, що складається зі справної та несправної підсистем. Несправна підсистема описується невідомою залежністю $\mathbf{Z}_{\mathrm{i}}(k+1) = f_{\mathrm{i}}[\mathbf{V}_{\mathrm{i}}(k)]$, де $\mathbf{Z}_i$, $\mathbf{V}_i$ — вектори сигналів на вході та виході підсистеми відповідно розмірностей r_i та m_i.

Для опису справної підсистеми видалимо з системи рівнянь (13) рівняння, що описують підсистему S_i. Крім того, виділимо шляхи проходження сигналів на виході справної та несправної підсистем. При цьому матриця $\mathbf{A}$ перетворюється в матриці $\mathbf{A}_i$, $\mathbf{N}_i$, а матриця $\mathbf{C}$ — в матриці $\mathbf{C}_i$, $\mathbf{P}_i$.

Нехай (для конкретності подальших розмірковувань) справна частина системи описується наступним чином:

$$\left.\begin{aligned}
\mathbf{X}_i(k+1) &= \mathbf{A}_i\,\mathbf{X}_i(k) + \mathbf{N}_i\,\mathbf{Z}_i(k) + \mathbf{B}_i\,\mathbf{u}(k),\\
\mathbf{V}_i(k) &= \mathbf{R}_i\,\mathbf{X}_i(k) + \mathbf{G}_i\,\mathbf{u}(k),\\
\mathbf{Y}_i(k) &= \mathbf{C}_i\,\mathbf{X}_i(k) + \mathbf{P}_i\,\mathbf{Z}_i(k),
\end{aligned}\right\}, \tag{15}$$

де $\mathbf{X}_i$ — вектор змінних стану справної підсистеми, $\mathbf{Y}_i$ — вектор сигналів системи на виході при несправній підсистемі S_i.

Вектор $\mathbf{X}_i$ сформовано з $\mathbf{X}^*$ заміною нулями компонент, що відповідають змінним стану справної підсистеми S_i. Вектор $\mathbf{Z}_i$ сформовано з вектору $\mathbf{X}^*$ заміною нулями компонент, що не є змінними на виході справної підсистеми S_i (вихідні сигнали справної підсистеми S_i в нашому випадку являють собою компоненти вектору змінних стану $\mathbf{X}^*$).

Формально матриці $\mathbf{A}_i$, $\mathbf{N}_i$ можна отримати з матриць $\mathbf{A}$, а $\mathbf{B}_i$ з $\mathbf{B}$ заміною нулями рядків, що описують справну підсистему S_i. Крім того, в матриці $\mathbf{A}_i$ нулями замінено всі стовпчики, елементи яких не являють собою співмножники змінних стану $\mathbf{X}_i$ справної підсистеми, в матриці $\mathbf{N}_i$ нулями замінено всі стовпчики, елементи яких не являють собою співмножники вектору змінних $\mathbf{Z}_i$.

Матрицю $\mathbf{C}_i$ отримано з матриці $\mathbf{C}$ заміною нулями стовпців, елементи яких не є співмножниками вектору змінних стану $\mathbf{X}_i$, а матрицю $\mathbf{P}_i$ отримано з матриці $\mathbf{C}$ заміною нулями стовпців, елементи яких не є співмножниками вектору змінних $\mathbf{Z}_i$.

Матриця $\mathbf{R}_i$, $m_i \times n$, виділяє з $\mathbf{X}_i$ (у відповідних клітинках матриці стоять одиниці) компоненти, які є сигналами на вході несправної підсистеми S_i.

Матриця $\mathbf{G}_i$, $m_i \times q$, виділяє з $\mathbf{u}$ у відповідних клітинках матриці стоять одиниці) компоненти, які є сигналами на вході справної підсистеми S_i.

В описі справної підсистеми несправної системи вектори та матриці формуються заміною нулями компонент, а не їх видаленням з первинних векторів та матриць для того, щоб спростити дотримання розмірностей при аналізі в матричному вигляді.

Властивості спостереження та розрізнення підсистем.

Визначення 3.1. Несправну підсистему S_i будемо називати такою, що має *властивість спостереження*, якщо за вимірюваннями сигналів на вході та виході системи можна визначити сигнал на її виході $\mathbf{Z}_i(0)$.

Можливі дві ситуації:

– початковий стан справної системи відомий;

– початковий стан справної системи невідомий (стан несправної підсистеми завжди відомий).

Отримаємо критерій можливості спостереження несправної підсистеми S_i при відомому початковому стані $\mathbf{X}_i(0)$ справної системи.

Як витікає з (15), вихідні сигнали системи з несправною підсистемою S_i визначаються залежністю

$$\begin{bmatrix} Y_i(0) \\ Y_i(1) \\ \vdots \\ Y_i(\upsilon_i) \end{bmatrix} = \begin{bmatrix} C_i \\ C_i A_i \\ \vdots \\ C_i A_i^{\upsilon_i} \end{bmatrix} \mathbf{X}_i(0) + \begin{bmatrix} P_i & & \\ C_i N_i & P_i & \\ \vdots & & \\ C_i A_i^{\upsilon_i - 1} N_i & C_i A_i^{\upsilon_i - 2} \ldots & P_i \end{bmatrix} \times \begin{bmatrix} Z_i(0) \\ Z_i(1) \\ \vdots \\ Z_i(\upsilon_i) \end{bmatrix} + \begin{bmatrix} 0 & & \\ C_i B_i & 0 & \\ \vdots & & \\ C_i A_i^{\upsilon_i - 1} B_i & C_i A_i^{\upsilon_i - 2} B_i \ldots & C_i B_i \end{bmatrix} \times \begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(\upsilon_i - 1) \end{bmatrix}. \quad (16)$$

В матричному вигляді систему рівнянь (16) запишемо, дотримуючись відповідність доданків, наступним чином:

$$\mathbf{\Lambda}_i(\upsilon_i) = \mathbf{\Psi}_i^{(\upsilon_i)} \mathbf{X}_i(0) + \\ + \mathbf{\Phi}_i^{(\upsilon_i)} \boldsymbol{\mu}_i(\upsilon_i) + \boldsymbol{\theta}_i^{(\upsilon_i)} \mathbf{U}(\upsilon_i - 1), \quad (17)$$

де

$$\mathbf{\Lambda}_i(\upsilon_i)=\left[Y_i(0),\ldots,Y_i(\upsilon_i)\right]^{\mathrm{T}},\ \mathbf{\mu}_i(\upsilon_i)=\left[Z_i(0),\ldots,Z_i(\upsilon_i)\right]^{\mathrm{T}},$$
$$\mathbf{U}(\upsilon_i-1)=\left[u(0),\ldots,u(\upsilon_i-1)\right]^{\mathrm{T}}.$$

Оскільки в систему рівнянь для визначення $\mathbf{Z}_i(0)$, яка формується, не повинні входити невідомі значення $\mathbf{Z}_i(k);\ k\geq 1$, то з (16) і (17) необхідно виключити рівняння, які містять $\mathbf{Z}_i(k);\ k\geq 1$. При цьому (17) перетворюється до вигляду:

$$\mathbf{\Lambda}_i(\upsilon_i)=$$
$$=\mathbf{K}_i^{(\upsilon_i)}\mathbf{X}_i(0)+\mathbf{F}_i^{(\upsilon_i)}\mathbf{Z}_i(0)+\mathbf{Q}^{(\upsilon_i)}\mathbf{U}(\upsilon_i-1). \quad (18)$$

Позначимо

$$\mathbf{\Delta}Z_i(0)=\mathbf{\Delta}Z_i(0)-\mathbf{\Delta}Z_i^*(0)\ \text{та}$$
$$\mathbf{\Delta\Lambda}_i(\upsilon_i)=\mathbf{\Lambda}_i(\upsilon_i)-\mathbf{\Lambda}_i^*(\upsilon_i). \quad (19)$$

де $\mathbf{\Lambda}_i^*(\upsilon_i)$ — вектор сигналів на виході справної системи, що визначається шляхом розрахунку або замірів сигналів справного екземпляра системи.

З (18) випливає

$$\mathbf{\Delta\Lambda}_i(\upsilon_i)=\mathbf{F}_i^{(\upsilon_i)}\mathbf{\Delta}Z_i(0). \quad (20)$$

Матрицю $\mathbf{F}_i^{(\upsilon_i)}$ будемо *називати матрицею спостереження* несправної підсистеми S_i. Формально $\mathbf{F}_i^{(\upsilon_i)}$ можна отримати за наступним алгоритмом:

— сформувати матрицю

$$\begin{bmatrix} P_i \\ \hline C_i N_i \\ \hline \vdots \\ \hline C_i A_i^{\upsilon_i-1} N_i \end{bmatrix},$$

— в черговій складовій матриці, яку відділено штриховими лініями, видалити рядки, що відповідають номерам ненульових рядків попередніх складових матриць (в даному випадку для зберігання розмірності матриць з метою забезпечення зручності їх співставлення рядки не видаляються, а замінюються прочерком).

Твердження 3.1. Підсистема S_i є такою, що характеризується властивістю спостереження в тому і тільки в тому випадку, якщо існує таке значення υ_i, що ранг $\mathbf{F}_i^{(\upsilon_i)}=n_i$.

Справедливість твердження витікає з умови можливості розв'язування рівняння (20) відносно $\mathbf{\Delta}Z_i(0)$.

Рівняння, складене відносно величини, яка оцінюється, будемо називати діагностичним. В даному випадку діагностичним є рівняння (20).

Позначимо через H_i гіпотезу про те, що несправною є підсистема S_i. Гіпотеза H_i перевіряється шляхом формування діагностичного рівняння (20) і перевірки його сумісності. Якщо рівняння (20) сумісне, то гіпотеза H_i приймається і підсистема S_i вважається несправною, якщо не сумісне, то гіпотеза H_i не приймається.

Будемо говорити, що підсистеми S_i, S_j є такими, що *не розрізняються*, якщо гіпотеза H_i приймається як при несправній підсистемі S_i, так і при несправній підсистемі S_j.

Рівняння (20) складено відносно $\mathbf{Z}_i(0)$ на відрізку часу $[0,\upsilon_i]$. Для впевненого розпізнавання гіпотези може знадобитися перевірка сумісності діагностичного рівняння, складеного відносно $\mathbf{Z}_i(\eta)$ на відрізку $[\eta,\eta+\upsilon_i]$, $\eta\geq 0$ при $\mathbf{\Delta\Lambda}_i(\eta+\upsilon_i)\neq 0$.

Підсистеми S_i, S_j є такими, що не розрізняються в тому і лише в тому випадку, якщо при несправній підсистемі S_j існує таке значення $\mathbf{Z}_i(0)$, що $\mathbf{\Delta\Lambda}_i(\upsilon_i)=\mathbf{\Delta\Lambda}_{i,j}(\upsilon_i)$, де $\mathbf{\Delta\Lambda}_{i,j}(\upsilon_i)$ — вектор, утворений з компонент вектора сигналів системи на виході з несправною підсистемою S_j, що відповідають компонентам вектора $\mathbf{\Delta\Lambda}_i(\upsilon_i)$.

Вихідні сигнали системи з несправною підсистемою S_j описуються виразом (17) при зміні індексу i на j. При цьому $\mathbf{\Delta\Lambda}_{i,j}(\upsilon_i)$ визначається залежністю

$$\mathbf{\Delta\Lambda}_{i,j}(\upsilon_i)=\mathbf{\Phi}_{j,i}^{(\upsilon_i)}\,\mathbf{\Delta\mu}_i(\upsilon_i), \tag{21}$$

де $\mathbf{\Phi}_{j,i}^{(\upsilon_i)}$ — матриця, отримана з матриці $\mathbf{\Phi}_j^{(\upsilon_i)}$ видаленням рядків, для яких не існує компонент в векторі $\mathbf{\Delta\Lambda}_i(\upsilon_i)$.

С урахуванням (20), (21) рівність $\mathbf{\Delta\Lambda}_i(\upsilon_i)=\mathbf{\Delta\Lambda}_{i,j}(\upsilon_i)$ запишемо у вигляді

$$\mathbf{F}_i^{(\upsilon_i)}\,\mathbf{\Delta}Z_i(0)=\mathbf{\Phi}_{j,i}^{(\upsilon_i)}\,\mathbf{\Delta\mu}_i(\upsilon_i). \tag{22}$$

Твердження 3.2. Підсистеми S_i, S_j є такими, що розрізняються, при гіпотезі H_i, якщо

$$\text{ранг}\left[\mathbf{F}_i^{(\upsilon_i)}\,\middle|\,\mathbf{\Phi}_{j,i}^{(\upsilon_i)}\right]=\eta_{\text{i}}+\text{ранг}\,\mathbf{\Phi}_{j,i}^{(\upsilon_i)}\ . \tag{23}$$

Зазначимо, що матриця $\mathbf{\Phi}_{j,i}^{(\upsilon_i)}$ може мати довільний ранг.

Справедливість твердження витікає з умови лінійної незалежності $\mathbf{\Delta\mu}_i(\upsilon_i)$, $\mathbf{\Delta}Z_i(0)$, що визначається рівністю (22).

Визначення 3.2. Підсистеми S_i, S_j будемо називати підсистемами *з незалежним спостереженням* при гіпотезі H_i, якщо вектори $\mathbf{\Delta\mu}_i(\upsilon_i)$, $\mathbf{\Delta}Z_i(0)$ є лінійно незалежними.

Необхідною і достатньою умовою незалежності спостережень підсистем S_i, S_j, яке забезпечує можливість їх розрізнення при гіпотезі H_i, є умова (23). Одначе, якщо ранг $\left[\mathbf{F}_i^{(\upsilon_i)}\,\middle|\,\mathbf{\Phi}_{j,i}^{(\upsilon_i)}\right]>n_i$, то підсистеми S_i, S_j вже є такими, що розрізняються, для широкого класу несправностей.

Якщо початковий стан несправної підсистеми $\mathbf{X}_i(0)$ невідомий, то при діагностуванні необхідно відновити не тільки $\mathbf{Z}_i(0)$, але й $\mathbf{X}_i(0)$.

Вважаючи невідомими $\mathbf{Z}_i(0)$ та $\mathbf{X}_i(0)$, з (12) отримаємо

$$\mathbf{\Lambda}_i(\upsilon_i)-\mathbf{Q}_i^{(\upsilon_{\text{i}})}\,\mathbf{u}(\upsilon_i-1)=$$
$$=\left[\mathbf{F}_i^{(\upsilon_i)}\,\middle|\,\mathbf{K}_i^{(\upsilon_i)}\right]\times\begin{bmatrix}\mathbf{Z}_i(0)\\ \mathbf{X}_i(0)\end{bmatrix}. \tag{24}$$

З (18) випливає твердження.

Твердження 3.3. При невідомому початковому стані системи несправна підсистема S_i є такою, що спостерігається, в тому і лише в тому випадку, якщо існує значення υ_i таке, що

$$\text{ранг}\left[\mathbf{F}_i^{(\upsilon_i)}\middle|\mathbf{K}_i^{(\upsilon_i)}\right] = n_i + \ell_i,$$

де ℓ_i — ранг матриці $\mathbf{K}_i^{(\upsilon_i)}$, який дорівнює числу змінних стану справної підсистеми.

Гіпотеза H_i перевіряється шляхом перевірки сумісності діагностичного рівняння (24). Аналогічно (23) можна отримати умову розрізнення підсистем S_i, S_j при гіпотезі H_i для умови, коли початковий стан справної системи невідомий.

Твердження 3.4. Підсистеми S_i, S_j є такими, що розрізняються, при гіпотезі H_i, якщо

$$\text{ранг}\left[\mathbf{F}_i^{(\upsilon_i)}\middle|\mathbf{K}_i^{(\upsilon_i)}\middle|\mathbf{\Phi}_{j,i}^{(\upsilon_i)}\middle|\mathbf{\Psi}_{j,i}^{(\upsilon_i)}\right] = n_{\text{i}} + \ell_{\text{i}} + \text{ранг}\,\mathbf{\Phi}_{j,i}^{(\upsilon_i)} + \text{ранг}\,\mathbf{\Psi}_{j,i}^{(\upsilon_i)},$$

де $\mathbf{\Psi}_{j,i}^{(\upsilon_i)}$ формується подібно $\mathbf{\Phi}_{j,i}^{(\upsilon_i)}$ з матриці $\mathbf{\Psi}_j^{(\upsilon_i)}$.

Якщо ранг

$$\left[\mathbf{F}_i^{(\upsilon_i)}\middle|\mathbf{K}_i^{(\upsilon_i)}\middle|\mathbf{\Phi}_{j,i}^{(\upsilon_i)}\middle|\mathbf{\Psi}_{j,i}^{(\upsilon_i)}\right] > n_i + \ell_i,$$

то це дає підставу вважати підсистеми S_i, S_j такими, що розрізняються при гіпотезі H_i для широкого класу несправностей.

3.2. Підсистеми з незалежним управлінням. Вхідні сигнали несправної підсистеми S_i на інтервалі $[0,\eta]$ у відповідності до (15) визначаються залежністю

$$\begin{bmatrix} V_i(0) \\ V_i(1) \\ \vdots \\ V_i(\eta) \end{bmatrix} = \begin{bmatrix} R_i \\ R_i A_i \\ \vdots \\ R_i A_i^{\eta} \end{bmatrix} \mathbf{X}_i(0) + \begin{bmatrix} 0 & & \\ R_i N_i & 0 & \\ \vdots & & \\ R_i A_i^{\eta-1} N_i & R_i A_i^{\eta-2} N_i \ldots R_i N_i & \end{bmatrix} \times \begin{bmatrix} Z_i(0) \\ Z_i(1) \\ \vdots \\ Z_i(\eta) \end{bmatrix} + \begin{bmatrix} 0 & & \\ R_i B_i & G_i & \\ \vdots & & \\ R_i A_i^{\eta-1} B_i & R_i A_i^{\eta-2} B_i \ldots G_i & \end{bmatrix} \times \begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(\eta) \end{bmatrix} \quad (25)$$

В матричному вигляді систему рівнянь (25) запишемо наступним чином:

$$\mathbf{V}_i(\eta) = \mathbf{E}_i^{(\eta)}\,\mathbf{X}_i(0) + \mathbf{\Gamma}_i^{(\eta)}\,\boldsymbol{\mu}_i(\eta-1) + \mathbf{W}_i^{(\eta)}\,\mathbf{U}(\eta) \quad (26)$$

Вхідні сигнали $\mathbf{V}_j(\eta)$ підсистеми S_j при гіпотезі H_i визначаються системою рівнянь (25) при заміні матриць $\mathbf{R}_i$, $\mathbf{G}_i$ на $\mathbf{R}_j$, $\mathbf{G}_j$. При цьому $\mathbf{V}_j(k)$ визначається k-м рівнянням системи (25).

Визначення 3.3. Підсистеми S_i, S_j будемо називати підсистемами з незалежним управлінням при гіпотезі H_i, якщо для кожної компоненти $V_{j,s}(k)$ вектора $\mathbf{V}_j(k)$ існує таке значення $k = k_{\text{s}}$, що змінна $V_{j,s}(k_s)$ лінійно незалежна з вектором $\mathbf{V}_i(\eta)$.

Для лінійно незалежних $V_i(\eta)$, $V_{j,s}(k_s)$ існують сигнали на вході системи, які забезпечують зміни $V_{j,s}(k_s)$ при незмінному значенні $\mathbf{V}_i(\eta)$. Якщо при зміні сигналів на вході системи на $\Delta U(\eta)$ сигнали на вході підсистеми S_i не міняються, то не міняються і сигнали на її виході. При цьому сигнал на вході $\mathbf{V}_j(k_s)$ підсистеми S_j зміниться на величину $\mathbf{V}_j(k_s) = \boldsymbol{\omega}_j^i(k_s)\,\Delta U(k_s)$, де $\boldsymbol{\omega}_j^i(k_s) = \mathbf{G}_j$ при $k_s = 0$, $\boldsymbol{\omega}_j^i(k_s) = \left[\mathbf{R}_j\,\mathbf{A}_i^{K_s-1}\,B_i\middle|\ldots\middle|\mathbf{R}_j\,\mathbf{B}_i\middle|\mathbf{G}\right]$ при $k_s \geq 1$.

Компонента $V_{j,s}(k_s)$ вектора $\mathbf{V}_j(k_s)$ зміниться на величину $\Delta V_{j,s}(k_S) = = \boldsymbol{\omega}^i_{j,s}(k_S)\Delta u(k_s)$ де s — рядок матриці $\boldsymbol{\omega}^i_j(k_s)$.

Варіацію сигналів на вході системи $\Delta u(\ell)$, які забезпечують зміну змінної $\mathbf{V}_{j,s}(k_s)$ при незмінному значенні $\mathbf{V}_i(\eta)$, можна віднайти з наступної системи рівнянь

$$\begin{bmatrix} \Delta V_i(\eta) = \mathbf{0} \\ \Delta V_{j,s}(k_s) \neq \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{W}_i^{(\eta)} \\ \boldsymbol{\omega}^i_{j,s}(k_s) \end{bmatrix} \times \Delta u(\ell),$$
$$\ell = \max\{\eta, k_s\}, \tag{27}$$

розв'язок якої існує в тому і лише в тому випадку, якщо

$$\text{ранг}\begin{bmatrix} \mathbf{W}_i^{(\eta)} \\ \boldsymbol{\omega}^i_{j,s}(k_s) \end{bmatrix} = \text{ранг}\ \mathbf{W}_i^{(\eta)} + 1. \tag{28}$$

На підставі викладеного вище, сформулюємо твердження.

Твердження 3.5. Підсистеми S_i, S_j мають незалежні управління при гіпотезі H_i в тому випадку, якщо існують такі значення k_s, $s = \overline{1, m_j}$, для яких виконується (28).

Виділимо клас несправностей $\mathbf{L}_j$, при якому описи несправностей підсистеми S_j відрізняються від описів справної підсистеми на деяку величину (вектор), яка являє собою в загальному випадку функцію часу.

Твердження 3.6. Нехай несправності підсистеми S_j не належать класу $\mathbf{L}_j$. Підсистеми S_i, S_j розрізняються при гіпотезі H_i, якщо їх управління незалежні.

Доведення твердження 3.6 можна отримати, спираючись на результати, отримані в роботі [17].Для перевірки гіпотези H_i сформулюємо сигнали на вході системи $\mathbf{u}^{\text{навч}}(\upsilon_i - 1)$, $\mathbf{u}^{\text{пер}}(\upsilon_i - 1)$ (навчаючі та перевірочні), які забезпечують варіацію змінної $V_{j,s}(k_s)$ при незмінному значенні $V_i(\eta)$. Ці сигнали можуть бути довільними, але повинні відрізнятися на величину $\Delta u(\ell)$, отриману з (27) для заданого значення $\Delta V_{j,s}(k_s) \neq 0$. Задавшись $\mathbf{u}^{\text{навч}}(\upsilon_i - 1)$, отримаємо $\mathbf{u}^{\text{пер}}(\upsilon_i - 1) = \mathbf{u}^{\text{навч}}(\upsilon_i - 1) + \Delta u(\ell)$.

Нехай існує можливість встановлення несправної системи в початковий стан, який для справної частини системи відомий, а для несправної підсистеми S_i невідомий. Тоді процедура перевірки гіпотези H_i наступна.

1. Система встановлюється у початковий стан і, при $\mathbf{u}^{\text{навч}}(\upsilon_i - 1)$, визначається у відповідності до (28) матриця $\Delta\Lambda_i^{\text{об}}(\upsilon_i)$.

2. Система встановлюється у початковий стан і, при $\mathbf{u}^{\text{пер}}(\upsilon_i - 1)$ визначається $\Delta\Lambda^{\text{пер}}(\upsilon_i)$.

3. Перевіряється сумісність системи рівнянь

$$\begin{bmatrix} \Delta\Lambda_i^{\text{навч}}(\upsilon_i) \\ \Delta\Lambda_i^{\text{пер}}(\upsilon_i) \end{bmatrix} = \begin{bmatrix} \mathbf{F}_i^{(\upsilon_i)} \\ F_i^{(\upsilon_i)} \end{bmatrix} \times \Delta\mathbf{Z}_i(0), \tag{29}$$

що еквівалентно перевірці рівності $\Delta\Lambda_i^{\text{навч}}(\upsilon_i) = = \Delta\Lambda_i^{\text{пер}}(\upsilon_i)$.

Якщо система рівнянь (29) несумісна, то гіпотеза H_i не приймається, якщо сумісна, то це не суперечить гіпотезі H_i. Для остаточної перевірки гіпотези H_i сумісність системи рівнянь (29) необхідно перевірити при сигналах на вході, які забезпечують варіацію сигналів на вході всіх підсистем, що мають з підсистемою S_i

незалежні управління. Зазначимо, що сигналі на вході $\mathbf{u}^{\text{навч}}(\upsilon_i - 1)$ та $\mathbf{u}^{\text{пер}}(\upsilon_i - 1)$, які забезпечують варіацію сигналів на вході підсистеми S_j, за звичай забезпечують також варіацію сигналів на вході для інших підсистем. Це дозволяє при одних й тих самих сигналах на вході системи забезпечити розрізнення підсистеми S_i з декількома підсистемами. Інтервал діагностування повинен забезпечувати варіацію сигналу на виході системи при варіації сигналу на вході підсистеми S_j. Крім того, діагностування має сенс проводити, якщо $\mathbf{\Delta\Lambda}_i^{\text{навч}}(\upsilon_i) \neq \mathbf{0}$. Тому, як і при діагностуванні підсистем з незалежним спостереженням, може знадобитися проведення діагностичного експерименту на інтервалі $[\eta, \eta + \upsilon_i]$, $\eta \geq 0$.

Висновок. Для діагностування несправності підсистем в безінерційних системах, за умови, що підсистеми спостерігаються незалежно, процедура діагностування підсистем полягає у перевірці спільності систем діагностичних рівнянь, що відповідають гіпотезам, які перевіряються. Якщо система діагностичних рівнянь спільна, то відповідна їй гіпотеза приймається, якщо не спільна — відкидається.

Слід також зазначити наступне. Для лінійних систем, що описуються за допомогою передаточних функцій, немає потреби виділяти з множини сигналів, які вимірюються, навчаючу та перевірочну множини, а тестування зводиться до перевірки сумісності системи рівнянь, що створює можливість для застосування словника у випадку локалізації несправних підсистем.

Список літератури

1. Положаєнко С.А., Гаращенко Ф.Г., Прокофьєва Л.Л. Математичне моделювання надійності тензометричних систем на основі евристичних моделей вимірювальних процедур. *Інформатика та математичні методи в моделюванні*. 2022. Т. 12, № 4. С. 358-367. DOI 10.15276/imms.v12.no4.358.
2. Прокофьєва Л.Л. Савєльєв А.А. Евристичні моделі вимірювальних процедур в задачах аналітичного дослідження тензометричних систем. *Математичне та комп'ютерне моделювання. Серія Техн. науки.* 2023. Вип. 24. С. 68-78. URL: https://doi.org/10.32626/2308-5916.2023-24.67-78.
3. Savelev A.A., Prokofieva L.L. Planning of the diagnostic experiment in the localization of troubleshooting failures of single-free systems *Informatics and mathematical methods in simulation*. 2025. Vol. 15. № 2. P. 166-175. DOI 10.15276/imms.v15.no2.166.
4. Savelev A.A. Prokofieva L.L. Methods of Mathematical Simulation and Machine Identification of Abnormal Energy Processes. *Colloquium-journa*l. 2024. Part 1. № 16 (209). P. 36–43. URL: https://colloquium-journal.org/wp-content/uploads/2024/06/Colloquium-journal-2024-209-1.pdf.
5. Заміховський Л.М., Калявін В.П. Основи теорії надійності і технічної діагностики систем: Навчальний посібник. Івано-Франківськ: Полум'я, 2009. 360 с.
6. Кутін В.М., Ілюхін М.О., Кутіна М.В.. Оцінка ефективності системи діагностичного контролю електромеханічних комплексів. *Вісник Вінницького політехнічного інституту*. 2004. №3. С. 51-54.
7. Catelani M., Fort A. Soft fault detection and isolation in analog circuits: some results and a comparison between a fuzzy approach and radial basis function networks. *IEEE Transactions on Instrumentation and Measurement*. 2002. Vol. 51. Is. 2. P. 196-202 DOI: 10.1109/19.997811.
8. Huang W.H. Wey C.L. Diagnosability analysis of analogue circuits. *Int. J. Circuit Theory and Applications*. 2008. Vol. 26. Issue 5. P. 439-451.
9. Jung D.E., Krysander M., Frisk E. A method for quantitative fault diagnosability analysis of stochastic linear descriptor models. Int. J. Automatica 2013. 49(6). P. 1591 — 1600. DOI: 10.1016/j.automatica. 2013.02.045

10. Kabisatpathy P., Barua A., Sinha S. Fault detection and diagnosis in analog integrated circuits using artificial neural network in a pseudorandom testing scheme. *IEEE 3rd Int. Conf. on Electrical & Computer Engineering ICECE* . 2004. P. 52-56.
11. Верлань А.А. Аналіз можливості діагностування об'єктів зі структурою, яка переналашиовується. *Моделювання та інформаційні технології. Зб. наук. праць ІПМЕ ім. Г. Є. Пухова НАН України*. 2008. Вип. 45. 2008. С. 3-9.
12. Верлань А.А., Положаєнко С.А.,. Осман І.Х. Декомпозиційний метод локалізації несправних електронних підсхем. *Електромашинобудування та електрообладнання* . 2007. Вип. 69. С. 72-76.
13. Верлань А.А., Положаєнко С.А.,. Осман І.Х. Локалізація несправних електронних підсхем методом навчаючих та перевірочних характеристик. *Математичне та комп'ютерне моделювання. Серія: Техн. Науки. Зб. наук. праць Кам'янець-Подільського нац. ун-та ім. Івана Огієнка*. 2008. Вип. 1. С. 140-144.
14. Верлань А.А. Стертен Ю., Положаєнко С.А. Формалізація представлення послідовності тестових гіпотез при діагностуванні електронних схем. *Informatics and Mathematical Methods in Simulation.* 2016. Vol. 6, № 4. P. 315-321.
15. Verlan A., Polozhaenko S. Formalization of Representation of Sequence of Test Hypotheses In Diagnosing Electronic Schemes. *IEEE 38th International Conference Electronics and Nanotechnology*. 2018. P. 548-552.
16. Положаєнко С.А., Прокофьєва Л.Л. Планування діагностичного експерименту при локалізації несправностей підсхем безінерційних систем *Інформатика та математичні методи в моделюванні*. 2018. Т. 8. №1. С. 5-16.
17. Верлань А.Ф. Положаєнко С.А. Локалізація несправних фрагментів при діагностуванні безінерційних систем. *Електротехнічні та комп'ютерні системи: Теорія і практика. Спеціальний випуск*. Одеса: Астропрінт, 2017. С. 439 — 445.

DIAGNOSING ELECTRICAL SUBSYSTEMS UNDER THE CONDITIONS OF INDEPENDENCE OF THEIR OBSERVATION AND CONTRO

A. A. Savelev[1], L. L. Prokofieva[2], M. A. Kotolup[3]

[1,2]National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
[3] Professional College of Maritime Transport of the National University "Odesa Maritime Academy", 40/42, Marazliivska St., 65014, Ukraine
Emails: savieliev.a.a@op.edu.ua, prokofieva@op.edu.ua, marinakstvdi@gmail.com

Modern practice of developing technical systems, and electrical systems in particular, shows that their reliability is laid at the design stage and ensured at the production stage. Imperfections in production technology and violations of operating modes can cause various types of defects in finished systems. Thus, diagnostics of a technical object (system) must necessarily be present at all stages of its life cycle. Therefore, various works to ensure the process of diagnosing a technical system are carried out during its development, manufacture, testing and operation. In this case, the purpose of diagnostics is to maintain the required level of indicators of the technical condition of the system. At the design stage, the main task of diagnostics is to ensure the possibility of potential diagnostics of the system being designed, and at the production and operation stage - current control of its operability. The constant increase in the complexity of technical systems, associated with the increase and complication of the functions performed, the improvement of production technology, the increase in requirements for quality indicators, etc., leads to the complication of diagnostic methods and tools that provide the necessary properties of systems. For the diagnosis of electrical devices, the following methods are used: peripheral scanning, automatic pattern generation technology, built-in self-scanning, as well as parametric identification methods, fault control methods, evaluation methods, etc. Many of these methods have the following disadvantages: a significant amount of calculations, the need to access all nodes of the electrical circuit, sensitivity to calculation errors, and, as a result, the complexity of practical implementation. In addition, the reference method has become widely used in the diagnosis of electrical devices, based on finding from a set of voltage or current values at control points those of them that are closest to the values obtained when measuring in the device being diagnosed. Despite significant achievements in the field of diagnosing the technical condition of systems, at present the relevance of theoretical research and practical application of diagnostic methods remains crucial as a basis for ensuring the necessary quality indicators of systems (and electrical systems, in particular) and increasing the reliability of assessments of the technical condition of the latter. The conditions of independent observation and control, which provide the possibility of conducting a diagnostic experiment without taking the controlled system out of operation, are considered and investigated.

Keywords: Diagnosis, diagnostic experiment, diagnostic methods, operating conditions, independent observation, independent control, technical system.

DOI 10.15276/imms.v15.no3.419
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 419-429

РОЗРОБКА АДАПТИВНОГО ДО КОНТЕНТУ АЛГОРИТМУ ДЛЯ ШИФРУВАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

А. В. Садченко, О. А. Кушніренко

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Email: koa@op.edu.ua

У сучасному інформаційному середовищі дедалі більшого значення набуває захист цифрових даних, серед яких важливу частку становлять графічні матеріали – фотографії, відсканові документи та мультимедійні файли. Вони, так само як і текстові дані, можуть містити персональну або критично важливу інформацію, що потребує надійних механізмів шифрування та збереження. Проте навіть за наявності розвинених криптографічних методів текстові й графічні файли залишаються вразливими через специфічні структурні особливості. Для текстових даних типовими є статистичні закономірності, наприклад частотний розподіл символів і слів, що може використовуватися для проведення криптоаналітичних атак у разі застосування слабких або однотипних шифрів. У графічних файлах одним із ключових ризиків є висока кореляція між сусідніми пікселями, особливо у випадку природних зображень або даних із мінімальним стисненням, що створює можливість реконструкції чи аналізу навіть частково зашифрованої інформації. Додаткову загрозу становлять метадані (EXIF, IPTC, XMP), які автоматично додаються під час створення або редагування файлів і можуть містити конфіденційні відомості про походження чи властивості даних. У роботі запропоновано комбінований алгоритм захисту текстових і графічних файлів, орієнтований на усунення зазначених вразливостей. Алгоритм реалізує багаторівневу симетричну схему, що поєднує три етапи: AES-CBC, перестановку блоків та AES-GCM. Ключі формуються на основі пароля та унікальної солі, що підвищує стійкість до атак перебором. Основною метою є формування розподілу байтів зашифрованих даних, максимально наближеного до рівномірного, що мінімізує можливість їх відновлення методами статистичного аналізу. Для підтвердження ефективності алгоритму застосовано вбудовані в середовище Matlab статистичні тести, серед яких ентропійний, χ^2, Колмогорова–Смирнова та кореляційний. Результати продемонстрували значне зростання ентропії та зниження рівня кореляції між елементами після шифрування, що свідчить про досягнення властивості невизначуваності вхідних даних. Практичне використання алгоритму передбачає можливість гнучкого налаштування – користувач може обирати компроміс між рівнем криптостійкості та показниками стиснення під час формування захищених архівів. Таким чином, запропонований підхід забезпечує комплексний захист різних типів цифрової інформації, поєднуючи високу ефективність із адаптивністю до конкретних практичних потреб.

Ключові слова: шифрування, надлишковість, графічна та текстова інформація, автентифікація даних

Вступ. У сучасному цифровому світі обсяг даних, що постійно створюються, передається та зберігається, зростає в геометричній прогресії. Це зумовлює підвищену увагу до питань забезпечення конфіденційності [1] інформації. Якщо раніше основний акцент робився на захист текстових документів, то сьогодні значну частку цифрових даних становлять графічні матеріали – фотографії, скановані копії документів, мультимедійні файли тощо. Вони, як і текстові дані, можуть містити критично важливу або персональну інформацію, тому також потребують надійного захисту від несанкціонованого доступу. Попри значний прогрес у галузі криптографії, як текстові, так і графічні дані залишаються вразливими до певних типів атак через свої внутрішні структурні особливості. У текстових файлах зберігаються характерні статистичні закономірності – зокрема, частотний розподіл символів, слів або фраз, що може

використовуватись для криптоаналізу навіть за умови зашифрованого вмісту. Це особливо актуально при використанні слабких або однотипних шифрів, які не маскують мовну структуру даних [2,3]. У графічних файлах існують інші, не менш критичні ризики. Однією з основних вразливостей є висока кореляція між пікселями [4], особливо в зображеннях із природними сценами або слабким стисненням. Така статистична залежність дозволяє використовувати методи аналізу зображень або реконструкції для витягування прихованої або частково зашифрованої інформації. Крім того, зображення часто містять відкриті метадані (наприклад, EXIF, IPTC, XMP), які автоматично додаються камерами або програмним забезпеченням під час створення чи редагування файлу. Ці метадані можуть містити інформацію про модель пристрою, дату та час створення, координати GPS, параметри зйомки, авторство тощо [5]. Окрему небезпеку становлять службові заголовки файлів, які розкривають тип кодування, формат даних і можуть слугувати додатковим джерелом технічної або персональної інформації [6]. Всі ці особливості підкреслюють необхідність не лише використовувати сучасні методи шифрування, а й звертати увагу на приховані властивості даних, що потенційно можуть бути використані для інформаційного витоку або відновлення змісту.

Метою статті є розробка алгоритму, призначеного для забезпечення надійного криптографічного захисту як текстових, так і графічних даних із використанням сучасних методів шифрування. Передбачено, що створене рішення унеможливлюватиме визначення початкового формату даних після їх шифрування, а оцінка ефективності приховування характерних ознак здійснюється статистичними методами.

Для досягнення поставленої мети необхідно виконати такі завдання:

– провести огляд та аналіз сучасних методів криптографічного захисту інформації, визначивши їх слабкі місця та можливі вектори атак;

– дослідити особливості процесів шифрування даних різних форматів, зокрема текстових і графічних файлів;

– створити математичну модель, що забезпечує функції шифрування, розшифрування та аналізу зазначених типів даних;

– здійснити експериментальне дослідження статистичних характеристик зашифрованих даних з метою оцінки можливості визначення їхнього вихідного формату, а також перевірити методи приховування таких ознак.

Характерні риси та типи існуючих криптографічних методів захисту інформації. Усі криптографічні методи умовно класифікуються на дві основні групи – класичні та сучасні, які відрізняються між собою рівнем складності реалізації, стійкістю до криптоаналітичних атак і сферами практичного використання [7].

Класичні криптографічні методи ґрунтуються на простих математичних принципах і широко застосовувалися до появи комп’ютерних обчислювальних систем. До них належать, зокрема, підстановочні та перестановочні шифри [8].

Підстановочні шифри замінюють символи відкритого тексту іншими згідно з певним фіксованим правилом. Наприклад, моноалфавітні шифри, такі як шифр Цезаря, використовують один і той самий алфавіт протягом усього повідомлення, що робить їх надзвичайно вразливими до частотного аналізу, оскільки зберігаються статистичні закономірності мови. У поліалфавітних шифрах, наприклад у шифрі Віженера [9], використовується кілька алфавітів, що ускладнює розшифрування, однак вимагає більших обчислювальних зусиль.

На відміну від підстановки, перестановочні шифри не змінюють самі символи, а лише їхній порядок у повідомленні. Вони є простими в реалізації, але не порушують частотних характеристик тексту, що обмежує їх криптографічну стійкість. Загалом класичні методи шифрування не відповідають сучасним вимогам безпеки, адже легко піддаються статистичному аналізу та не забезпечують належного рівня захисту в умовах автоматизованої обробки даних.

Сучасна криптографія включає значно складніші алгоритми, які розроблялися з урахуванням високої обчислювальної потужності сучасних комп'ютерів і необхідності протистояти складним методам злому. Вона охоплює три ключові напрямки: симетричне шифрування, асиметричне шифрування та хешування [10].

Симетричні алгоритми. Симетричні методи базуються на використанні одного секретного ключа як для шифрування, так і для дешифрування повідомлення. Їх поділяють на дві категорії: блочні та потокові шифри.

Блочні шифри, такі як AES (Advanced Encryption Standard), обробляють дані блоками фіксованого розміру (наприклад, 128 або 256 біт). Вони характеризуються високою швидкістю та стійкістю до широкого спектра атак, однак за відсутності додаткових заходів (наприклад, режимів роботи) можуть зберігати структуру повідомлення, що призводить до витоку шаблонів. Повторення однакових блоків у відкритому тексті може зумовити повторення тих самих блоків у шифротексті. Для усунення цього недоліку використовуються режими роботи блочного шифрування [11], зокрема CBC (Cipher Block Chaining) та GCM (Galois/Counter Mode), які забезпечують диференціацію блоків завдяки введенню випадкових значень (ініціалізаційних векторів).

Потокові шифри, наприклад ChaCha20, працюють з потоком даних на рівні бітів або байтів, послідовно обробляючи інформацію з використанням ключового потоку. Завдяки високій продуктивності та низькій затримці, такі алгоритми ідеально підходять для шифрування потокових даних – аудіо, відео або реального часу передавання.

Асиметричні алгоритми. Асиметричні криптосистеми передбачають використання пари ключів – публічного та приватного. Публічний ключ застосовується для шифрування, а приватний – для дешифрування.

Одним із найвідоміших прикладів є RSA (Rivest–Shamir–Adleman), який базується на складності факторизації великих чисел [12] і використовується як для шифрування даних, так і для створення цифрових підписів.

Інший важливий алгоритм – Diffie–Hellman [13]– забезпечує безпечний обмін ключами між двома сторонами без попереднього узгодження, навіть через відкриті канали зв'язку. DSA (Digital Signature Algorithm) – спеціалізований алгоритм для створення цифрових підписів, який гарантує автентичність і цілісність повідомлень [14].

Основна перевага асиметричних методів полягає у відсутності необхідності передавати секретний ключ, що є критично важливим у розподілених та відкритих мережах. Проте їхнім недоліком є значно нижча швидкість у порівнянні із симетричними алгоритмами, що обмежує сферу їхнього використання – зазвичай, асиметрія застосовується лише для початкової фази встановлення захищеного зв'язку або цифрового підпису, тоді як самі дані шифруються симетрично.

Хешування. Хеш-функції є основним інструментом для забезпечення цілісності даних. Вони перетворюють вхідне повідомлення довільної довжини у вихідний рядок фіксованої довжини – хеш, або дайджест.

На відміну від шифрування, хешування є одностороннім процесом – отриманий хеш не може бути використаний для відновлення початкових даних.

Криптографічна хеш-функція повинна відповідати кільком важливим властивостям [15]:

- детермінованість – однакові вхідні дані завжди дають однаковий хеш;
- ефективність – обчислення хешу має виконуватись швидко;
- односторонність – неможливість відновлення вихідного повідомлення з хешу;
- лавиноподібний ефект – незначна зміна вхідних даних повинна спричиняти значну зміну хешу;
- стійкість до колізій – ймовірність того, що два різні повідомлення матимуть однаковий хеш, повинна бути мінімальною.

Завдяки цим характеристикам хеш-функції широко застосовуються у зберіганні паролів, перевірці цілісності файлів, створенні цифрових підписів, а також як фундаментальний елемент блокчейн-технологій та розподілених облікових систем.

Вразливості текстових даних. Текстові дані – це інформація, представлена у вигляді символів, слів або речень, яка використовується у широкому спектрі цифрових документів: текстових файлах (наприклад, TXT, DOCX, PDF), електронному листуванні, повідомленнях, програмному коді тощо. Завдяки своїй структурованості, стандартизованості й передбачуваності, такі дані є привабливими цілями для криптоаналітичних атак. Зокрема, характерні шаблони, частотний розподіл символів і граматичні закономірності можуть бути використані для спрощення процесу дешифрування. Саме ці особливості зумовлюють необхідність у глибокому криптоаналізі – галузі, що досліджує вразливості криптографічних алгоритмів та методів захисту.

Криптоаналіз – це прикладна і теоретична дисципліна [16], що має на меті виявлення недоліків у криптографічних системах, а також розробку методів обходу засобів захисту без знання секретного ключа. На відміну від криптографії, яка створює засоби захисту, криптоаналіз спрямований на їх випробування та злам. Він спирається на аналіз математичних структур алгоритмів, статистичні особливості даних, а також на слабкості в реалізації чи управлінні ключами.

Сучасний криптоаналіз включає декілька підходів:

1) атаки на криптосистеми:
   а) Known-Plaintext Attack (KPA) – аналізуючи відомі пари відкритого тексту та шифротексту, атакуючий може вивести ключ або вразливості шифру;
   б) Chosen-Plaintext Attack (CPA) – зловмисник може обирати відкриті тексти й отримувати їхні шифровані варіанти для аналізу зв’язків;
   в) Ciphertext-Only Attack (COA) – аналізуються лише шифротексти, часто з використанням статистичних методів;
   г) Chosen-Ciphertext Attack (CCA) – атакуючий має доступ до розшифрування певних шифротекстів, що дає змогу виявити алгоритмічні слабкості;
2) статистичний криптоаналіз:
   а) частотний аналіз – вивчає частоти появи символів у шифротексті, особливо ефективний проти простих підстановочних шифрів;
   б) лінійний криптоаналіз – використовує апроксимації між відкритим текстом, шифротекстом і ключем;
   в) диференційний криптоаналіз – досліджує вплив змін у відкритому тексті на шифротекст для виявлення залежностей;
3) атаки на ключі:
   а) Brute Force – повний перебір ключів;
   б) словникові атаки – використання баз даних поширених паролів;
   в) райдужні таблиці – попередньо згенеровані відповідності між хешами та вхідними даними;
4) математичні атаки:
   а) факторизація – для зламу RSA шляхом розкладу модуля на прості множники;
   б) атаки на основі дискретного логарифма – загрожують алгоритмам Diffie-Hellman та ECC.

Захист від криптоаналізу передбачає:

– використання криптостійких алгоритмів (AES, RSA, ECC);
– впровадження випадкових компонентів (IV, соль, хешування з ключем);
– режими шифрування, що знищують статистичні ознаки (CBC, GCM);
– застосування хеш-функцій із доказаною стійкістю до колізій (SHA-2, SHA-3, bcrypt, Argon2).

Особливості захисту текстових даних полягають у необхідності розриву мовних шаблонів. Наприклад, однакові слова не повинні давати однаковий шифротекст. Для цього застосовуються режимні алгоритми з випадковими послідовностями символів, а також методи згладжування ентропії.

Вразливості графічних даних. Для графічних даних загрози мають інший характер [17]. Графіка, особливо у форматах JPEG, PNG, BMP, зберігає просторові й колірні кореляції, які можуть бути використані при атаках:

- атаки за типом пазлу (Jigsaw puzzle attack);
- атаки на сусідні пікселі (Neighbor attack);
- частотний аналіз кольорових каналів.

Для протидії цим атакам використовуються методи повного перемішування даних (наприклад, блокові шифри з комбінованими перестановками та підстановками) та хаотичні перетворення, які повністю руйнують структуру зображення. Крім того, обов'язковим є видалення або шифрування метаданих (EXIF, заголовки), які можуть зберігати чутливу інформацію навіть після шифрування пікселів.

Алгоритм (модуль) шифрування текстової інформації. Розглянемо алгоритм шифрування текстової інформації.

Для практичного застосування алгоритмів шифрування текстової інформації розроблено низку програмних рішень, що спрощують процес захисту даних та відповідають сучасним вимогам безпеки. Серед них найбільш поширеними є AES Crypt і AxCrypt [18]. Одне з рішень, забезпечує швидке шифрування файлів за допомогою алгоритму AES-256 без потреби у складному налаштуванні. Натомість AxCrypt пропонує розширені можливості: наскрізне шифрування, інтеграцію з хмарними сервісами та підтримку різних операційних систем – від Windows і macOS до Android та iOS [19].

Алгоритм AES обрано основним методом шифрування завдяки його високій стійкості до сучасних криптографічних атак, оптимальному співвідношенню швидкодії та рівня захищеності, а також широкій підтримці на різних платформах.

Advanced Encryption Standard (AES) є симетричним блочним шифром, де дані поділяються на блоки розміром 128 біт. Такий розмір позначається як $N_b = 4$, що відповідає чотирьом 32-бітним словам. Довжина секретного ключа може становити 128, 192 або 256 бітів, тобто $N_k = 4{,}6$ або 8 слів по 32 біти. Від вибору довжини ключа залежить і кількість раундів (N_r) у процесі шифрування: для AES-128 це 10 раундів, для AES-192 – 12, а для AES-256 – 14, як зазначено в табл. 1. Під час розширення ключа (Key Expansion) формується $N_r + 1$ раундових ключів (Round Keys) $K_0, K_1, \ldots, K_{Nr}$, кожен з яких має ті ж 128 біт, що збігається з розміром блоку [20].

Таблиця 1.

Комбінації ключ-блок-раунд

Алгоритм	Розмір блоку (Nb слів)	Довжина ключа (Nk слів)	Кількість раундів (Nr)
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14

Під час шифрування вхідний блок даних (plaintext) розміром 128 біт подається у вигляді матриці 4×4, яка називається State**.** Кожен її елемент ($a_{i,j}$) відповідає одному байту. Формування матриці здійснюється за стовпцевим принципом: спочатку послідовно заповнюється перший стовпець зверху вниз, далі – другий і так далі.

Після виконання всіх етапів перетворення ця матриця State набуває вигляду зашифрованого блоку (ciphertext).

Розглянемо приклад успішного тесту, який наведено в табл. 2.

Таблиця 2.

Параметри шифрування та розшифрування

Параметр	Значення
Ключ (16 символів)	hGkLmNpQrStUvWxY
Вихідний текст	secret
Зашифрований текст (HEX)	cf970df14a9433bbed1ff2cac9299dd295cd3aceda7d6db5cbee68 883d90ab63
Розшифрований текст	secret

При дотриманні вимог до довжини ключа та коректному введенні вихідного тексту система безпомилково шифрує та розшифровує дані. Як можна побачити, процедура шифрування сформувала випадково «cf97» та додала його до початку результату, а розшифрування з тим самим ключем відновило вихідне слово без помилок. Якщо б ключ було змінено хоча б на один символ, алгоритм не зміг би правильно дешифрувати повідомлення.

Отже, модуль AES, робота якого тестувалася у пакеті Matlab успішно пройшов тестування на коректність роботи у звичайних і виняткових ситуаціях, що підтверджує надійність обраного режиму CBC та реалізації алгоритму AES, наприклад, у вигляді окремого застосунку.

Для наочного представлення результатів було побудовано два графіки. На першому (рис 1) ліворуч відображено розподіл байтів вихідного файлу, де простежується концентрація значень у межах типового діапазону ASCII-символів (близько 32–122 у десятковому представленні), що властиво текстовим даним. Праворуч наведено розподіл байтів зашифрованого файлу, який рівномірно охоплює майже весь діапазон від 0 до 255, що свідчить про втрату видимої структури після шифрування.

У результаті обчислень зафіксовано зростання ентропії файлу до ~7,99 біт/байт, а показник розподілу імовірностей χ^2 наблизився до значення, характерного для випадкових послідовностей, що підтверджує ефективне усунення вихідних статистичних закономірностей.

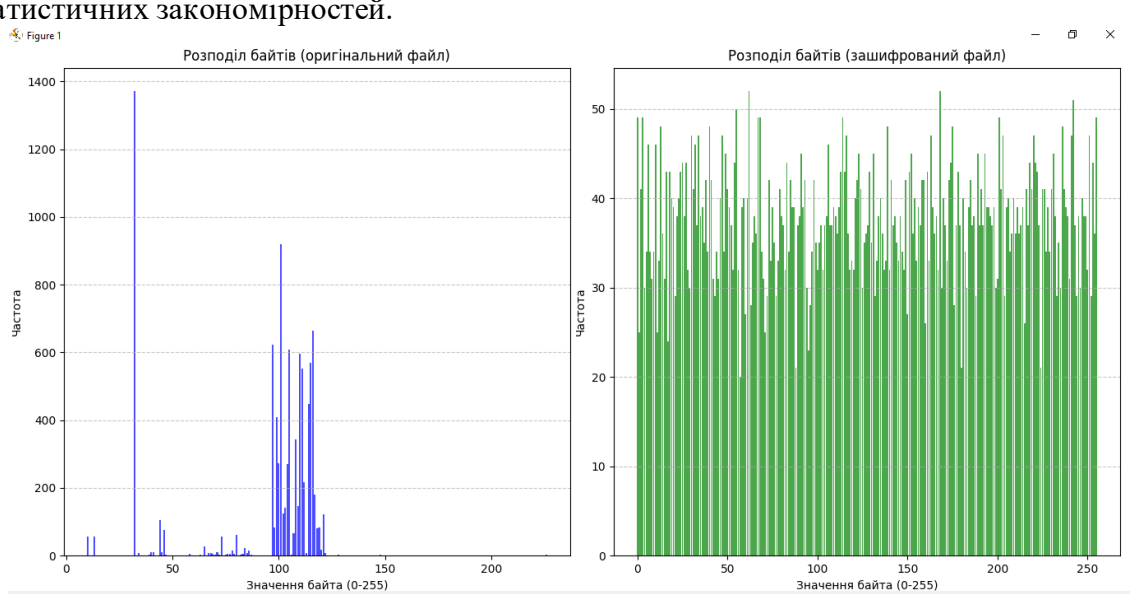


Рис. 1. Розподіл байтів у текстовому файлі до та після шифрування

Другий графік (рис. 1) відображає порівняння нормованих частот появи байтів у вихідному та зашифрованому файлах.

У початковому файлі помітні виражені піки, що відповідають найбільш уживаним символам, тоді як у зашифрованому файлі розподіл є майже рівномірним. Це свідчить про підвищену ентропію даних та ефективність застосованого методу шифрування.

Подібна візуалізація чітко демонструє суттєві зміни у структурі даних після шифрування, що підтверджується статистичними показниками та засвідчує високий рівень криптографічного захисту.

Алгоритм (модуль) шифрування графічної інформації із урахуванням статистичних характеристик. Алгоритм шифрування графічної інформації (наприклад, зображень) повинен враховувати специфіку таких даних – великий обсяг, сильну корельованість пікселів та вимоги до швидкодії. Також, так як вимогою до модулю, що розробляється є умова ускладнення процедури розрізнення типу контенту після шифрування, необхідно ввести критерій складності алгоритму аналізу зашифрованого контенту. У якості такого критерію може виступати допуск на цільове значення ентропії, що обчислюється із умови відхилення закону розподілу байтів зашифрованого файлу від рівно ймовірного.

Було запропоновано наступний алгоритм.

Крок 1. Задається початковий допуск на цільове значення ентропії графічного файлу ΔH в діапазоні 0.1…8 бітів на піксель. Задаємо значення лічильнику кількості проходів алгоритму j=0.

Крок 2. Завантажується графічний файл і здійснюється його перекодування в нестиснений формат, наприклад BMP.

Крок 3. Здійснюється обчислення обсягу зображення J в бітах. Зображення представимо у вигляді масиву із m рядків та n стовпців. Яскравість кожного пікселю зображення кодується за допомогою k розрядів. Якщо зображення кольорове то $k=k_r+k_b+k_g$, де k_r – кількість розрядів яскравості червоного каналу, k_b – кількість розрядів яскравості синього каналу, k_g – кількість розрядів яскравості червоного каналу, k_b – кількість розрядів яскравості зеленого каналу. Таким чином:

$$J = n \bullet m \bullet Log_2 k \text{ бітів.}$$

Крок 4. Обчислюємо вихідне значення ентропії H_i нестисненого зображення в бітах на піксель:

$$H_i = -\sum_{i=0}^{2^k-1} p_i Log_2(p_i),$$

де p_i – ймовірність появи пікселю із яскравістю, що дорівнює i.

Загальне значення ентропії H_{it} для всього зображення (m×n пікселів):

$$H_{it} = H_i \bullet m \bullet n$$

Крок 5. Обчислюємо максимально можливе значення ентропії H_m нестисненого зображення. Максимально можливе значення ентропії досягається при умові, що всі ймовірності появи пікселю із довільною яскравістю однакові та дорівнюють: $p_i = \frac{1}{2^k}$.

Таким чином: $H_m = -\sum_{i=0}^{2^k-1} \frac{1}{2^k} Log_2\left(\frac{1}{2^k}\right) = Log_2 2^k = k$ бітів на піксель. Тобто загальне значення ентропії H_{mt} для всього зображення (m×n пікселів):

$$H_{mt} = H_m \bullet m \bullet n$$

Крок 6. Обчислюємо різницю ентропії, що обчислені на кроках 5 та 4:

$$\Delta\hat{H} = H_m - H_i$$

Крок 7. Якщо $\Delta\hat{H} \le \Delta H$ переходимо на крок 9. Шифруємо файл із додаванням ентропії із використанням алгоритму AES-128 чи AES-256 чи AES-512 в залежності від номеру проходу j. Збільшуємо лічильник кількості проходів j = j + 1.

Крок 8. Якщо j > 3, збільшуємо початковий допуск на цільове значення ентропії графічного файлу ΔH= ΔH+0.1, прирівнюємо j=0 і переходимо на крок 2.

Крок 9. Здійснюємо стиснення зображення в необхідному форматі чи формуємо zip архів.

Для наочного відображення результатів було виконано візуалізацію даних у формі трьох графіків. На рисунку 3 представлено розподіл значень RGB-каналів вихідного оригінального зображення (Lena) (рис 2 а) розміром 512×512 пікселів, що є стандартним для задач тестування алгоритмів графічної обробки зображень.

а б

Рис. 2. Вигляд тестувального зображення «Лена» (джерело: [21]): а) оригінальне зображення; б) зашифроване зображення

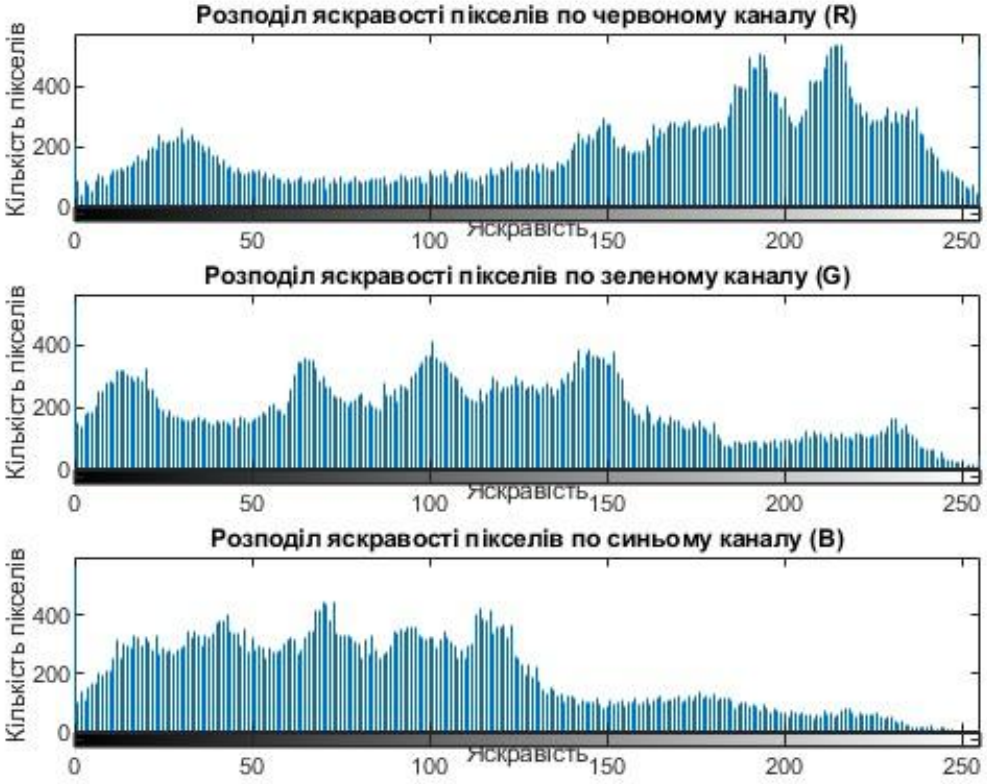


Рис. 3. Розподіл значень яскравості RGB-каналів у зображенні «Лена» до шифрування

З аналізу рисунку 3, можна побачити, що для оригінального файлу, спостерігаються характерні піки й спадини, що виникають внаслідок JPEG-стиснення. Видно, що основна частина інтенсивностей зосереджена поблизу мінімальних та

максимальних значень яскравостей (близько 0 і 255), що характерно для JPEG-файлів із підвищеною контрастністю або наявністю великих однотонних областей.

На рисунку 4 подано розподіл байтів у файлі після JPEG-стиснення до та після шифрування.

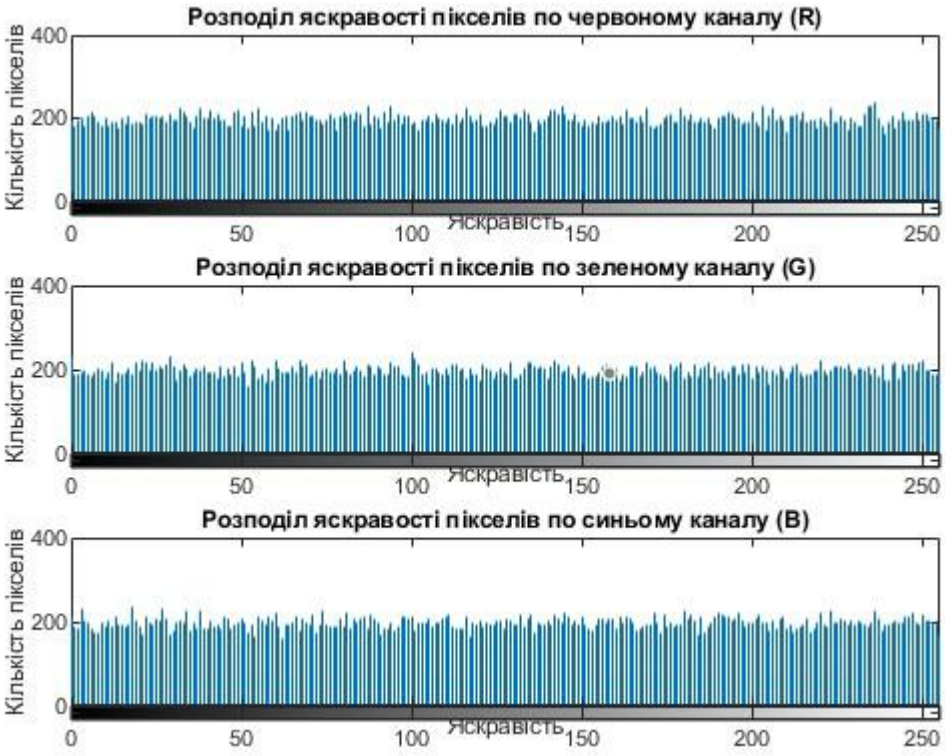


Рис. 4. Розподіл значень байтів яскравості RGB каналів у графічному файлі після шифрування

У зашифрованому файлі, рис 4, розподіл значень у межах 0 – 255 набуває майже рівномірного характеру при заданому цільовому значенні ентропії 4 біта на піксель.

Слід зазначити, що шифрування зображень за алгоритмами AES-128 чи AES-256 чи AES-512 суттєво знижують ефективність алгоритмів стиснення без втрат, таких як кодування кодом Гафмана, а після JPEG-стиснення якість зображення може бути гіршою в порівнянні із випадком відсутності шифрування.

Висновки. Встановлено, що класичні методи шифрування, зокрема шифр Цезаря, шифр Віженера, а також алгоритми DES і RC4, є недостатньо надійними, оскільки вразливі до частотного та статистичного аналізу через обмежений простір ключів і передбачуваність структури шифротексту. Натомість сучасні криптографічні алгоритми – AES (FIPS 197, офіційний стандарт NIST) у режимах CBC та GCM, RSA (PKCS #1) і ECC (ANSI X9.62) – за умови правильного вибору режимів роботи та належного управління ключами демонструють високу стійкість до частотного, диференційного й лінійного криптоаналізу.

Розроблений алгоритм реалізує багаторівневу симетричну схему, що поєднує три етапи: AES-CBC, перестановку блоків та AES-GCM, із використанням ключів, отриманих на основі пароля та солі. Такий підхід забезпечує захист як текстових, так і графічних файлів. Вбудований модуль статистичного аналізу (ентропійний, χ^2, Колмогорова–Смирнова та кореляційний тести) підтвердив ефективність перевірки властивості невизначуваності типу вхідних даних після шифрування.

Розроблений алгоритмічний модуль щодо адаптивного шифрування графічної інформації враховує такі її особливості як висока корельованість пікселів, особливо при наявності на зображенні фону із рівномірною яскравістю. З метою додаткового ускладнення ідентифікації типу контенту після шифрування було запропоновано

алгоритм, що заснований на послідовному досягненні цільового рівня ентропії, що задається користувачем на етапі підготовки даних.

Експериментальні дослідження показали, що зашифровані файли за своїми статистичними характеристиками наближені до випадкового шуму, що унеможливлює ідентифікацію їхнього початкового формату. Перевірка працездатності алгоритму шляхом моделювання в середовищі Matlab довела його придатність для автоматизованого захисту бухгалтерської та юридичної документації.

Список літератури

1. Сирбу К. Д., Садченко А. В. Розробка застосунку для криптографічного захисту текстових та графічних даних. *Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль*. 2025. С. 175-178.
2. Константинова Л. В., Норов А. О. Криптографія та стеганографія: різниця та застосування в захисті інформації. *VI Міжнародна науково-практична конференція Інформаційна безпека та комп'ютерні технології*. 2023. С.5-7.
3. Kordov K. Text_encryption_algorithm_for_secure_communication. *International Journal of Applied Mathematics*. 2021. Vol. 34. No. 4. P. 705. URL: http://dx.doi.org/10.12732/ijam.v34i4.9
4. Sabonchi A. Kh. Sh., Akay B. A survey on the Metaheuristics for Cryptanalysis of Substitution and Transposition Ciphers. *Computer Systems Science & Engineering*. 2021. Vol. 39. No. 1. P. 47.
5. Орловський В. О. Системи і технології захисту інформації при її обміні між користувачами. *Міжнар. наук. інтернет-конф*. 2022. С.50. URL: www.konferenciaonline.org.ua.
6. Trysnyuk V., Smetanin K., Humeniuk I., Samchyshyn O. Information Encryption Method based on a Combination of Steganographic and Cryptographic Algorithm's Features. *Cybersecurity Providing in Information and Telecommunication Systems*. 2021. P. 150-159. URL: https://ceur-ws.org/Vol-3187/paper14.pdf
7. Prajapat S., Thakur R. S. Various approaches towards cryptanalysis. *International Journal of Computer Applications*. 2015. Vol. 127, No. 14. P. 15–24.
8. Schroé W. Cryptanalysis of Submission to the CAESAR Cryptographic Competition iFeed. URL: https://cosicdatabase.esat.kuleuven.be/backend /publications/files/these/262.
9. Najaftorkaman M., Kazazi N. S. A method to encrypt information with DNA-based cryptography. *International Journal of Cyber-Security and Digital Forensics*. 2015. Vol. 4. No. 3. P. 417–426.
10. Rhea Gupta, Sara Dharadhar, Prathamesh Churi; CloudJS: novel cloud-based design framework for text-file encryption. *World Journal of Engineering*. 2023. Vol.20 (3). P. 472–485. URL: https://doi.org/10.1108/WJE-04-2021-0234
11. Лужецький В. А., Кисюк Д. В. Метод хешування даних на основі їх характеристичних ознак. *II Міжнар. наук.-практ. конф. «Актуальні питання забезпечення кібербезпеки та захисту інформації»*. 2016. С. 100–102.
12. Blondeau C., Leander G., Nyberg K. Differential-linear cryptanalysis revisited. *Journal of Cryptology*. 2017. Vol. 30. P. 859–888.
13. Data Encryption Methods & Types: A Beginner's Guide. URL: https://www.splunk.com/en_us/blog/learn/data-encryption-methods-types.html
14. Mourouzis T., Song G., Courtois N., Christofi M. Advanced differential cryptanalysis of reduced-round SIMON64/128 using large-round statistical distinguishers. *Cryptology ePrint Archive*. 2015. Report 2015/481. P. 1–9.
15. Noor N.S., Hammood D.A., Al-Naji A., Chahl J. A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication. *Computers*. 2022. Vol.11(3): 39. URL: https://doi.org/10.3390/computers11030039

16. Jebur, R.S.; Der, C.S.; Hammood, D.A. A Review and Taxonomy of Image Denoising Techniques. In Proceedings of the 6th International Conference on Interactive Digital Media (ICIDM), Bandung, Indonesia, 14–15 December 2020; pp. 1–6.
17. Aparna V. S., Rajan A., Jairaj I., Nandita B., Madhusoodanan P and Remya A. S., *Implementation of AES Algorithm on Text And Image using MATLAB. 3rd International Conference on Trends in Electronics and Informatics. India.* 2019. P. 1279-1283. DOI: 10.1109/ICOEI.2019.8862703
18. Huang X., Dong Y., Ye G., Yap W.S., Goi B.M. Visually meaningful image encryption algorithm based on digital signature. *Digital Communications and Networks*. 2023. Vol. 9. Is.1., P 159-165. URL: https://doi.org/10.1016/j.dcan.2022.04.028.
19. Abusukhon A., AlZu'bi S. New Direction of Cryptography: A Review on Text-to-Image Encryption Algorithms Based on RGB Color Value. 2020 *Seventh International Conference on Software Defined Systems. France*. 2020. P. 235-239, DOI: 10.1109/SDS49854.2020.9143891.
20. Abusukhon A., Anwar M.N., Mohammad Z., Alghannam B. A Hybrid. Network Security Algorithm Based on Diffie Hellman and Text-to-Image Encryption Algorithm. URL:https://researchportal.northumbria.ac.uk/ws/portalfiles/portal/18728434/Abusukhon_et_al_A_hybrid_network_security_algorithm_based_on_Diffie_Hellman_and_Text_to_Image_Encryption_algorithm_AAM.pdf
21. Banerjee M., Naskar S., Basuli K., Sarma S.S. A novel scheme for text data encryption. *Journal of Global Research in Computer Science.* 2012. Vol. 3. P 39-41. URL: https://www.rroij.com/open-access/a-novel-scheme-for-text-data-encryption-39-41.pdf

DEVELOPMENT OF A CONTENT-ADAPTIVE ALGORITHM FOR ENCRYPTION OF CONFIDENTIAL INFORMATION

A. V. Sadchenko, O. A. Kushnirenko

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: koa@op.edu.ua

In the modern information environment, the protection of digital data is becoming increasingly important, among which an important share is made up of graphic materials - photographs, scanned documents and multimedia files. They, as well as text data, can contain personal or critically important information that requires reliable encryption and storage mechanisms. However, even with the availability of advanced cryptographic methods, text and graphic files remain vulnerable due to specific structural features.Text data typically exhibits statistical patterns, such as the frequency distribution of characters and words, which can be exploited for cryptanalytic attacks when weak or similar ciphers are used. In graphic files, one of the key risks is the high correlation between neighboring pixels, especially in the case of natural images or data with minimal compression, which creates the possibility of reconstructing or analyzing even partially encrypted information. An additional threat is metadata (EXIF, IPTC, XMP), which is automatically added when creating or editing files and may contain confidential information about the origin or properties of the data. The paper proposes a combined algorithm for protecting text and graphic files, aimed at eliminating the above vulnerabilities. The algorithm implements a multi-level symmetric scheme that combines three stages: AES-CBC, block permutation and AES-GCM. The keys are formed based on a password and a unique salt, which increases resistance to brute force attacks. The main goal is to form a distribution of bytes of encrypted data that is as close to uniform as possible, which minimizes the possibility of their recovery by statistical analysis methods. To confirm the effectiveness of the algorithm, statistical tests built into the Matlab environment were used, including entropy, χ^2, Kolmogorov–Smirnov, and correlation. The results demonstrated a significant increase in entropy and a decrease in the level of correlation between elements after encryption, which indicates the achievement of the property of uncertainty of the input data. Practical use of the algorithm provides for flexible configuration - the user can choose a compromise between the level of cryptographic strength and compression rates when creating protected archives. Thus, the proposed approach provides comprehensive protection of various types of digital information, combining high efficiency with adaptability to specific practical needs.

Keywords: encryption, redundancy, graphic and text information, data authentication.

DOI 10.15276/imms.v15.no3.430
УДК 004.31:004.22

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 430-438

МЕТОДИ ТА СПЕЦПРОЦЕСОРИ ВИЗНАЧЕННЯ ЕНТРОПІЇ СПЕКТРАЛЬНОЇ ХАРАКТЕРИСТИКИ СИГНАЛІВ

А. І. Сегін[1], О. М. Заставний[2], Н. Я. Возна[3], Ю.І. Попик[4]

Західноукраїнський національний університет
11, Львівська, Тернопіль, 46009, Україна
Emails: andriy.segin@gmail.com[1], olegz80@gmail.com[2], nvozna@ukr.net[3], yup@wunu.edu.ua[4]

Ентропійний аналіз є ефективним інструментом, який може використовуватися в найрізноманітніших сферах науки і техніки. На сьогоднішній день він дещо недооцінений, внаслідок розвитку інших інформаційних технологій, таких як нейронні мережі, штучний інтелект, методи обробки великих даних та інших. Проте, використання ентропії можна поєднувати з перерахованими інформаційними технологіями, досягаючи хороших результатів. Крім того, оцінку ентропії можна використовувати як самостійний інструмент аналізу інформаційних характеристик сигналів. Інформація відіграє дедалі більше значення в усіх сферах діяльності людини. З розвитком інтернету, комунікаційних та комп'ютерних мереж, мобільного зв'язку та інших безпровідних телекомунікаційних технологій обсяг інформації, яку необхідно обробляти, невпинно зростає. При цьому, оцінки ентропії в різних їх варіаціях, як один з елементів теорії інформації, є сильним засобом обробки та аналізу інформаційних характеристик потоків даних даних. В статті акумульовано розрізнену інформацію про різноманітні оцінки ентропії та показано розвиток теоретичних положень. Представлено також дослідження властивостей ентропії дискретних сигналів. Показана можливість організації ліній передачі даних на основі ентропійно-маніпульваних сигналів, за рахунок чого можна досягнути високої завадозахищеності. Крім того, запропоновано використовувати ентропійно-маніпульвані сигнали, які базуються на обчисленні ентропії не амплітуди сигналів, а їх спектральних характеристик. Для визначення ентропії спектру сигналів розроблено структуру спецпроцесора та описано принцип його функціонування. Визначення ентропії по частоті сигналу дозволяє підвищити криптографічну стійкість та завадозахищеність передавання інформації. Запропонований спецпроцесор призначений для використання в системах прийому/передавання даних в каналах з підвищеною завадостійкістю.

Ключові слова: ентропія, спецпроцесори, теорія інформації, спектр сигналу, телекомунікаційні системи, завадозахищені сигнали, ентропійно-маніпульовані сигнали.

Вступ. З часу опублікування відомої статті Клода Шенона [1], в якій він визначив поняття ентропії, вона в основному використовувалася для оцінок інформаційних характеристик джерел інформації, повідомлень, каналів з'язку, кодів [2] та іншого. З розвитком комп'ютерної та мікропроцесорної техніки її застосування стає все частішим в найрізноманітніших сферах. Так, оцінка ентропії використовується в системах діагностування медичного призначення [3], захисту даних в інформаційних каналах [4], завадозахищенему передаванні даних [5], для чисельної оцінки образного сенсу вербальних конструкцій [6].

Розширення сфери застосувань ентропійних оцінок потребує подальшого розвитку теорії, методів та пристроїв її визначення. Це обумовлюється потребою в адаптації самої оцінки у відповідності до конкретної сфери її використання, необхідністю підвищення точності та швидкості її розрахунку та іншими вимогами. В даній роботі проведено аналіз існуючих оцінок ентропії та представлено архітектуру вдосконаленого спецпроцесора обчислення ентропії, який характеризується

підвищеною швидкодією, що особливо актуально для кібер-фізичних систем реального часу, які використовують ентропійні характеристики.

Огляд літератури. Виокремленням теорії інформації в самостійний напрямок вважається стаття Клода Шенона «Математична теорія зв'язку» в технічному журналі Bell System, в якій математично сформульовані основні положення, в тому числі визначено поняття ентропії в її інформаційному аспекті. В подальшому вона була розвинута в його наступних публікаціях [7].

Л. Г. Лапи в своїх працях [8] відмітив, що необхідні детальні характеристики кореляційних зв'язків між різними символами для точнішого визначення ймовірнісних показників джерел інформації (ДІ). Він довів, що збільшення кореляційних зв'язків між станами ДІ, веде до збільшення нерівноймовірності розподілу умовної ймовірності у виразі визначення ентропії ДІ з залежними станами, що в свою чергу, призводить до зменшення ентропії джерела. Оскільки властивість ергодичних ДІ визначається розповсюдженням кореляційних зв'язків на скінченну кількість символів, то для визначення ентропії необхідно включити кореляційну функцію на цю скінченну кількість символів.

В роботі Л. Г. Лапи також звертається увага на те, що функція ентропії Шенона використовує виключно одновимірні розподіли імовірностей, в той час як кореляційна функція використовує двовимірні ймовірнісні розподіли. Тому принципово оцінка ентропії на базі кореляційної функції змістовніша, ніж функція ентропії Шенона.

До подібних висновків приходить Ж. Макс [9], визначаючи вплив коефіцієнта кореляції на оцінки ентропії. Ф. Г. Ланге [10] доводить, що врахування математичного сподівання двовимірної щільності ймовірності – кореляція, дозволяє точніше здійснити оцінку ентропії, ніж середні одновимірної щільності.

С. Голдман [11], розширюючи теорію інформації Шенона, доводить, що кореляційний аналіз зв'язує спектральну теорією з теорією інформації.

На базі доведень та висновків зазначених авторів, стає очевидним необхідність врахування кореляційних зв'язків у визначенні шенонівської оцінки ентропії. В подальшому, теорію визначення ентропії розвивав Николайчук Я. М. [12] та його наукова школа. Ним було запропоновано визначення ентропії на основі структурної функції Колмогорова [13], а в подальшому – на основі кореляційної функції еквівалентності [14]. Узагальнений аналіз та розвиток теорія побудови ентропійних моделей здійснено в роботі [15].

Мета роботи. Метою цієї роботи є вдосконалення спецпроцесорів визначення ентропії, які можуть використовуватися в телекомунікаційних системах для підвищення завадостійкості передачі сигналів. Для досягнення мети потрібно вирішити наступні завдання:

– аналіз оцінок визначення ентропії на основі кореляційних функцій;

– аналіз існуючих пристроїв визначення ентропії та їх характеристик;

– розробка методу визначення ентропії сигналів на основі їх частотного представлення;

– розробка структури спецпроцесора визначення ентропії спектральних характеристик сигналу.

Теоретичні положення визначення ентропії. Ентропія за Шеноном для дискретних сигналів визначається відомим виразом:

$$H = -\sum_{i=1}^{n} p(x_i) \cdot log_2 p(x_i) \qquad (1)$$

де x_i – дискретні значення сигналу;

$p(x_i)$ – імовірність появи дискретного відліку x_i;

n – загальна кількість відліків дискретного сигналу.

Д. Мідлтон [16] в розвиток шенонівської ентропії для дискретних сигналів, які

формуються послідовністю символів довільної довжини в певному порядку розподілених в часі, запропонував власну оцінку ентропії. Для дискретного випадкового сигналу $X=\{x_i\}$, кожен із відліків якого x_i, може приймати одне з l_i різних значень ($l \le l_i \le L;\ i=1,\ 2,\ \ldots,\ n$), отримав вираз для апріорної невизначеності $x_1,\ldots,x_i,\ldots,x_n$:

$$H(X)=-\sum_{l_1}^{L}\ldots\sum_{l_n}^{L}p(X)\log p(X); \tag{2}$$

де сума здійснюється по всім можливим варіантам кожного з відліків x_i сигналу.

Для дискретних сигналів з статистично залежною послідовністю значень Д. Мідлтон запропонував вираз середньої умовної ентропії:

$$H(X/Y)=\sum_{l_1}^{L}\ldots\sum_{l_n}^{L}\sum_{m_1}^{M}\ldots\sum_{m_k}^{M}p(x_1,\ldots,x_n,y_1,\ldots y_m)\cdot\log p(x_1,\ldots,x_n/y_1,\ldots,y_m); \tag{3}$$

де x_i, y_i – статистично залежні стани ДІ.

З останнього виразу випливає, що для розрахунку ентропії таких ДІ необхідно знати сумісні щільності імовірностей різного порядку $W_1(y_1,t_1)$, $W_1(y_1,t_1;y_2,t_2)$,..., $W_1(y_1,t_1;\ldots;y_n,t_n)$. При вивченні статистичних характеристик сигналів обґрунтовано, що на практиці вони не є настільки статистично складними, щоб їх описувати багатомірними розподілами. Тому для достатньо повного опису ергодичних стаціонарних сигналів достатньо застосовувати тільки двомірні розподіли. Зрозуміло, що їх ентропія і швидкість передачі повідомлень, за рахунок кореляційних зв'язків між різними послідовностями символів і нерівномірності розподілу їх імовірності, виявляються меншими в порівнянні з ентропією Шенона.

Багаторазовими дослідженнями [17] реальних об'єктів управління і джерел інформації показано, що стохастичні параметри дискретних сигналів на локальних проміжках часу досить точно описуються моделлю гаусівського закону розподілу ймовірностей.

Оцінка ентропії джерел з корельованими станами, які мають гаусівський закон розподілу, визначається за виразом [15]:

$$h[x(t),x(t+\tau)]=\log_2\left(2\pi\sigma_{\circ x}^{2}\sqrt{1-\rho_{xx}^{2}(\tau)}\right)+\frac{1}{1-\rho_{xx}^{2}(\tau)}\log_2 e-$$
$$-\frac{\rho^{2}{}_{xx}(\tau)}{1-\rho_{xx}^{2}(\tau)}\log_2 e=\log_2\left(2\pi e\sigma_{\circ x}^{2}\sqrt{1-\rho_{xx}^{2}(\tau)}\right) \tag{4}$$

.

Розрахунок ентропії дискретного сигналу з нерівноймовірними корельованими станами здійснюється за виразом:

$$H[x_i,x_{i+j}]=\log_2 2\pi e+\log_2\sigma_{\circ x}^{2}+\frac{1}{2}\log_2[1-\rho_{xx}^{2}(j)]; \tag{5}$$

де перший доданок є константою, що пов'язана із типом закону розподілу випадкової величини, другий доданок визначає дисперсію:

$$\sigma_{\circ x}^{2}=\frac{1}{N-1}\sum_{i=1}^{N}\left(x_i-\frac{1}{N}\sum_{i=1}^{N}x_i\right)^2,$$

а третій елемент характеризує взаємну ентропію корельованих нерівноймовірних відліків сигналу на основі квадрату нормованої функції автокореляції:

$$\rho_{xx}(j)=\frac{\frac{1}{N}\sum_{i=1}^{N}\left(x_i-\frac{1}{N}\sum_{i=1}^{N}x_i\right)\cdot\left(x_{i+j}-\frac{1}{N}\sum_{i=1}^{N}x_i\right)}{\frac{1}{N-1}\sum_{i=1}^{N}\left(x_i-\frac{1}{N}\sum_{i=1}^{N}x_i\right)^2}. \tag{6}$$

Розрахунок ентропії дискретного сигналу на базі нормованої автокореляційної функції $\rho_{xx}(j)$ є незручним при обчисленні в зв'язку з необхідністю центрування послідовності x_i у відповідності до (6). Тому для визначення ентропії сигналу пропонується на основі структурної функції Колмогорова і відповідно формула (5) набуде вигляду вигляду:

$$\begin{aligned}H(x_i,x_{i+j})&=log_2\,2\pi e\sqrt{D_x^2-D_x^2\cdot\rho_{xx}^2(j)}=\\&=log_2\,2\pi e+\frac{1}{2}log_2\left(\left[D_x-R_{xx}(j)\right]\cdot\left[D_x+R_{xx}(j)\right]\right);\end{aligned} \tag{7}$$

де $R_{xx}(j)=D_x\cdot\rho_{xx}(j)$ – кореляційна функція сигналу.

Кореляційна функція для стаціонарних процесів $R_{xx}(j)$ легко можна виразити через коваріаційну функцію $K_{xx}(j)$, яка швидша в обчисленні через відсутність операції центрування. Тоді визначення ентропії на основі коваріаційної функції матиме вигляд:

$$\begin{aligned}H(x_i,x_{i+j})&=log_2\,2\pi\,e\sqrt{D_x^2-D_x^2\cdot\rho_{xx}^2(j)}=\\&=log_2\,2\pi\,e+\frac{1}{2}log_2\left(\left[D_x-K_{xx}(j)\right]\cdot\left[D_x+K_{xx}(j)\right]\right)\end{aligned} \tag{8}$$

Аналітичне співвідношення структурної та автокореляційної функцій визначається виразом

$$C_{xx}(j)=2\left|D_x+M_x^2-K_{xx}(j)\right|=2\left[D_x-R_{xx}(j)\right]$$

Підставивши його в (7), отримаємо оцінку ентропії:

$$H(x_i,x_{i+j})=log_2\,2\pi\,e+\frac{1}{2}log_2\left[\frac{C_{xx}(j)}{2}\left(2D_x-\frac{C_{xx}(j)}{2}\right)\right]. \tag{9}$$

Якщо визначити середнє значення ентропії сигналу, отримаємо робочу формулу міри ентропії

$$\overline{H(x_i,x_{i+j})}=\frac{1}{2T}\sum_{j=1}^{T}log_2(2\pi e)^2\left[\frac{C_{xx}(j)}{2}\left(2D_x-\frac{C_{xx}(j)}{2}\right)\right],$$

або

$$\overline{H(x_i,x_{i+j}x_i)}=\frac{1}{2T}\sum_{j=1}^{T}log_2(2\pi\,e)^2\left[C_{xx}(j)\left(D_x-\frac{C_{xx}(j)}{4}\right)\right]; \tag{10}$$

де T – інтервал усереднення.

Дослідження властивостей ентропії дискретних сигналів. Ентропія кожного окремого відліку дискретного сигналу за Шеноном визначається виразом:

$$H_i=-\,p(x_i)\cdot log_2 p(x_i). \tag{11}$$

де $p_i=\frac{n_i}{N}$ – імовірність появи *i*-го відліку; H_i

n_i – кількість відліків x_i з загальної вибірки сигналу.

Якщо прийняти, що загальна кількість відліків дискретного сигналу N, то для зручності подальшого дослідження (11) можна переписати в іншому вигляді:

$$H = -\frac{n_i}{N} log_2 \frac{n_i}{N} = \frac{n_i}{N}\left(log_2 N - log_2 n_i\right). \qquad (12)$$

З даного виразу (12) можна визначити розподіл ентропії при різних кількостях появи x_i значення. Якщо для наочності представлення результатів прийняти $N = 256$ і вважати, що всі дискретні відліки є статистично незалежними, тоді графік ентропії згідно (12) матиме вигляд представлений на рис. 1, де по осі абсцис відраховується кількість значень x_i з загального об'єму вибірки N, а по осі ординат – відповідне значення ентропії.

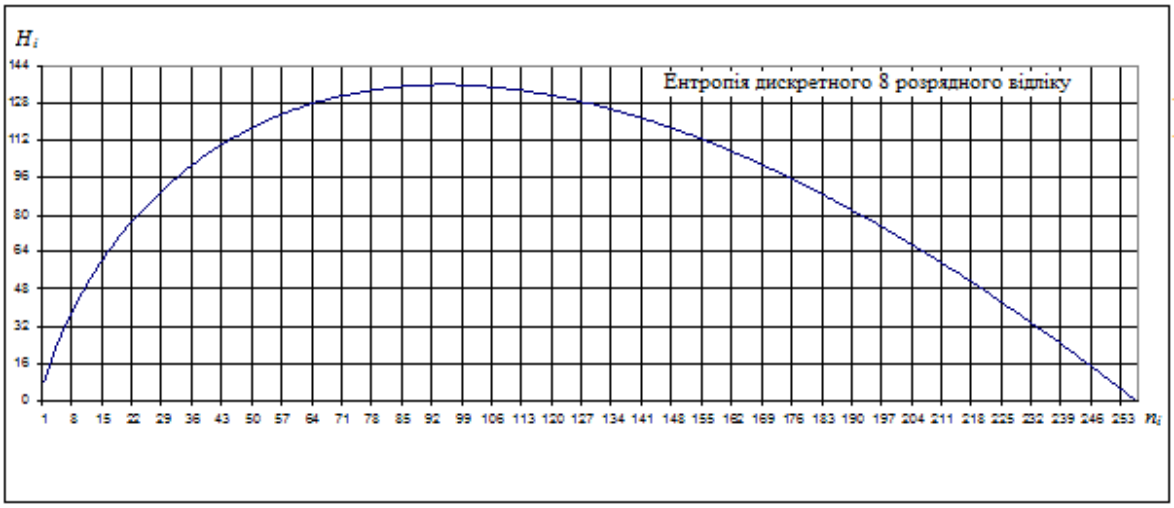


Рис 1. Графік ентропії при різних значеннях n_i появи x_i, для $n_i = \overline{1, N}$

Як видно з представленого графіку на рис. 1 та проведених розрахунків, максимальне значення ентропії буде при $n_i = 94$, при всіх інших значеннях n_i ентропія приймає попарно однакові значення. Цю властивість можна використати для побудови АЦП та спецпроцесорів для отримання ентопійно-маніпульованих сигналів.

До цього часу розглядалися міри визначення ентропії амплітуди сигналів. Проте відомо, що цифрова обробка сигналів здійснюється в основному в їх частотному представленні. Тому природним розвитком є визначення ентропії для спектральних характеристик сигналу, тобто визначається ентропія спектральних значень.

Якщо деякий сигнал представлений в часовому просторі:

$$s(t) = \sum_{i=-\infty}^{\infty} s(i \cdot \Delta t) \cdot s_0(t - \Delta t),$$

де $s(t)$ – аналоговий сигнал;

Δt – крок дискретизації,

то його спектральна характеристика буде мати вигляд:

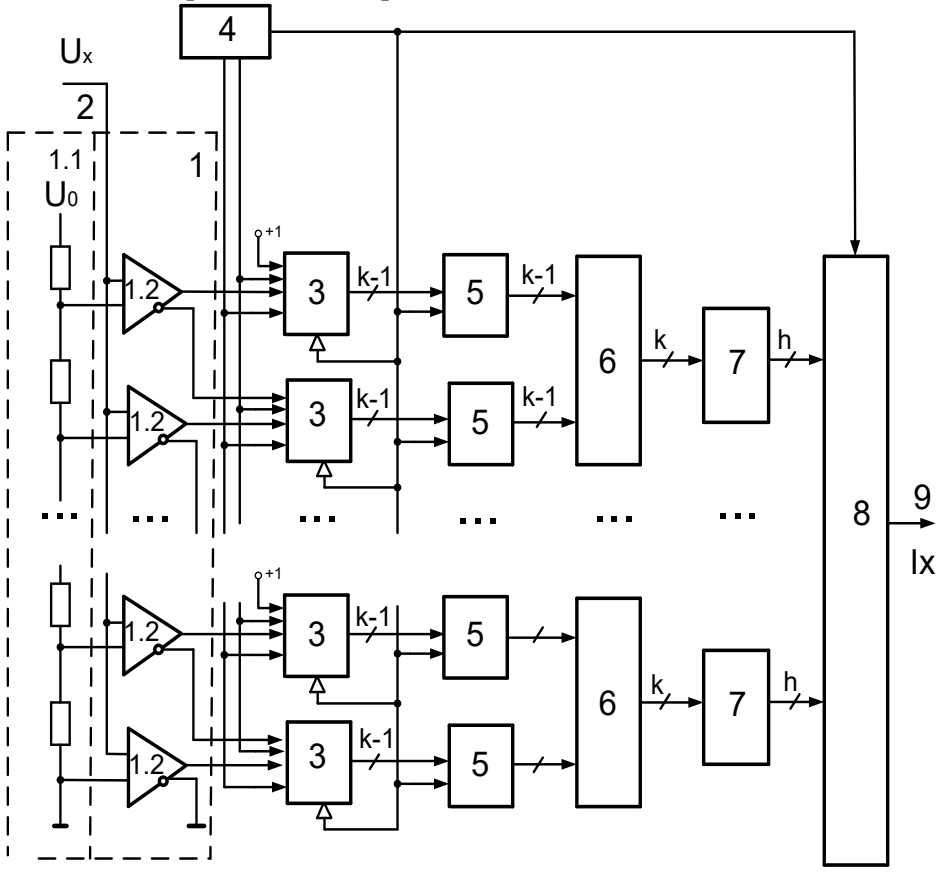
$$S(\omega) = \frac{s(t)}{\Delta t} \sum_{j=-\infty}^{\infty} S\left(\omega - \frac{2 \cdot \pi \cdot j}{\Delta t}\right).$$

Якщо повернутися до прийнятих позначень дискретного сигналу: $x_i = s(\Delta t \cdot i)$, то йому буде відповідати дискретна частотна характеристика: $s_j = S(\Delta\omega \cdot j)$. Відповідно, при обчисленні ентропії будемо використовувати замість значень ймовірностей відліків амплітуди сигналу $p(x_i)$, значення ймовірностей його спектру $p(s_j)$. Тоді ентропія спектру сигналу буде визначатись за виразом:

$$H_i = - p(s_j) \cdot log_2 p(s_j). \qquad (13)$$

Таким чином, для організації ліній передачі даних на основі ентропійно-маніпульваних сигналів можна досягнути високої завадозахищеності, оскільки завади на певних частотах не будуть призводити до критичної зміни ентропії спектру. Для реалізації таких ліній зв'язку на основі ентопійно-маніпульваних сигналів, в яких ентропія визначається не по амплітудних, а частотних характеристиках сигналу необхідно спроектувати відповідний спецпроцесор для обчислення ентропії спектру.

Структура спецпроцесора визначення ентропії частотних характеристик сигналів та його функціонування. Структура розробленого спецпроцесора базується на прототипі, схему якого подано на рис. 2 [18]. Представлений пристрій складається з АЦП 1, на вхід якого подається вхідний сигнал $x(t)$, який фактично нормалізований до відповідного діапазону напруги U_x. Дискретизовані значення з АЦП надходять на входи лічильників 3, робота яких узгоджується синхронізатором 4, відповідні значення підраховані лічильниками значення через визначену кількість тактів передаються в регістри пам'яті 5, шифраторів а з них на пірамідальні суматори 6. Отримані суми перетворюються шифраторами 7 у відповідний код та подаються на входи пірамідального суматора, на виході якого формується значення ентропії сигналу, позначеного на рисунку Ix. В якості компонентів суматорів 6 та пірамідального суматора 8 використаний й однорозрядний двійковий суматор з прямими входами та виходами структурна схема якого представлена на рис. 3.



1 - АЦП, 2 - інформаційний вхід пристрою, 1.1 - група взірцевих резисторів, 1.2 - компаратори з парафазними виходами (прямим та інверсним), 3 - лічильники, 4 - синхронізатор, 5 - регістри пам'яті, 6 – суматори; 7 - шифратори, 8 - пірамідальний суматор, 9 - вихід пристрою

Рис. 2. Структурна схема пристрою визначення ентропії із застосуванням парафазних компараторів

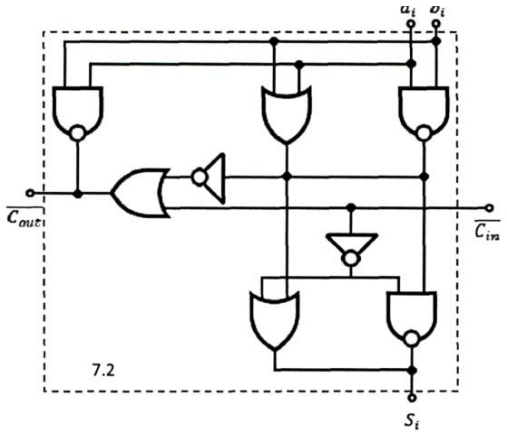
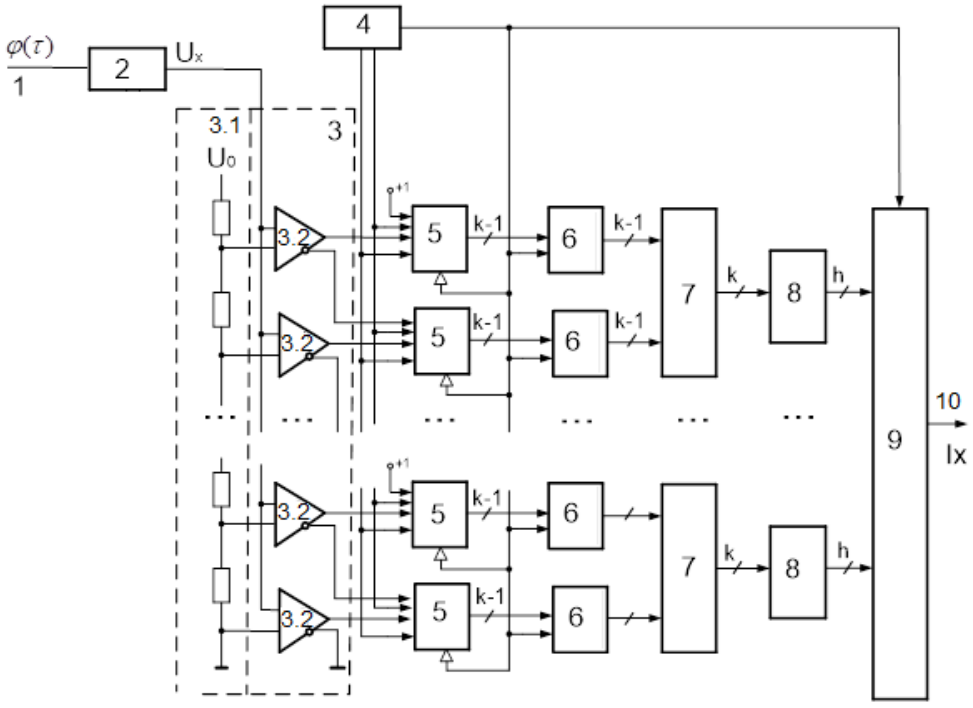


Рис. 3. Структура двійкового суматора з прямими входами та виходами

Підвищення швидкодії досягається застосуванням парафазних компараторів, швидкодія яких на порядок вища за традиційні JK-тригери, а також впровадженням паралельної обробки результатів через два (k-1)-розрядні регістри пам'яті та k-розрядний суматор з часовим зсувом тактування. Завдяки цим удосконаленням, загальна швидкодія пристрою зросла приблизно у три рази

В розробленому спецпроцесорі (рис. 4), на відміну від представленого на рис. 2, пропонується визначати ентропію частоти сигналу. На вхід пристрою подається значення спектральної характеристики, які за допомогою перетворювача частоти 2 приводяться до сигналу напруги U_x яка передається на вхід АЦП 3. Подальша робота пристрою аналогічна до прототипу представленого на рис.2.



1 – вхід пристрою, 2 – перетворювач частот, 3 - АЦП, 3.1 – група взірцевих резисторів, 3.2 - компаратори з парафазними виходами, , 4 - синхронізатор,
5 – лічильники, 6 – регістри пам'яті, 7 – суматори; 8 – шифратори, 9 - пірамідальний суматор, 10 – вихід пристрою.

Рис. 4. Структурна схема спецпроцесора визначення ентропії частотних характеристик сигналу

Визначення ентропії по частоті сигналу дозволяє підвищити криптографічну стійкість та завадозахищеність передавання інформації.

В результаті, на виході запропонованого пристрою отримаємо ентропію не амплітуди сигналу, а його частотної характеристики. Це забезпечить завадостійкість сигналу, що передається, навіть при наявності сильних завад на відповідних частотах. Це обумовлено тим, що при спотворенні сигналу на певних частотах його амплітудна характеристика сильно зміниться, проте на ентропію частоти це значно не вплине.

Очевидно, що запропонований пристрій втрачатиме у швидкодії, проте характеризується розширеними функціональними можливостями за рахунок визначення ентропії частоти сигналів. Його можна використовувати у системах прийому/передавання даних в каналах з підвищеною завадостійкістю.

Висновки. В роботі представлено перспективи розвитку та застосування ентропійного аналізу. Здійснено узагальнення теоретичного розвитку визначення ентропії та проаналізовано можливості їх застосування в різних сферах. Досліджено властивості ентропії дискретних сигналів та запропоновано її використання для створення завадозахищених каналів передачі даних. Для швидкого розрахунку ентропії сигналів представлено спецпроцесори визначення ентропії. Також запропоновано використовувати ентропійно-маніпульовані сигнали, які базуються на розрахунку ентропії не амплітуди сигналів, а їх спектральних характеристик. Розроблено архітектуру спецпроцесора для обчислення ентропії частотних характеристик дискретних сигналів.

Список літератури

1. Shannon C.E. A Mathematical Theory of Communication. *Bell System Technical Journal*, Vol. 27, pp. 379–423, 623–656.
2. Николайчук Я.М. Теорія джерел інформації. Тернопіль: ТНЕУ, 2008. 536с.
3. Мельничук С.І., Василик В.М. Можливості використання оцінок ентропії при опрацюванні сигналів в інформаційних діагностичних системах. *Вісник Хмельницького національного університету* ’2011. №3. С. 175—179.
4. Мельничук С. І., Козленко М. І., Гарматій О. Б. Ентропійні методи захисту даних в інформаційних каналах комп’ютерних систем. *Проблемно-наукова міжгалузева конференція Інформаційні проблеми комп'ютерних систем, юриспруденції, економіки та моделювання. Бучач, Україна.* 2008. URL: DOI: 10.5281/zenodo.5520045
5. Козленко М. І., Мельничук С. І. Дослідження завадостійкості способу передавання та приймання інформації на основі широкосмугових сигналів зі змінною ентропією для дискретних повідомлень. *Електроніка та зв'язок*. 2007. № 2(37). С. 82 - 92.
6. Бісікало О. В., Кондратюк Н.В. Застосування поняття ентропії для чисельної оцінки образного сенсу вербальних конструкцій. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/28825/1/verbal%20constructions.pdf
7. Шенон К. Работы по теории информации и кибернетике. М.: Иностранная литература, 1963, 830с.
8. Лапа В. Г. Математичні основи кібернетики. К.: «Вища школа», 1974. 452с.
9. Макс Ж. Методы и техника обработки сигналов при физических измерениях: М.: Мир, 1983. Т. 1. 311 с.; Т. 2. 256 с.
10. Ланге Ф. Статистические аспекты построения измерительных систем. М.: Радио и связь, 1981. 168с.
11. Голдман С. Теория информации. М.: Изд-во иностранной литературы, 1975. 382 с.
12. Николайчук Я.М. Розробка теорії і комплексу технічних засобів формування, передачі і обробки цифрових повідомлень в низових обчислювальних мережах автоматизованих систем: дис.д-ра .техн. наук. Івано-Франківськ, ІФІНГ, 1991. 573 с
13. Колмогоров А. Н. Теория вероятности и математическая статистика. М.: Наука, 1986. 534 с.

14. А. с. 1317455 СССР, МКИ G 06 F 15/36. Многоканальное устройство для вычисления функции эквивалентности./ Я.Н. Николайчук и С.М. Ищеряков; Опубл. 30.04.87, Бюл. № 22.
15. Сегін А. І,. Николайчук Я. М. Сабадаш І. О. Теорія побудови ентропійних моделей складних об'єктів управління на базі кореляційних функцій. Оптико-електрон. інформ.-енерг. технології. 2002. № 1. С. 69-79.
16. Миддлтон Д. Введение в статистическую теорию связи. М: Советское радио, 1961. 768 с
17. Кузьмин И. В., Кедрус В. А. Основы теории информации и кодирования. К.: Выща школа, 1986. 238 с
18. Николайчук Я.М., Сегін А.І., Возна Н.Я., Грига В.М. Пристрій для визначення ентропії: Пат.156501 Україна МПК G06F 17/10 (2006.01). № u2023 05558 заявл. 20.11.2023; опубл. 03.07.2024 Бюл. №27.

METHODS AND SPECIAL PROCESSORS FOR DETERMINING THE ENTROPY OF THE SPECTRAL CHARACTERISTICS OF SIGNALS

A. I. Segin[1], O. M. Zastavny[2], N. Ya. Vozna[3], Yu.I. Popyk[4]

West Ukrainian National University
11, Lvivska Str., Ternopil, 46009, Ukraine
Emails: andriy.segin@gmail.com[1], olegz80@gmail.com[2], nvozna@ukr.net[3], yup@wunu.edu.ua[4]

Entropy analysis is an effective tool that can be used in a wide variety of fields of science and technology. Today, it is somewhat underestimated, due to the development of other information technologies, such as neural networks, artificial intelligence, big data processing methods, and others. However, the use of entropy can be combined with the listed information technologies, achieving good results. In addition, entropy estimation can be used as an independent tool for analyzing the information characteristics of signals. In the modern world, information plays an increasingly important role in all areas of human activity. With the development of the Internet, communication and computer networks, mobile communications and other wireless telecommunication technologies, the amount of information that needs to be processed is constantly growing. At the same time, entropy estimation in its various variations, as one of the elements of information theory, is a powerful tool for processing and analyzing the information characteristics of data streams. The presented article accumulates disparate information on various estimates of entropy and shows the development of theoretical positions. The study of the properties of entropy of discrete signals is also presented. The possibility of organizing data transmission lines based on entropy-manipulated signals is shown, due to which it is possible to achieve high noise immunity. In addition, it is proposed to use entropy-manipulated signals, which are based on calculating the entropy not of the amplitude of signals, but of their spectral characteristics. To determine the entropy of the signal spectrum, the structure of a special processor has been developed and the principle of its operation is described. Determining entropy by signal frequency allows to increase cryptographic stability and noise immunity of information transmission. The proposed special processor is intended for use in data reception/transmission systems in channels with increased noise immunity.
Keywords: entropy, special processors, information theory, signal spectrum, telecommunication systems, noise-protected signals, entropy-manipulated signals.

DOI 10.15276/imms.v15.no3.439
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 439-453

ІМІТАЦІЙНА МОДЕЛЬ КІБЕРІМУННОЇ СИСТЕМИ: ПЕРЕНЕСЕННЯ МЕДИЧНИХ ПРИНЦИПІВ У СУЧАСНИЙ КІБЕРЗАХИСТ

О.А. Сиропятов, Л.М. Тимошенко

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044,Україна
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

Представлено міждисциплінарний підхід до підвищення стійкості інформаційних систем шляхом перенесення принципів біологічної імунної системи та медичних протоколів у галузь кібербезпеки. Проведено порівняльний аналіз фаз розвитку біологічних інфекцій (COVID-19, гепатит А) та сучасних кібератак (PlugX Worm, ILOVEYOU), що дозволило виявити структурні паралелі й визначити універсальні стратегії реагування. Особливу увагу приділено можливості інтеграції медичних принципів у архітектуру сучасних IDS/IPS на прикладі системи SURICATA. Описано ключові обмеження аналогій, пов'язані з відмінностями у механізмах передачі, архітектурі середовища та поведінці загроз. Запропоновано концептуальну імітаційну модель кіберімунної системи, яка базується на багаторівневій структурі, самонавчанні, автоматичній корекції політик і формуванні кіберпам'яті. Модель охоплює компоненти, що відповідають за моніторинг, швидке реагування, аналітику, накопичення знань та еволюцію захисних механізмів. Проведено порівняння з класичними SIEM-системами та показано, що імунна модель забезпечує вищу швидкість реагування, кращу адаптивність і можливість накопичення колективного знання про загрози. Практична значимість дослідження полягає у можливості використання імітаційного моделювання для валідації нових підходів до кіберзахисту, оптимізації процедур реагування та профілактики. Стаття закладає підґрунтя для подальших досліджень у сфері інтеграції медичних принципів у кібербезпеку, пропонуючи концепцію децентралізованих, самонавчальних і стійких систем захисту нового покоління.

Ключові слова: кіберімунна система, медичні протоколи, багаторівнева діагностика, SURICATA, імітаційна модель кіберімунної відповіді, кіберпам'ять, адаптивний захист.

Вступ. Сучасні інформаційні системи стикаються зі зростаючою складністю та динамічністю кіберзагроз, що вимагає пошуку нових, міждисциплінарних стратегій захисту [1]. Останні роки характеризуються не лише із зростанням кількості атак, а й появою складних цільових загроз, що використовують штучний інтелект, соціальну інженерію та автоматизовані інструменти для обходу класичних систем захисту. У такій ситуації актуальним стає пошук нових архітектур кіберзахисту, здатних до самонавчання, адаптації та формування «кіберпам'яті».

Кіберімунна система — це міждисциплінарна концепція, яка імітує принципи біологічної імунної системи та медичної діагностики для побудови стійких і адаптивних систем захисту даних. [2] Основними характеристиками такої системи є багаторівнева відповідь, механізми саморозпізнавання, формування кіберпам'яті, раннє виявлення загроз і можливість самонавчання на основі попереднього досвіду. Подібний підхід активно досліджується у світовій практиці, зокрема в контексті використання AI/ML для підвищення ефективності IDS/IPS-систем[3].

У статті [3] обґрунтовано концептуальну архітектуру кіберімунної системи та визначено основні принципи її функціонування. Однак для переходу від теорії до практики необхідна верифікація запропонованих аналогій на основі реальних сценаріїв атак і медичних протоколів. Зокрема, актуальним є питання: наскільки принципи медичних стратегій реагування на інфекційні захворювання можуть бути адаптовані для

побудови алгоритмів кіберзахисту. Відповідь дозволяє не лише теоретично обґрунтувати міждисциплінарну модель, а й розробити практичний інструментарій для вдосконалення сучасних систем безпеки.

Мета роботи: провести верифікацію концепції кіберімунної системи шляхом порівняльного аналізу протоколів лікування біологічних інфекцій та сценаріїв кібератак; дослідити можливість перенесення медичних принципів у архітектуру сучасних IDS/IPS на прикладі SURICATA; запропонувати прототип імітаційної моделі кіберімунної відповіді, яка окреслює потенційні напрямки R&D для практичного впровадження.

Завдання: здійснити порівняльний аналіз етапів розвитку та протоколів реагування на прикладі пар аналогій (COVID-19 ↔ PlugX Worm, гепатит А ↔ ILOVEYOU); дослідити можливість інтеграції медичних принципів у сучасні системи кіберзахисту; запропонувати концепцію імітаційної моделі кіберімунної системи та визначити її обмеження.

Порівняльний аналіз етапів розвитку та протоколів реагування на прикладі пар аналогій (COVID-19 ↔ PlugX Worm, гепатит А ↔ ILOVEYOU). Для аналізу аналогій між біологічними інфекціями та сучасними кібератаками доцільно брати приклади, які чітко ілюструють ключові етапи розвитку загрози та реакції на неї.

COVID-19 – масштабна інфекція з вираженою фазовістю, а PlugX Worm – сучасний цифровий черв'як, що активно використовується для атак на різні системи.

Збудник COVID-19 - коронавірус SARS-CoV-2. Передача: повітряно-крапельний, контактний шляхи. Фази: експозиція, інкубація (2–14 днів), початкові симптоми, загострення, ускладнення, відновлення. Особливості: тривалий безсимптомний період, складність раннього виявлення, потреба в масовому тестуванні й ізоляції.

PlugX Worm - комп'ютерний черв'як із функціями бекдору. Шляхи проникнення: використання вразливостей ОС, фішингові листи, заражені USB-носії, RDP. Фази: початкове проникнення, прихована присутність, активація, масове поширення, завантаження додаткових модулів, пошкодження інфраструктури. Особливості: маскування, автоматичне поширення, крадіжка даних, запуск додаткових атак

Обидва приклади мають чітко визначені етапи розвитку, що дозволяє провести структурний аналіз аналогій [3]. І COVID-19, і PlugX Worm вимагають системного підходу до виявлення, ізоляції, реагування та відновлення. На рис 1. показано етапи розвитку COVID-19 та PlugX Worm. Зліва наведені основні фази розвитку COVID-19, справа – відповідні етапи атаки PlugX Worm. Така паралельна візуалізація демонструє структурну подібність між біологічною інфекцією та сучасною цифровою атакою[4].

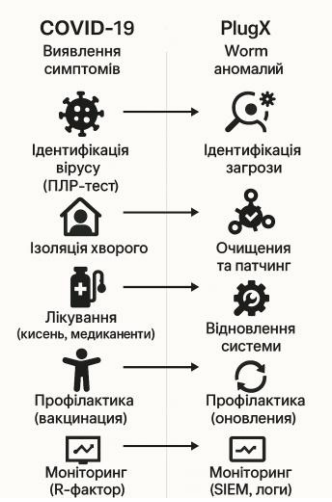


Рис.1. Етапи розвитку COVID-19 та PlugX Worm

Вона дозволяє швидко співставити критичні точки для раннього виявлення, ізоляції, реагування та відновлення в обох сферах. Схема підкреслює, що адаптація медичних

принципів може бути корисною для розробки ефективних стратегій кіберзахисту, але потребує врахування специфіки цифрового середовища[5].

Аналіз цієї пари дає змогу застосувати перевірені медичні підходи для розробки стратегій кіберзахисту, враховуючи сучасні технології та загрози.

Обидва процеси – біологічна інфекція та цифрова атака – мають чітко виражену фазову структуру. Це дозволяє не лише порівнювати окремі етапи розвитку загрози, а й знаходити спільні принципи реагування, які можуть бути корисними для побудови ефективних стратегій захисту в обох сферах. Таблиця 1 ілюструє ці паралелі.

Таблиця 1.

Етапи розвитку: біологічна та цифрова паралель

Фаза COVID-19	Етап атаки PlugX Worm	Опис аналогії
Експозиція	Первинне проникнення	Контакт із вірусом (людина) чи експлуатація вразливості/USB (PlugX)
Інкубаційний період	Прихована присутність	Безсимптомний розвиток інфекції або приховане перебування PlugX у системі до активації
Початкові симптоми	Активація шкідливого коду	Поява перших ознак хвороби чи запуск основних функцій PlugX
Загострення	Масове розповсюдження/завантаження модулів	Прогресування захворювання чи активне поширення PlugX мережею, завантаження додаткового ПЗ
Ускладнення	Пошкодження інфраструктури	Критичний стан організму або руйнування/шифрування цифрової інфраструктури, викрадення даних
Відновлення	Нейтралізація/відновлення	Реабілітація пацієнта або очищення й відновлення системи після атаки

Ця таблиця ілюструє, як структурна подібність фаз розвитку біологічної інфекції та цифрової атаки дозволяє адаптувати перевірені підходи з медицини для розробки ефективних стратегій кіберзахисту.

Ключові обмеження аналогії. Відмінність механізмів передачі: COVID-19 поширюється через фізичний контакт, PlugX – через мережу, USB-носії, фішингові листи [5]. Архітектурна різниця: імунна система діє в межах організму, PlugX часто атакує розподілені IT-інфраструктури. Пам’ять та еволюція: біологічна імунна пам’ять формується природним шляхом або вакцинацією; у PlugX кіберсистеми потребують спеціальних механізмів накопичення знань [6]. Метрики ефективності: медичні показники (летальність, реабілітація) не мають прямих відповідників у кібербезпеці (час виявлення, false positives/negatives) [7].

Визначення цих обме.жень дозволяє уникати некоректних узагальнень і формувати рекомендації, які враховують специфіку цифрового середовища.

Для деталізації особливостей сучасних атак PlugX наведено окрему таблицю 2, що підкреслює ключові характеристики кожного етапу.

Таблиця 2.

Порівняльна таблиця: особливості PlugX (2024)

Фаза біологічної інфекції	Етап PlugX-атаки	Особливості PlugX (2024)
Експозиція	Зараження через USB/мережу	Використання фішингу, USB-носіїв, RDP
Інкубація	Приховане перебування	Складні механізми маскування
Симптоми	Активація, крадіжка даних	Витік даних, запуск бекдорів
Загострення	Масове поширення, завантаження модулів	Завантаження додаткового ПЗ, lateral movement
Відновлення	Очищення системи, оновлення захисту	Відкат систем, оновлення політик

Ця таблиця дозволяє побачити не лише загальні структурні паралелі, а й специфіку сучасних цифрових атак, що важливо для практичного застосування аналогій.

Деталізація допомагає зрозуміти, які підходи з медицини можуть бути корисними для кіберзахисту, а які потребують адаптації чи переосмислення. Водночас очевидно, що не всі принципи можна перенести без змін: відмінності у механізмах передачі, архітектурі середовища та поведінці загроз вимагають обережного й критичного підходу до використання аналогій. Пошук релевантних аналогій і критичний аналіз їхніх обмежень дозволяють не лише підвищити ефективність цифрових систем, а й забезпечити їхню стійкість до нових, раніше невідомих загроз.

Розглянемо аналогію гепатиту А ↔ сучасні атаки соціальної інженерії. Для аналізу аналогій між біологічними інфекціями з тривалим прихованим перебігом і сучасними кібератаками доцільно розглядати приклади, що демонструють залежність від соціальних контактів, пасивну фазу розвитку та відкладений масовий ефект. Гепатит А – класичний приклад інфекції з довгою інкубацією та соціальною передачею. У цифровому середовищі аналогічними є атаки, що поширюються через фішинг, вкладення у листах або соціальні мережі, зокрема історичний випадок ILOVEYOU та сучасні багатоступеневі фішингові кампанії.

Коротко про гепатит А**.** Передача: через інфіковану воду, їжу, побутові контакти. Фази: експозиція, інкубація (15–50 днів), продромальна, іктерична, відновлення. Особливості: тривалий безсимптомний період, приховане поширення, залежність від соціальних контактів.

Коротко про атаки типу ILOVEYOU і сучасний фішинг. Канал: електронна пошта, месенджери, соціальні мережі. Фази: експозиція (отримання листа/вкладення), інкубація (очікування дії користувача), активація, масове поширення, побічні ефекти, відновлення. Особливості: прихована фаза, залежність від людського фактору, лавиноподібне поширення через контакти.

Обидва процеси – біологічна інфекція та цифрова атака – мають фазову структуру з прихованим початком і залежністю від поведінки носіїв/користувачів. Це дозволяє порівнювати ключові етапи розвитку загрози та знаходити спільні принципи реагування. На рис 2. показано етапи розвитку гепатиту А і ILOVEYOU.

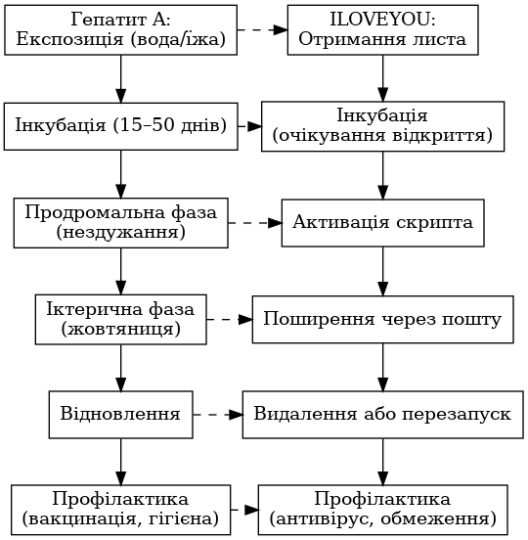


Рис. 2. Зіставлення фаз розвитку гепатиту А та етапів атаки вірусом ILOVEYOU

Далі наведена таблиця 3, яка ілюструє ці паралелі та структурну подібність фаз розвитку біологічної інфекції та цифрової атаки соціальної інженерії. Такий підхід дозволяє адаптувати медичні стратегії для підвищення ефективності кіберзахисту.

Таблиця 3.

Етапи розвитку: біологічна та цифрова паралель між гепатитом А та вірусом ILOVEYOU

Фаза гепатиту А	Етап атаки ILOVEYOU / сучасний фішинг	Опис аналогії
Експозиція	Отримання листа/вкладення	Контакт із джерелом: заражена їжа/вода або фішинговий лист
Інкубаційний період	Прихована присутність	Безсимптомне носійство або очікування дії користувача
Продромальна фаза	Перші ознаки (неспецифічні)	Незначні симптоми або підозріла активність, ще не розпізнана
Іктерична фаза	Активація, масове поширення	Явні симптоми або запуск шкідливого коду, автоматичне розсилання
Відновлення	Очищення системи, профілактика	Реабілітація організму або видалення шкідливого ПЗ, навчання

Ключові обмеження аналогії. Відмінність механізмів передачі: гепатит А – через фізичний контакт, їжу, воду; фішинг – через електронні канали. Інкубаційний період у біології має біохімічну природу, у кіберпросторі – це соціальний фактор (користувач сам запускає шкідливий код). Медична профілактика передбачає вакцинацію, у кіберзахисті – це навчання користувачів та автоматизовані засоби ізоляції. Відновлення після хвороби формує біологічну пам’ять, а у кіберзахисті потрібні спеціальні механізми накопичення знань (playbooks, сигнатури).

Визначення цих обмежень дозволяє уникати некоректних узагальнень і формувати рекомендації, які враховують специфіку цифрового середовища. У таблиці 4 показано особливості сучасних фішингових атак.

Таблиця 4.

Порівняльна таблиця: особливості сучасних фішингових атак

Фаза біологічної інфекції	Етап сучасної фішингової атаки	Особливості (2024–2025)
Експозиція	Отримання email/вкладення/посилання	Використання PDF, ZIP, LNK, SVG, QR-кодів
Інкубація	Приховане перебування	Очікування дії користувача, маскування
Симптоми	Активація, крадіжка даних	Витік даних, запуск бекдорів, credential theft
Загострення	Масове поширення, автоматизація	Автоматичне розсилання, використання AI
Відновлення	Очищення системи, оновлення захисту	Відкат систем, навчання користувачів

Така деталізація допомагає зрозуміти, які саме підходи з медицини можуть бути корисними для кіберзахисту, а які потребують адаптації чи переосмислення. Водночас очевидно, що не всі принципи можна перенести без змін: відмінності у механізмах передачі, архітектурі середовища та поведінці загроз вимагають обережного й критичного підходу до використання аналогій.

Тому наступним кроком є формулювання практичних рекомендацій для кіберзахисту – з урахуванням зазначених обмежень і специфіки сучасних IT-систем.

Рекомендації для кіберзахисту на основі аналізу аналогій COVID/PlugX та Гепатит А/ILOVEYOU. Аналіз аналогій між біологічними вірусними інфекціями (COVID-19, гепатит А) та цифровими атаками (PlugX, ILOVEYOU) дає змогу сформулювати універсальні підходи до підвищення стійкості кіберінфраструктури. Врахування медичних принципів дозволяє пропонувати більш гнучкі, багаторівневі й адаптивні стратегії захисту.

Багаторівнева діагностика та тестування. Доцільно впроваджувати кілька типів детекторів і аналізаторів для різних рівнів інфраструктури (мережа, кінцеві точки, пошта), що сприятиме своєчасному виявленню загроз навіть у розподіленому

середовищі. Варто застосовувати різні методи перевірки вкладень, посилань і файлів для підвищення ймовірності виявлення нових або складних атак.

Контекстна діагностика**.** Рекомендується аналізувати не лише сам факт інциденту, а й джерело, спосіб проникнення, особливості поведінки шкідливого коду чи листа. Використання даних про попередні атаки може підвищити точність реагування та дозволити формувати профілі ризику.

Карантин та ізоляція. Може бути доцільне автоматичне ізолювання підозрілих об'єктів (вкладень, вузлів, листів) до завершення аналізу. Сегментація мережі та ізоляція уражених зон здатна обмежити поширення атаки навіть у разі невідомого джерела загрози.

Формування кіберпам'яті. Рекомендується створювати та оновлювати бази знань про інциденти, сценарії реагування, ознаки компрометації. Використання накопиченого досвіду сприятиме пришвидшенню реагування на повторні чи схожі атаки.

Автоматизація реагування. Варто розглядати впровадження AI/ML для автоматичного виявлення аномалій, фішингових листів і шкідливих вкладень. Політики Zero Trust і концепція Digital Immune System можуть підвищити стійкість інфраструктури навіть у разі проникнення загрози.

Моніторинг ефективності та адаптація. Регулярний аналіз результатів реагування та коригування політик захисту з урахуванням нових типів атак і змін у структурі інфраструктури може підвищити ефективність системи. Автоматичний фідбек-цикл сприятиме постійному вдосконаленню захисних механізмів.

Навчання користувачів. Доцільно проводити регулярні тренінги з розпізнавання фішингу, шкідливих вкладень, соціальної інженерії. Моделювання атак може підвищити обізнаність персоналу й знизити ризики успішних атак соціальної інженерії.

Отже, багаторівневий підхід дозволяє виявляти як типові, так і нові, раніше невідомі загрози, мінімізуючи кількість хибних спрацювань. Контекстна діагностика підвищує точність реагування, дозволяє враховувати індивідуальні особливості інфраструктури та користувачів. Кіберпам'ять і автоматизація забезпечують швидке реагування та адаптацію системи до нових сценаріїв атак. Навчання користувачів підвищує загальний рівень кібергігієни та зменшує ймовірність успішних атак соціальної інженерії. Узагальнення досвіду боротьби з біологічними вірусами (COVID-19, гепатит А) та аналіз сучасних цифрових атак (PlugX, ILOVEYOU) підтверджують ефективність багаторівневого, адаптивного та самонавчального підходу до кіберзахисту. Інтеграція медичних принципів у архітектуру захисних систем може сприяти підвищенню стійкості інфраструктури до складних, цільових і нових загроз.

Дослідження можливості перенесення медичних принципів у архітектуру сучасних IDS/IPS на прикладі SURICATA. Покажемо практичну трансформацію ідей з медичної практики в інструменти кіберзахисту шляхом порівняння функціоналу системи SURICATA (IPS/IDS) із протоколами медичної імунної відповіді [1].

Водночас важливо визнати обмеження такого порівняння. Природа загроз у кіберпросторі та біологічних системах суттєво відрізняється: SURICATA працює з цифровими атаками (шкідливий трафік, експлойти), тоді як імунна система організму протидіє біологічним патогенам [4]. Метрики ефективності також різні: у медицині — це чутливість, специфічність, імунна пам'ять; у кіберзахисті — швидкість виявлення, FP/FN, масштабованість. Крім того, біологічна імунна система функціонує як єдиний цілісний механізм, тоді як IT-інфраструктури часто розподілені та гетерогенні.

Це порівняння не претендує на пряме зіставлення метрик ефективності. Його головна цінність – виявлення архітектурних і концептуальних подібностей та відмінностей і пошук напрямів вдосконалення IPS/IDS через запозичення медичних принципів: контекстуальності, динамічного моніторингу, самонавчання та профілактики [10].

Аналіз призначення SURICATA та її сучасні характеристики. SURICATA– це популярний інструмент з відкритим кодом, який поєднує сигнатурний і поведінковий підходи та інтегрується із SIEM-системами [8]. Проте його архітектура класично реактивна, орієнтована на фіксацію відомих загроз [9]. Це аналіз пакетів (Deep Packet Inspection) та підтримка масштабованих розгортань [12]. SURICATA запобігає атакам - сканування портів і мереж, DDoS-атаки, Brute-force та pass-the-hash атаки, експлуатація вразливостей протоколів, виявлення шкідливого трафіку (malware, botnet C2), аномалії в мережевій поведінці. На рис. 3 схематично зображено алгоритм роботи системи виявлення та запобігання вторгненням SURICATA. Діаграма демонструє основні етапи аналізу мережевого трафіку: від початкового захоплення та парсингу пакетів до прийняття рішень щодо блокування або подальшого моніторингу. Кожна гілка відображає логіку обробки подій – сигнатурний та аномальний аналіз, глибоку перевірку, генерацію алертів і блокування трафіку.

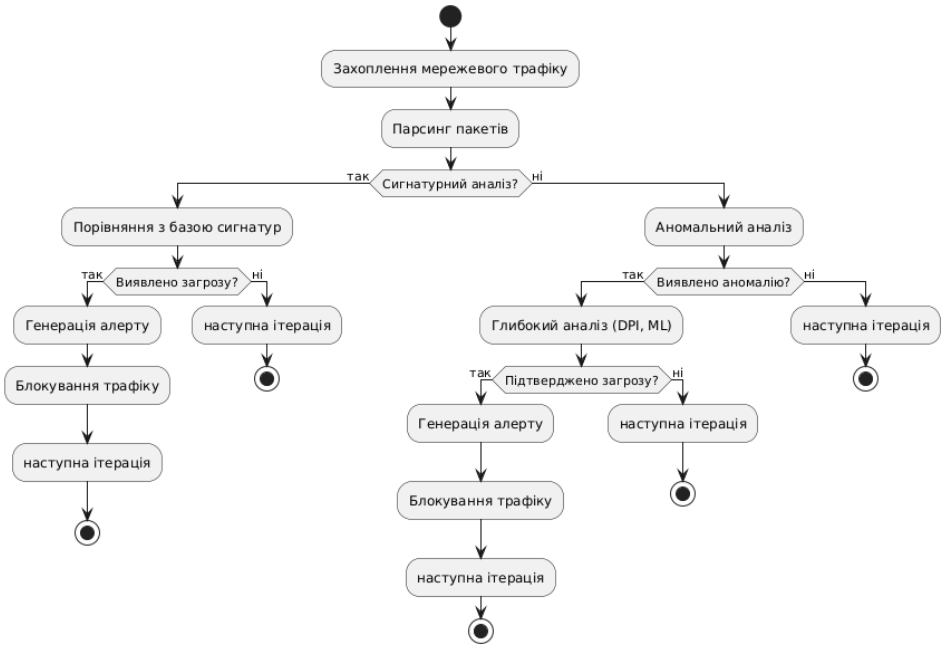


Рис.3. Алгоритм роботи системи SURICATA

Схема ілюструє те, що SURICATA працює у безперервному циклі: після завершення кожної ітерації система повертається до обробки нового трафіку. Відображено два основних підходи до аналізу – сигнатурний (порівняння з базою відомих загроз) та аномальний (виявлення нетипових патернів). Для підозрілих ситуацій передбачено глибокий аналіз із використанням DPI та машинного навчання – це підвищує точність і дозволяє реагувати на нові типи атак. Блок «наступна ітерація» підкреслює циклічність і постійну готовність системи до обробки нових загроз. Ключові алгоритми включають pattern matching, flow analysis, використання flowbits, підтримку динамічних правил та можливість інтеграції з ML-модулями.

Однак, навіть найсучасніші технології кіберзахисту мають обмеження, пов’язані з адаптивністю, контекстною обізнаністю та здатністю до самонавчання. Ці властивості є ключовими для природної імунної системи людини, яка протягом мільйонів років еволюціонувала для ефективного виявлення та нейтралізації вірусних загроз[1,4].

Для подальшого вдосконалення архітектури IDS/IPS доцільно звернутися до досвіду медицини, зокрема, до принципів і алгоритмів роботи імунної системи. Медичні протоколи виявлення вірусних атак побудовані на багаторівневій діагностиці, адаптивності, формуванні пам’яті та динамічній корекції реакцій організму. Їх аналіз дозволяє знайти нові підходи до підвищення ефективності кіберзахисту.

Далі розглянемо, як саме організовані алгоритми та принципи медичних протоколів виявлення вірусних атак, і які з них можуть бути імплементовані в сучасні системи захисту інформації.

Медичні протоколи виявлення вірусних атак: алгоритми та принципи

Медична імунна система людини є унікальним прикладом ефективної багаторівневої системи захисту, яка здатна виявляти, ідентифікувати й нейтралізувати широкий спектр вірусних загроз. Її принципи та алгоритми можуть слугувати джерелом ідей для вдосконалення сучасних систем кіберзахисту.

Основні алгоритми та принципи роботи імунної системи

1. Багаторівнева діагностика: імунна система застосовує поетапний підхід до виявлення патогенів. На першому рівні здійснюється швидкий скринінг (наприклад, неспецифічна імунна відповідь – фагоцитоз, інтерферони), а у разі підозри на інфекцію запускаються глибші лабораторні дослідження (специфічна імунна відповідь - активація Т- і В-лімфоцитів, вироблення антитіл). Такий підхід дозволяє ефективно фільтрувати більшість нешкідливих впливів і зосереджувати ресурси на справжніх загрозах.
2. Імунологічні методи розпізнавання антигенів: ключовим механізмом є розпізнавання чужорідних молекул (антигенів) за допомогою спеціалізованих рецепторів. Це аналог сигнатурного аналізу в IDS/IPS, коли система порівнює зразки з базою відомих загроз1,2,4]. Вироблення антитіл та активація клітинного імунітету забезпечують швидке реагування на знайомі патогени.
3. Адаптивність через формування імунної пам’яті: після контакту з вірусом імунна система формує клітини пам’яті, які дозволяють у майбутньому розпізнавати та нейтралізувати цей патоген значно швидше й ефективніше. Це забезпечує здатність системи навчатися на попередньому досвіді та підвищувати свою ефективність з часом.
4. Алгоритми визначення «своє-чуже»: імунна система використовує складні механізми для розмежування власних і чужорідних клітин та молекул. Алгоритми негативної селекції та клонального відбору дозволяють уникати автоімунних реакцій і зосереджуватися на реальних загрозах. Ці процеси нагадують машинне навчання: система формує набір правил для розпізнавання «чужого» на основі досвіду та селекції.
5. Динамічний моніторинг стану організму: постійний контроль за змінами у внутрішньому середовищі (температура, рівень запальних маркерів, поява нових антигенів) дозволяє імунній системі оперативно реагувати на нові загрози. Це аналог постійного моніторингу мережевого трафіку й поведінки у кіберзахисті.
6. Зворотній зв’язок для корекції імунної відповіді: імунна система здатна коригувати свою активність на основі результатів боротьби з патогеном: посилювати чи послаблювати реакцію, запобігати надмірному ушкодженню власних тканин. Такий механізм зворотного зв’язку є важливим для підтримки балансу між ефективністю захисту та мінімізацією побічних ефектів.

Для кращого розуміння принципів функціонування імунної системи людини схема відображає основні етапи виявлення та нейтралізації вірусних атак організмом. Вона ілюструє, як захист організму організований на різних рівнях – від швидкої неспецифічної відповіді до формування імунної пам’яті для забезпечення стійкості до повторних інфекцій.

Схема (рис.4) демонструє поетапний характер імунної відповіді від моменту проникнення вірусу до активації неспецифічного та специфічного захисту. Важливим етапом є виявлення антигену, після чого запускається адаптивна імунна відповідь із залученням Т- і В-лімфоцитів. Якщо виробляються антитіла, відбувається нейтралізація вірусу та формування імунної пам’яті, що забезпечує швидку реакцію при повторному зараженні. Динамічний моніторинг і зворотний зв’язок дозволяють коригувати інтенсивність імунної відповіді, підтримуючи баланс між ефективністю захисту та мінімізацією шкоди для організму. Такий багаторівневий і адаптивний підхід до захисту є орієнтиром для вдосконалення сучасних систем кібербезпеки.

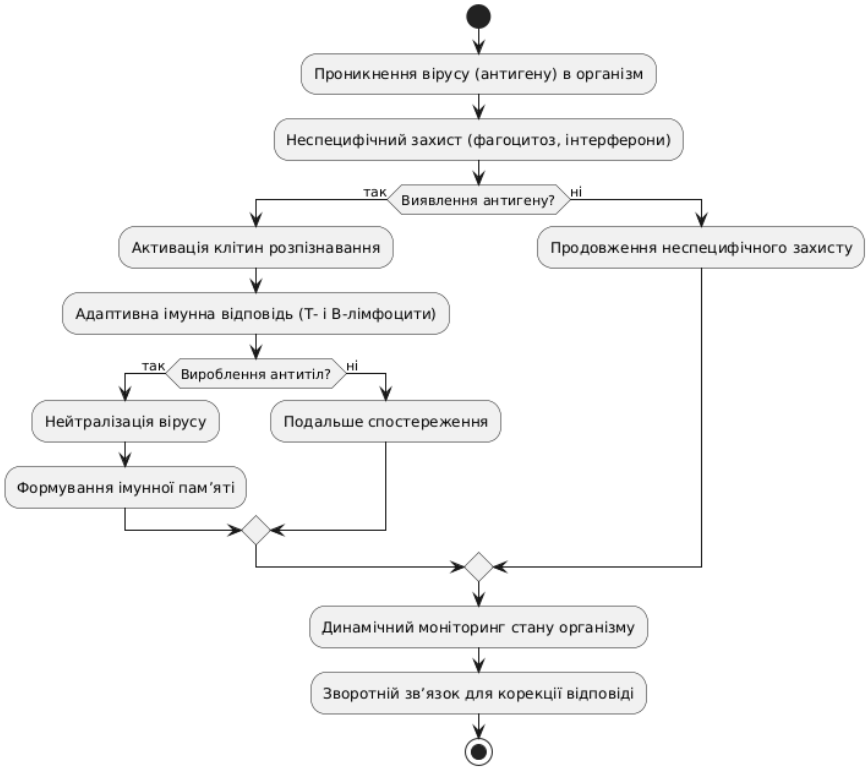


Рис.4. Алгоритм функціонування імунної системи людини

Порівняння алгоритмів SURICATA, медичних протоколів та концепції. Таке порівняння дозволяє не лише виявити спільні риси й ключові відмінності, а й визначити потенційні напрями розвитку сучасних систем кіберзахисту [10]. Концепція - практичний орієнтир для розвитку системи, відображає, як сучасна IDS/IPS може трансформуватися з реактивної у проактивну, самонавчальну й адаптивну платформу, якщо інтегрувати принципи, перевірені мільйонами років еволюції біологічних систем. Порівняння трьох моделей дозволяє чітко побачити, які саме функції вже реалізовані, які відсутні, а які можна впровадити для підвищення ефективності кіберзахисту.

SURICATA (імунна модель) виступає як міст між класичним підходом і майбутніми інтелектуальними системами, придатними до самонавчання, гнучкої адаптації, автоматичного оновлення політик і глибокого контекстного аналізу [13,14].

Отже, медична імунна система забезпечує гнучкий, багаторівневий і контекстно-чутливий захист для ефективного реагування на нові загрози; SURICATA (стандарт) зосереджена на швидкому сигнатурному виявленні, має обмежену адаптивність і контекстну обізнаність; SURICATA (імунна модель), як концепція, об'єднує кращі риси обох систем: багаторівневий аналіз, самонавчання, автоматичну корекцію політик, профілювання та повноцінну роботу з контекстом.

Розширене порівняння демонструє (таблиця 5), що інтеграція імунних принципів у архітектуру SURICATA відкриває шлях до створення дійсно адаптивної, стійкої та самонавчальної системи кіберзахисту нового покоління. Такий підхід дозволяє не лише підвищити точність виявлення складних атак, а й забезпечити гнучкість і швидкість реагування на нові, невідомі загрози.

Як концепція імунної моделі може покращити адаптивність SURICATA. Імунна модель в контексті кіберзахисту – це концепція, що запозичує принципи роботи біологічної імунної системи для побудови гнучких, самонавчальних і адаптивних систем виявлення та реагування на загрози. Її впровадження у SURICATA дає перейти від статичного, реактивного до динамічного, проактивного, контекстно-чутливого кіберзахисту.

Таблиця 5.

Порівняльна таблиця алгоритмів

Критерій	Медична імунна система	SURICATA (стандарт)	SURICATA (імунна модель, концепт)
Природа загроз	Біологічні патогени	Цифрові атаки	Цифрові атаки
Анамнез	Збір анамнезу	Відсутній	Контекстуальний профіль, історія подій
Скринінг	Багаторівневий	Сигнатурний	Сигнатурний + поведінковий аналіз
Підтвердження	Лабораторна діагностика	Частково (правила)	Sandbox, ML-агенти, глибокий аналіз
Імунна оцінка	Оцінка стану організму	Відсутня	Аналіз навантаження, вразливостей
Моніторинг ефективності	Динамічна оцінка лікування	Відсутній	Автоматичний фідбек-цикл
Профілактика	Вакцинація, освіта	Ручне оновлення правил	Автоматичне самооновлення, навчання
Самонавчання	Формування імунної пам’яті	Обмежено (ML-модулі)	Постійне оновлення на основі досвіду
Адаптивність	Висока	Обмежена	Гнучка зміна політик, самонавчання
Динамічна корекція	Автоматична	Переважно ручна	Автоматичне коригування політик
Контекстна обізнаність	Врахування анамнезу, стану	Частково (інтеграція з SIEM)	Повний контекст, профілювання, історія

Ключові механізми покращення адаптивності SURICATA [1,4,10].

1.Контекстна обізнаність та “анамнез”: збір та аналіз історичних даних про мережеву активність, профілювання користувачів і пристроїв. Врахування попередніх інцидентів для формування “імунологічної пам’яті” системи.

2. Багаторівнева діагностика: поєднання швидкого сигнатурного скринінгу з глибинним поведінковим та ML-аналізом підозрілих подій. Автоматичне визначення ступеня загрози та вибір оптимальної стратегії реагування.

3. Адаптивне оновлення правил: використання механізмів зворотного зв’язку: автоматичне коригування політик та правил на основі аналізу результатів реагування. Самостійне формування нових “антитіл” (правил) для невідомих атак за аналогією з клональним відбором у біології.

4. Динамічний моніторинг та оцінка стану: постійний контроль за змінами у мережевому середовищі, виявлення аномалій у реальному часі. Оцінка “здоров’я” інфраструктури та автоматичне пристосування до нових умов.

5. Формування імунної пам’яті: збереження інформації про попередні атаки та ефективні способи реагування. Використання цього досвіду для швидшого й точнішого виявлення повторних або схожих загроз.

Переваги для SURICATA – зменшення кількості хибних спрацювань завдяки врахуванню контексту та історії подій; підвищення стійкості до нових типів атак через самонавчання та автоматичне оновлення правил; гнучкість реагування: зміна стратегії захисту залежно від типу, сили та контексту загрози; підвищення ефективності профілактики – автоматичне впровадження нових політик і навчання користувачів після інцидентів.

Інтеграція імунної моделі в архітектуру SURICATA дозволяє створити дійсно адаптивну систему кіберзахисту, що не лише ефективно реагує на відомі загрози, а й здатна навчатися на нових інцидентах, автоматично вдосконалювати свої механізми захисту та забезпечувати стійкість до складних і цільових атак.

Імітаційна модель кіберімунної відповіді. Попередній аналіз аналогій та порівняння принципів медичної імунної системи з архітектурою SURICATA дозволили окреслити ключові напрями вдосконалення сучасних засобів кіберзахисту. Наступним логічним

кроком є спроба об'єднати ці принципи у єдину концептуальну модель, яка імітує поведінку біологічної імунної системи. Такий підхід не лише демонструє потенціал міждисциплінарного перенесення знань, але й пропонує дорожню карту для подальших досліджень та розробки практичних рішень.

Обґрунтуємо доцільність залучення моделі як дослідницького інструменту [15]. Така модель виконує одразу кілька важливих завдань у контексті розвитку систем кіберзахисту.

По-перше, вона дозволяє синтезувати результати порівняльного аналізу між медичними протоколами та сучасними IPS/IDS (як-от SURICATA), переносячи виявлені принципи (багаторівнева діагностика, формування пам’яті, профілактика) у єдину цілісну архітектуру. Це створює підґрунтя для системного переосмислення підходів до побудови систем захисту. По-друге, імітаційна модель слугує мисленнєвим експериментом – способом формалізувати ідеї ще до етапу інженерного прототипування. Вона дозволяє визначити ключові компоненти, їхню взаємодію та потенційні «точки росту» для подальших R&D-досліджень. По-третє, запропонована модель виконує освітню функцію. Вона допомагає фахівцям із кібербезпеки уявити, як принципи з іншої дисципліни (медицини) можуть бути інтегровані у їхню практику. Такий міждисциплінарний підхід стимулює пошук нових рішень для підвищення стійкості цифрової інфраструктури.

Обґрунтуємо абстрактну архітектуру та її цінність як практичного інструменту для планування інновацій у сфері кіберзахисту. Запропонована імітаційна модель кіберімунної відповіді будується за аналогією з біологічною імунною системою людини, яка характеризується багаторівневою структурою, взаємодією спеціалізованих клітин і механізмами самонавчання [4]. Кожен компонент цієї моделі виконує специфічну роль, що разом створює цілісний, адаптивний механізм захисту (рис.5).

Рис.5. Візуалізація імітаційної моделі кіберімунної відповіді

Клітини-розвідники (сенсори, IDS-агенти): відповідають за постійний моніторинг мережевого трафіку та активності системи. Вони виконують функцію первинного виявлення аномалій або потенційних «антигенів» — підозрілих патернів чи дій.

Макрофаги (IPS, фільтруючі вузли): здійснюють швидке реагування — ізоляцію або блокування виявлених загроз на ранньому етапі. Їхня роль полягає у запобіганні поширенню атаки в межах інфраструктури.

Т-клітини (аналітичні ML-агенти, SIEM): координують реагування системи, проводять поглиблений аналіз інцидентів, класифікують загрози та ухвалюють рішення про подальші дії. Це рівень стратегічного керування безпекою.

Клітини пам’яті (бази інцидентів, системи Threat Intelligence): зберігають інформацію про попередні атаки, типові сценарії реагування та ознаки компрометації; дозволяє системі швидко впізнавати схожі загрози у майбутньому та підвищувати ефективність захисту.

Кістковий мозок (центри оновлення, R&D): відповідає за створення нових «антитіл» –

оновлених правил, сигнатур, політик безпеки. Це аналог постійної еволюції системи через дослідження нових загроз і генерацію оновлень.

Візуалізація узагальнює ідею побудови адаптивної, самонавчальної архітектури кіберзахисту за медичною аналогією. Багаторівнева архітектура дозволяє моделювати поведінку кіберзахисної системи як єдиного адаптивного організму, здатного не лише відбивати відомі атаки, але й самостійно вчитися та вдосконалювати свої механізми протидії у відповідь на нові загрози [10].

Принципи біологічної імунної відповіді: клітини-розвідники — IDS/сенсори для виявлення аномалій; макрофаги – IPS для ізоляції та блокування; Т-клітини – ML-агенти, SIEM для аналітики й координації; клітини пам'яті – бази інцидентів, Threat Intelligence; кістковий мозок – центри оновлення правил, R&D.

Приклад сценарію роботи системи. Для кращого розуміння пропонованої архітектури варто розглянути спрощений сценарій її функціонування у реальному середовищі. Виявлення аномалії. Сенсори та IDS-модулі постійно моніторять трафік і події на хостах. При виявленні підозрілої активності формується початкове повідомлення про загрозу. Попередня оцінка (швидкий скринінг). IPS-модулі (макрофаги) здійснюють негайну перевірку сигнатур і поведінкових правил. Якщо загроза підтверджується – з'єднання блокується або ізолюється.

Поглиблений аналіз. Підозрілі випадки передаються на розгляд аналітичним модулям (Т-клітинам) – ML-агентам або SIEM-системі, які здійснюють кореляцію подій, класифікацію типу атаки та приймають рішення про подальші дії.

Реакція та ізоляція**.** На основі результатів аналізу формуються правила реагування – карантин хосту, зміна політик брандмауера, блокування певних портів чи процесів.

Запис у пам'ять системи**.** Інформація про інцидент, ознаки компрометації та ефективні дії реагування зберігаються у базі знань (клітини пам'яті), що дозволяє швидше реагувати на подібні загрози у майбутньому.

Оновлення та еволюція. Центри оновлення (кістковий мозок) аналізують накопичені дані про нові типи атак, розробляють нові сигнатури, оновлення правил і політик безпеки для розповсюдження на всі вузли системи.

Такий сценарій демонструє можливість створення самонавчальної системи кіберзахисту, яка поєднує швидке реагування, поглиблений аналіз, накопичення знань і постійне вдосконалення [16].

Порівняння з класичною SIEM-архітектурою. Порівняння має важливе значення для оцінки практичності запропонованої кіберімунної моделі. SIEM є стандартним елементом сучасних систем кіберзахисту, забезпечуючи централізований збір, зберігання, кореляцію та аналіз подій безпеки з різних джерел.

Наведемо переваги SIEM-систем. Централізація даних: консолідація журналів подій і логів з різних систем для єдиного моніторингу. Кореляція інцидентів: можливість виявлення комплексних атак через аналіз патернів і зв'язків між подіями. Аудит і відповідність: підтримка відповідності стандартам (PCI DSS, ISO 27001) через документування і зберігання даних. Підтримка розслідувань: надання даних для форензики і аналізу інцидентів.

Обмеження і виклики традиційних SIEM. Реактивний характер: фокус на виявленні після факту, з потенційною затримкою між компрометацією і сповіщенням. Обмежений контекст: аналіз переважно базується на логах без повноцінної оцінки поточного стану системи чи користувача. Високий рівень FP/FN: значна кількість хибнопозитивних і хибнонегативних спрацювань через жорстко задані правила. Трудомістке обслуговування: потреба ручного оновлення правил, сценаріїв кореляції і постійного налаштування.

Обмежене самонавчання: відсутність або обмежене використання механізмів машинного навчання та автоматичного оновлення знань.

Медична імунна система функціонує як інтегрована багаторівнева структура з можливістю раннього виявлення, локалізації, координації реагування та формування імунної пам’яті. Аналогічно кіберімунна модель прагне подолати обмеження SIEM через:

1) децентралізовану архітектуру агентів, які забезпечують гнучке розгортання моніторингу; 2) механізми швидкого реагування на рівні IPS/IDS (аналог макрофагів); 3) координацію через аналітичні модулі (аналог Т-клітин); 4) збереження знань про атаки (клітини пам’яті); 5) автоматичне оновлення та генерацію нових правил (кістковий мозок) [1].

Результати порівняльного аналізу

За такими параметрами можна умовно оцінити відмінності між традиційною SIEM-архітектурою та запропонованою кіберімунною моделлю.

1.Швидкість виявлення і реагування: SIEM часто має затримки через централізований аналіз журналів після факту. Імунна модель передбачає локальне виявлення агентами в реальному часі.

2.Контекстна обізнаність: SIEM обмежена історичними логами без поточного стану системи. Імунна модель інтегрує динамічну оцінку стану хостів і поведінковий аналіз.

3.Самонавчання і оновлення: класична SIEM потребує ручного оновлення правил, що збільшує ризик FP/FN. Імунна модель передбачає автоматичне збереження досвіду інцидентів і генерацію нових правил.

4.Масштабованість: SIEM-централізація ускладнює горизонтальне масштабування без збільшення витрат. Імунна модель ґрунтується на розподілених агентах, що легше масштабуються.

5.Ефективність профілактики: SIEM майже не має профілактичного рівня. Імунна модель включає автоматичне оновлення політик і навчання користувачів.

Умовна інтегральна оцінка: імунна модель пропонує підвищення ефективності захисту за рахунок скорочення часу реагування, зменшення FP/FN, кращої адаптивності до нових типів атак і можливості накопичення колективного знання про загрози. У таблиці 6 показано порівняння класичної SIEM та кіберімунної моделі.

Таблиця 6.

Порівняння класичної SIEM та кіберімунної моделі

Параметр	Класична SIEM	Кіберімунна модель
Швидкість виявлення і реагування	Централізований аналіз логів → затримка між атакою і сповіщенням	Локальне виявлення агентами → реагування в реальному часі
Контекстна обізнаність	Історичні логи без оцінки стану системи	Динамічний моніторинг стану, поведінковий аналіз
Самонавчання і оновлення	Ручне налаштування правил	Автоматичне збереження досвіду і генерація нових правил
Масштабованість	Централізована архітектура обмежує горизонтальне масштабування	Розподілена система агентів → легка масштабованість
Ефективність профілактики	Відсутня або мінімальна	Автоматичне оновлення політик, навчання користувачів

Ця таблиця підкреслює системні відмінності між класичними SIEM-рішеннями та запропонованою кіберімунною моделлю. Хоч SIEM є критично важливою для централізованого аудиту, форензики і відповідності стандартам, вона є переважно реактивним інструментом з обмеженою контекстною обізнаністю та автоматизацією.

Кіберімунна модель пропонує інший підхід: децентралізоване, багаторівневе і самонавчальне середовище захисту, що поєднує швидке локальне реагування з накопиченням колективного знання про атаки. Це дозволяє знизити час реагування, підвищити точність виявлення та адаптуватися до нових типів загроз [17].

Висновки. У статті виконано комплексний міждисциплінарний аналіз можливостей перенесення принципів біологічної імунної системи та медичних протоколів у сферу кіберзахисту. Проведено порівняння етапів розвитку біологічних інфекцій і сучасних кібератак, що дало змогу виявити структурні паралелі та визначити універсальні стратегії реагування. Підтверджено доцільність використання медичних аналогій для побудови багаторівневих, адаптивних і самонавчальних систем кіберзахисту.

Проведено аналіз архітектури SURICATA та визначено обмеження класичних IDS/IPS у контексті адаптивності, формування пам'яті та профілактики. Запропоновано концепцію імітаційної моделі кіберімунної системи, яка об'єднує переваги біологічної імунної відповіді та сучасних технологій машинного навчання для побудови стійких і гнучких захисних архітектур. Розроблено сценарії застосування імітаційного моделювання як інструменту валідації та розвитку нових підходів до кіберзахисту, що дозволяє не лише перевірити життєздатність концепцій, а й виявити їхні переваги й обмеження до етапу практичного впровадження. Проведено порівняння з класичними SIEM-системами та показано, що імунна модель забезпечує вищу швидкість реагування, кращу адаптивність і можливість накопичення колективного знання про загрози.

Результати дослідження можуть бути використані для удосконалення сучасних IDS/IPS-систем шляхом впровадження багаторівневої діагностики, механізмів самонавчання та формування кіберпам'яті; розробки нових прототипів захисних систем, що поєднують переваги біологічних і цифрових підходів; підвищення стійкості IT-інфраструктур до складних, цільових і нових типів атак; оптимізації процедур реагування, профілактики завдяки використанню імітаційного моделювання як інструменту валідації.

Стаття закладає підґрунтя для подальших досліджень у сфері інтеграції медичних принципів у кібербезпеку, пропонуючи нову концептуальну модель, що поєднує міждисциплінарний підхід, імітаційне моделювання та сучасні інструменти кіберзахисту. Отже, проведене дослідження підтверджує ефективність і перспективність використання імунних принципів і імітаційного моделювання для розвитку адаптивних, самонавчальних і стійких систем кіберзахисту нового покоління.

Список літератури

1. Tallam K. The Cyber Immune System: Harnessing Adversarial Forces for Security Resilience. arXiv preprint arXiv:2502.17698. 2024. 15 p. URL: https://arxiv.org/abs/2502.17698.
2. Widuliński P. Artificial Immune Systems in Local and Network Cybersecurity. *ACIG Journal.* 2023. Vol. 12. No. 3. C. 34–45. URL: https://www.acigjournal.com /pdf-184306-105064.
3. Marshall J.S. The cyber-physical immune system: work-in-progress. 2022. No. 4. P. 56–67. URL: https://journals.indexcopernicus.com /publication/4485947.
4. Forrest S., Hofmeyr S. Immunology as inspiration for computer security. *Nature*. 1999. Vol. 397. P. 34–36.
5. World Economic Forum. What the human body teaches us about cyber security. 2015. URL: https://www.weforum.org/stories/2015/08/good-immune-system-wards-off-cyber-threats/
6. Nasreen F. Digital immune system. LinkedIn, 2024. URL: https://www.linkedin.com/pulse/digital-immune-system-fathima-nasreen-awevc
7. Yang H. A Survey of Artificial Immune System Based Intrusion Detection. *Journal of Biomedical Science and Engineering.* 2014. Vol. 7. No. 3. P. 147–156. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC3981469/
8. Rotimi E. Cyber Immune: A New Paradigm in Cybersecurity. LinkedIn, 2024. URL: https://www.linkedin.com/posts/enitan-rotimi-a763baa-cyber-immune-a-new-paradigm-in-cybersecurity-activity-7245067066808963073-loNu
9. Suricata Project. Suricata IDS/IPS Documentation. 2025. URL: https://suricata.io/docs/

10. Stamus Networks. Suricata Architecture Overview. 2024. URL: https://www.stamus-networks.com/suricata-architecture
11. Yu Q. An Immunology-Inspired Network Security Architecture . *Computers & Security*. 2022. Vol. 115. P. 102–115.
12. Hackzone.in. Suricata IDS: Protocol Analysis and Anomaly Detection. 2024. URL: https://hackzone.in/suricata-ids-protocol-analysis
13. Tecracer. SIEM Integration with Suricata. 2024. URL: https://www.tecracer.com/blog/siem-integration-suricata
14. Kantharaju V. Artificial Immune System Inspired Intrusion Detection in IDS/IPS. *IEEE Access*. 2023. Vol. 11. P. 1234–1246.
15. Беляєва О.В., Грицик В.А. Імітаційне моделювання систем захисту інформації: методи та засоби . *Інформаційна безпека*. 2023. Т. 29, № 1. С. 55–68.
16. Сиропятов О.А., Тимошенко Л.М. Кіберімунна модель захисту даних: міждисциплінарний аналіз, діагностика та архітектура. *Informatics and Mathematical Methods in Simulation*. 2025. Vol.15. No. 2. P. 260-275.
17. Gartner Precedence Research. Digital Immune System Market Trends and Forecast. 2024. URL: https://www.gartner.com/en/ insights/digital-immune-system

SIMULATION MODEL OF A CYBER-IMMUNE SYSTEM: TRANSFERRING MEDICAL PRINCIPLES TO MODERN CYBER DEFENCE

O.A. Syropiatov, L.M.Tymoshenko

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

The article proposes an interdisciplinary approach to enhancing the resilience of information systems by transferring the principles of the biological immune system and medical protocols to the field of cybersecurity. A comparative analysis was conducted of the phases of development of biological infections (e.g. those of the virus causing the disease known as "coronavirus", or "covid-19", and the liver fluke Hepatitis A) and modern cyberattacks (e.g. the "PlugX" and "Worm" viruses and the "ILOVEYOU" worm). This analysis enabled the identification of structural parallels and the definition of universal response strategies. This study focuses on the potential integration of medical principles into the architecture of contemporary IDS/IPS, using the SURICATA system as a case study. The fundamental limitations of analogies related to differences in transmission mechanisms, environment architecture, and threat behaviour are described. The author proposes a conceptual simulation model of a cyber defence system based on a multi-level structure, self-learning, automatic policy correction and cyber memory. The model incorporates components that are responsible for monitoring, rapid response, analytics, knowledge accumulation and the evolution of defence mechanisms. A comparison with classical SIEM systems is carried out and it is demonstrated that the immune model provides a higher response speed, better adaptability and the ability to accumulate collective knowledge about threats. The practical significance of the study lies in the possibility of using simulation modelling to validate new approaches to cyber defence, optimise response and prevention procedures.The article establishes the foundation for subsequent research endeavours concerning the integration of medical principles into the domain of cybersecurity. It proposes the concept of decentralised, self-learning, and resilient new generation defence systems.

Keywords: cyberimmune system, medical protocols, multilevel diagnostics, SURICATA, simulation model of cyberimmune response, cybermemory, adaptive protection.

DOI 10.15276/imms.v15.no3.454
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 454-463

АЛГОРИТМ ВБУДОВУВАННЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В АУДІО- ТА ВІДЕОКОМПОНЕНТИ МУЛЬТИМЕДІЙНОГО ФАЙЛУ

К.С. Чабаненко, Н.І. Кушніренко, В.В. Подуфалов

Національний університет «Одеська політехніка»
1, Шевченко пр., Одеса, 65044, Україна
Emails: chabanenkoksenia3@gmail.com, kushnirenko@op.edu.ua

У статті розглянуто застосування цифрових водяних знаків (ЦВЗ) як ефективного засобу захисту мультимедійних файлів. Описано основні методи вбудовування ЦВЗ, зокрема просторовий метод заміни найменш значущого біта та частотні підходи, зокрема дискретне Фур'є перетворення (ДФП), дискретне вейвлет-перетворення (ДВП) та дискретне косинусне перетворення (ДКП). Запропоновано алгоритм вбудовування ЦВЗ у відеофайл, який використовує як відеокадри, так і аудіодоріжку вхідного файлу в якості контейнера для прихованої інформації. Алгоритм ґрунтується на застосуванні методу Коха-Жао для модифікації частотних коефіцієнтів, отриманих у результаті застосування ДКП, а також криптографічної хеш-функції HMAC-SHA256 для генерації цифрового водяного знака на основі повідомлення-ключа користувача. Описано послідовність реалізації методу: розділення відеофайлу на кадри та аудіоблоки, генерація вибірки блоків на основі довжини повідомлення-ключа та загальної кількості блоків, частотне перетворення вибраних сегментів, формування та вбудовування ЦВЗ. Вбудовування здійснюється лише у фрагменти з порядковими номерами, кратними параметру, що обчислюється на основі довжини ключа та загальної кількості блоків. Розроблений алгоритм реалізовано у вигляді веб-застосунку, що дозволяє виконувати як вбудовування, так і перевірку цифрового водяного знака. Якість зображення та звуку після вбудовування оцінено за допомогою метрик PSNR, SSIM та SNR. Результати експериментів підтвердили збереження високого рівня візуального та аудіального сприйняття. Запропонований алгоритм має перспективи практичного застосування в системах захисту авторських прав, моніторингу цілісності контенту та цифрової ідентифікації мультимедійних даних. Водночас, з огляду на поточний етап апробації, доцільним є проведення додаткових експериментальних досліджень для оцінки його стійкості, масштабованості та ефективності у різних прикладних умовах.

Ключові слова: стеганографія, цифровий водяний знак, дискретне косинусне перетворення, HMAC, мультимедійні дані, захист інформації.

Вступ. Із розвитком інтернет-технологій процес цифровізації охоплює дедалі більше сфер людської діяльності – від особистої комунікації до промисловості, торгівлі та систем безпеки. Перенесення інформації в цифрове середовище забезпечує її зручну доступність, однак водночас підвищує ризики, пов'язані з несанкціонованим доступом, копіюванням, підробкою або знищенням даних. У контексті відкритого доступу до мережі Інтернет мультимедійний контент, який відіграє провідну роль у цифровому середовищі, є особливо вразливим. З метою захисту авторських прав, підтвердження автентичності, протидії фальсифікаціям і маніпуляціям, а також для забезпечення доказової бази в юридичних спорах, широко застосовується технологія вбудовування цифрових водяних знаків (ЦВЗ) [1].

Стаття присвячена дослідженню застосування цифрових водяних знаків як засобу захисту мультимедійних файлів. У ній запропоновано алгоритм вбудовування ЦВЗ, що використовує в якості стеганоконтейнера як відеоряд, так і аудіосупровід відеофайлу. У роботі [2] розглянуто модифікований метод заміни найменш значущого біта, що застосовується для вбудовування у вибрані кадри відео, визначені на основі максимальної абсолютної різниці гістограм між сусідніми кадрами. Аналогічний підхід можна застосовувати для вбудовування у частотному домені, як це представлено в

роботі [3]. Окрім методів вбудовування у піксельну інформацію відео у просторовому та частотному доменах, також досліджуються методи вбудовування цифрового водяного знака у вектори руху кадрів відеопотоку, як запропоновано в роботі [4]. На відміну від підходів, описаних у роботах [5,6], розроблений у межах цього дослідження алгоритм реалізовує вбудовування ЦВЗ у частотну область як відеокадрів, так і аудіоблоків відеофайлу, отриману за допомогою дискретного косинусного перетворення.

Мета роботи. Метою роботи є підвищення ефективності захисту авторських прав на мультимедійний контент шляхом розробки алгоритму комбінованого вбудовування цифрового водяного знаку у відеоряд та аудіодоріжку відеофайлу.

Для досягнення поставленої мети необхідно:

− провести дослідження існуючих методів вбудовування цифрових водяних знаків у мультимедійні файли, визначити їх переваги, недоліки та особливості застосування;

− розробити алгоритм комбінованого вбудовування цифрового водяного знака у відеофайл (відеокадри та аудіодоріжку);

− реалізувати запропонований алгоритм програмно та провести його експериментальне тестування.

Основна частина. Методи для вбудовування цифрових водяних знаків за способом обробки даних розділяються на просторові та частотні. Одним із найпоширеніших просторових методів є метод заміни найменш значущого біта (НЗБ), який застосовується для різних типів контейнерів – зображень, аудіо- та відеофайлів. Його суть полягає у безпосередній заміні найменш значущих бітів оригінальних даних на біти цифрового водяного знака (див. рисунок 1).

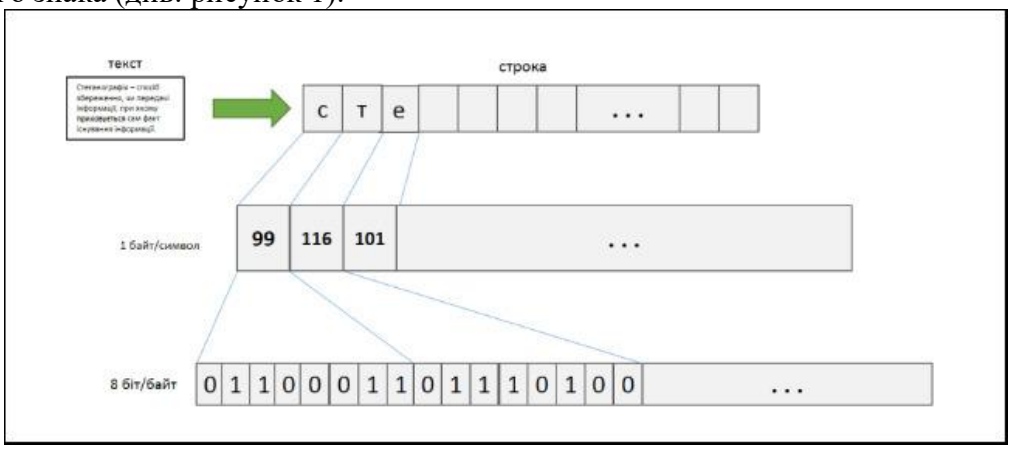


Рис. 1. Схема вбудовування за методом НЗБ

Метод відзначається простотою реалізації та може бути ефективно використаний в умовах обмежених обчислювальних ресурсів. До основних недоліків методу заміни найменш значущого біта відносять низьку стійкість до зовнішніх впливів, зокрема до зашумлення, стиснення, обрізання та масштабування, що робить його менш надійним у порівнянні з частотними методами, які забезпечують вищий рівень збереження водяного знака після атак або обробки мультимедійного контенту [1].

До основних частотних методів обробки вхідних даних належать дискретне перетворення Фур'є, дискретне вейвлет-перетворення, дискретне косинусне перетворення та їхні модифікації, зокрема у вигляді гібридних підходів, що поєднують кілька типів перетворень з метою підвищення ефективності вбудовування.

Частотні методи дозволяють ефективно розподіляти водяний знак у менш помітних для людського сприйняття частинах сигналу, що мінімізує ймовірність його виявлення або видалення, збільшують стійкість до атак, таких як стиснення, шумові перешкоди, масштабування, обрізання тощо.

Загальна схема вбудовування у частотну область представлена на рисунку 2.

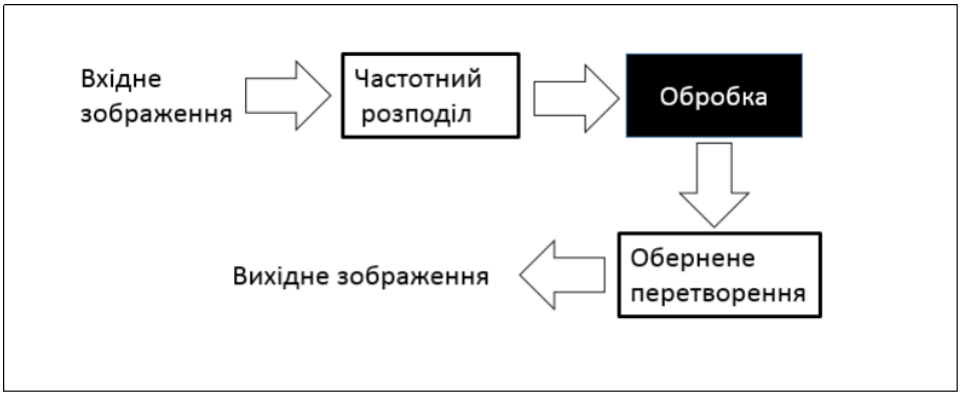


Рис.2. Схема вбудовування ЦВЗ в частотну область

Дискретне перетворення Фур'є здійснює перетворення сигналу або зображення у частотну область, представляючи його як суму синусоїд і косинусоїд різної частоти [7]. Завдяки цьому можливо вбудовувати водяний знак у спектральні компоненти, які є менш чутливими до атак. Водночас, через глобальність перетворення кожен елемент водяного знака впливає на всю структуру зображення, що знижує локалізацію та обмежує гнучкість. Крім того, ДПФ є обчислювально складним методом.

Дискретне вейвлет-перетворення, на відміну від ДПФ, забезпечує мультироздільний аналіз зображення завдяки поетапній декомпозиції сигналу на піддіапазони різної частоти та орієнтації: LL (низькочастотний компонент), LH, HL та HH (високочастотні компоненти) [8]. Завдяки локальній обробці даних та відповідності до особливостей людського зору, ДВП дозволяє ефективно вбудовувати водяні знаки в низькочастотну область, забезпечуючи стійкість до типових атак.

Серед частотних методів слід відзначити дискретне косинусне перетворення, яке характеризується порівняно низькою обчислювальною складністю. ДКП є універсальним методом обробки сигналів, який застосовується як для зображень, так і для аудіо, забезпечуючи оптимальне співвідношення між продуктивністю та якістю результату. Завдяки зазначеним перевагам цей метод було обрано для реалізації в рамках розробленого алгоритму.

Для кадрів відео використовується формула двовимірного перетворення:

$$C(u,v) = \frac{1}{4} \cdot \alpha(u) \cdot \alpha(v) \cdot \sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cdot \cos\left[\frac{(2x+1)u\pi}{16}\right] \cdot \cos\left[\frac{(2y+1)v\pi}{16}\right], \qquad (1)$$

де $f(x,y)$ – значення пікселя в координатах x,y в блоці, $C(u,v)$ – ДКП-коефіцієнти у частотному просторі на позиції (u,v), x, y – просторові координати вхідного блоку (пікселі), u, v – частотні координати – індекси вихідного ДКП, $a(u)$, $a(v)$ – нормалізаційні коефіцієнти. Для аудіосигналу застосовують формулу одновимірного ДКП:

$$C(u) = a(u) \sum_{x=0}^{N-1} f(x) \cdot \cos\left[\frac{(2x+1)u\pi}{2N}\right], \qquad (2)$$

де $f(x)$ – значення амплітуди аудіосигналу в точці x, $C(u)$ – ДКП-коефіцієнти, N-довжина блоку, $a(u)$ – нормалізаційний коефіцієнт [9].

Результатом перетворення сигналу є набір частотних коефіцієнтів, які можна поділити на три основні піддіапазони:

– низькочастотні – великі контури, основні переходи між різними областями зображення, такі як зміни фону чи основні геометричні форми;

– середньочастотні – текстури та краї об'єктів, а також деталі середнього рівня;

– високочастотні – мікроструктури та різкі переходи між областями зображення, містять інформацію про дрібні деталі.

Для покращення точності перетворення зображення розбивають на блоки розміром 8×8 пікселів. Блок зображення після застосування ДКП наведено на рисунку 3.

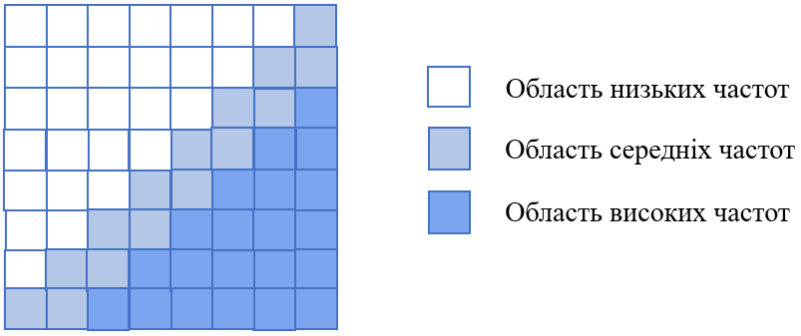


Рис.3. Блок зображення після застосування ДКП

Запропонований в роботі алгоритм вбудовування ЦВЗ в відеофайл складається з таких етапів:

1) розподіл відео на аудіодоріжку та кадрові складові;
2) ініціалізація псевдовипадкового числа за текстовим ключем;
3) вибір кадрів/семплів та блоків на основі псевдовипадкової вибірки;
4) перетворення обраних фрагментів у частотну область методом ДКП;
5) вбудовування ЦВЗ за модифікованим методом Коха-Жао.

На початковому етапі вихідний відеофайл піддається розділенню на дві основні компоненти: відеокадри та аудіодоріжку. У результаті формуються два окремих набори даних: перший складається з послідовності кадрів (зображень), а другий – з аудіосигналу, який розділяється на блоки по 1024 семпли кожен. Для вбудовування використовуються лише вибрані фрагменти мультимедійного контенту – кадри та аудіоблоки, порядкові номери яких кратні числовому ключу, що розраховується за формулою:

$$R = \min + \left(N \bmod(\max - \min) + 1 \right), \tag{3}$$

де R – псевдовипадкове число в межах діапазону [min,max], N – кількість символів повідомлення-ключа; *min, max* – мінімальне та максимальне значення діапазону, в якому генерується число. Мінімальне значення дорівнює 1, а максимальне обчислюється за формулою:

$$\max = \frac{M_{audio} + M_{frames}}{256}, \tag{4}$$

де M_{audio} – кількість блоків аудіо, M_{frames} – кількість кадрів у відео.

Повідомлення-ключ – це текстове повідомлення (символьна послідовність), що задається користувачем (автором або розпорядником контенту). Воно використовується як складова частина самого цифрового водяного знака, тоді як числове значення, отримане шляхом підрахунку кількості його символів, застосовується для формування псевдовипадкового ключа. Цей ключ, у свою чергу, визначає закономірність вибірки блоків для вбудовування цифрового водяного знака (див. рисунок 4).

Застосування лише обраних за ключем кадрів та аудіоблоків забезпечує рівномірний розподіл цифрового водяного знака та мінімізує вплив на якість мультимедійного контенту.

Оскільки аудіосигнал та відеокадри обробляються окремо, використання одного й того самого ключа R для обох типів медіа не створює жодних проблем. Вибірки аудіо- та відеоданих є незалежними одна від одної: N-й елемент аудіосиналу та N-й елемент вибірки кадрів не мають прямого зв'язку або взаємозалежності.

Таким чином, застосування однакового ключа для обох типів даних дозволяє уникнути перетину, знижує загальну складність алгоритму, одночасно забезпечуючи достатню стійкість ЦВЗ.

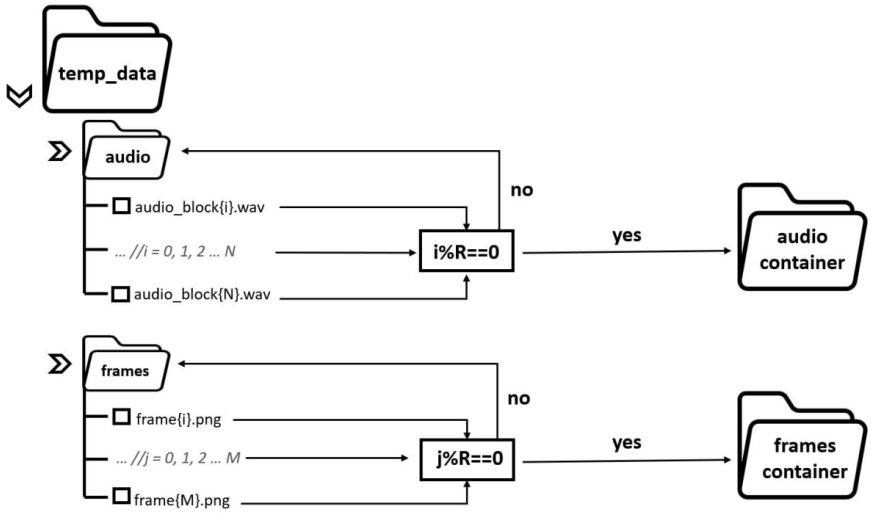


Рис. 4. Схема створення вибірки файлів для вбудовування

Такий підхід є універсальним і може бути застосований для вбудовування цифрових водяних знаків різного змісту – від ідентифікаційних кодів до контрольних сум, що використовуються для перевірки автентичності або цілісності медіаконтенту.

У межах запропонованого алгоритму в якості цифрового водяного знака використовується хеш відеофайлу, згенерований за допомогою алгоритму HMAC із застосуванням криптографічної хеш-функції SHA-256.

Алгоритм HMAC реалізується шляхом послідовного виконання операцій, що забезпечують генерацію хешу на основі двох вхідних параметрів: ключа та повідомлення. У межах розробленого підходу в якості ключа використовується текстове повідомлення-ключ, задане автором або розпорядником контенту, а в якості вхідного повідомлення – сам відеофайл.

Перед вбудовуванням вхідні дані, а саме вибрані кадри та аудіоблоки, піддаються додатковій обробці. Для кадрів ця обробка включає отримання значень яскравості зображення шляхом перетворення його з моделі RGB у простір YCbCr, де використовується лише компонента яскравості (Y), яка найбільш чутлива для людського ока. Такий підхід дозволяє досягти високої якості зображення навіть після модифікацій.

Для аудіоданих передбачене розділення сигналу на два канали (стереофонічного сигналу), з яких лише один модифікується відповідно до алгоритму вбудовування. Другий канал залишається незмінним, що дозволяє після обробки об’єднати їх назад у стереосигнал і зберегти високу якість звучання. Такий підхід мінімізує можливі спотворення та забезпечує акустичну цілісність кінцевого файлу.

Вбудовування виконується за методом Коха-Жао шляхом модифікації співвідношення абсолютних значень обраних коефіцієнтів згідно з бітовим значенням [10]. Для вбудовування одного біта цифрового водяного знаку з кожного блоку обирається пара середньочастотних коефіцієнтів. Це зумовлено тим, що низькочастотні коефіцієнти містять найважливішу інформацію про загальну структуру, а високочастотні – менш стійкі до атак. За замовченням один вхідний блок може містити один біт значення ЦВЗ. Якщо необхідно вбудувати біт 0, забезпечується умова:

$$|C_1| - |C_2| > T, \tag{5}$$

Якщо ж вбудовується біт 1, виконується умова:

$$|C_1| - |C_2| < -T, \tag{6}$$

де T – заздалегідь заданий поріг, C_1 та C_2 – коефіцієнти.

Після модифікації для кадрів та аудіоблоків застосовується зворотне дискретне косинусне перетворення (ЗДКП) за формулою:

$$x_{m,n} = a_m a_n \sum_{k=0}^{M-1} \sum_{l=0}^{N-1} X_{k,l} \cos\left[\frac{\pi}{M}(m+\frac{1}{2})k\right] \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)l\right], \quad (7)$$

де $x_{m,n}$ – піксель або значення сигналу в просторі після зворотного перетворення, $X_{k,l}$– коефіцієнти ДКП для кожного блоку сигналу, a_m, a_n – коефіцієнти масштабування для кожного індексу, M,N – розміри блоку, m,n – просторові індекси для відновлення сигналу. Для блоків аудіо аналогічно виконується одновимірне ЗДКП. Метою цього перетворення є відновлення просторового або часово-просторового представлення мультимедійних даних. ЗДКП дозволяє перетворити частотні коефіцієнти назад у значення пікселів (для зображень або відео) або амплітуди семплів (для аудіо), відтворюючи таким чином оригінальний сигнал з урахуванням змін, внесених у процесі вбудовування цифрового водяного знака.

Ключовим аспектом цих змін є вибір порогу вбудовування T, що визначає ступінь модифікації коефіцієнтів. Значення порогу вбудовування є критичним параметром, оскільки воно безпосередньо впливає на стійкість і непомітність цифрового водяного знака. Надто мале значення призводить до нестабільного вбудовування, тоді як надмірно велике – до візуально помітних спотворень контенту. Оптимальне значення порогу визначається експериментально залежно від типу контейнера, характеру очікуваних атак та вимог до якості вихідного мультимедійного файлу.

Оскільки запропонований алгоритм передбачає незалежну обробку відеокадрів та аудіоблоків, для визначення оптимального порогу вбудовування було проведено два окремих експериментальних дослідження: перше – для оцінки впливу порогу на якість відеозображення, друге – для аналізу його впливу на якість аудіосигналу.

Для оцінки якості аудіо була використана метрика SNR (Signal-to-Noise Ratio) – відношення сигналу до шуму, що визначається за формулою:

$$SNR = 10\log_{10}\left(\frac{\sum_{a=1}^{M} Z^2(a)}{\sum_{a=1}^{M}\left(Z(a)-Z'(a)\right)}\right), \quad (8)$$

де $Z(a)$ – вихідний звуковий сигнал, $Z'(a)$ – аудіосигнал із водяним знаком, M — кількість семплів в обох аудіосигналах .

Для вбудовування використовувалася пара коефіцієнтів із порядковими номерами 225 та 250, визначена експериментально. Для встановлення оптимальних параметрів проводилося вбудовування цифрового водяного знака із застосуванням пар коефіцієнтів у діапазоні від 150 до 350 з кроком 25. Пара 225 та 250 демонструвала стабільно високі значення показника SNR для всіх тестових файлів, як це показано на рисунку 5.

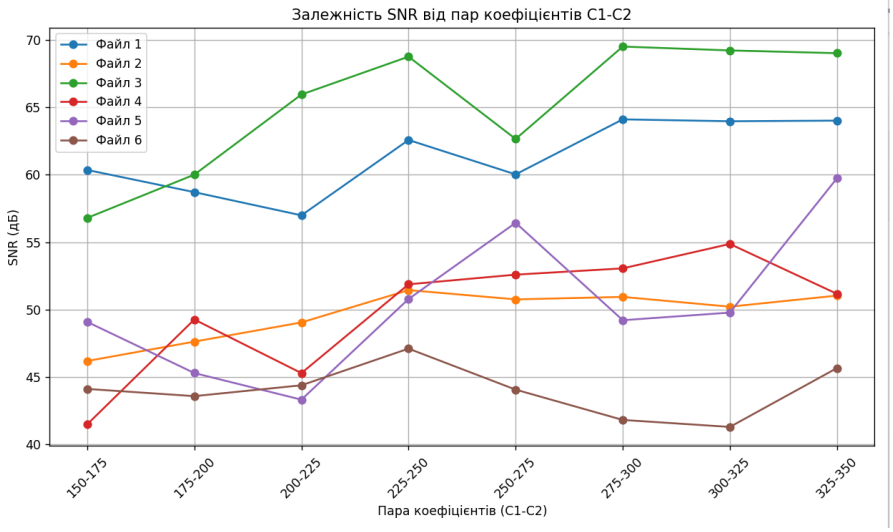


Рис. 5. Графік впливу частотних коефіцієнтів на якість ЦВЗ

Ці коефіцієнти належать до середньочастотного діапазону спектра ДКП та забезпечують оптимальний компроміс між непомітністю змін для сприйняття людиною та стійкістю вбудованого знака до атак. Водночас варто зазначити, що хоча дана пара є ефективною для більшості типових аудіо- та відеофайлів, вибір оптимальної пари коефіцієнтів може потребувати адаптації для конкретного мультимедійного сигналу з урахуванням його частотно-енергетичної структури.

Результати дослідження впливу порогу вбудовування T на якість аудіо показані в таблиці 1. Дані наведені для шести аудіофайлів (A1-A6). У більшості випадків варіації SNR не перевищують кількох децибел, що свідчить про мінімальний вплив параметра T на якість відновленого сигналу.

Таблиця 1.

Результати дослідження впливу порогу вбудовування T на якість аудіо

Параметр T	A1	A2	A3	A4	A5	A6
T=1	62.736	51.686	68.843	51.923	50.798	47.272
T=1.5	62.712	51.649	68.826	51.917	50.796	47.238
T=2	62.686	51.614	68.811	51.908	50.793	47.231
T=2.5	62.660	51.567	68.796	51.899	50.790	47.192
T=3	62.633	51.519	68.779	51.890	50.788	47.175
T=3.5	62.593	51.482	68.762	51.883	50.786	47.139
T=4	62.572	51.445	68.747	51.875	50.784	47.107
T=4.5	62.542	51.410	68.732	51.867	50.781	47.076
T=5	62.518	51.378	68.713	51.859	50.779	47.015
T=5.5	62.469	51.345	68.698	51.849	50.777	46.929
T=6	62.378	51.309	68.682	51.840	50.774	46.869
T=6.5	62.296	51.276	68.663	51.831	50.772	46.811
T=7	62.230	51.236	68.646	51.819	50.769	46.755
T=7.5	62.156	51.196	68.632	51.809	50.767	46.699
T=8	62.092	51.155	68.616	51.801	50.764	46.664
T=8.5	62.035	51.119	68.599	51.791	50.762	46.625
T=9	61.970	51.066	68.584	51.784	50.760	46.575

Наприклад, для файлу A1 рівень SNR змінюється незначно — з 62,736 дБ до 61,970 дБ при збільшенні порогу T від 1 до 9, що демонструє слабкий ефект порогової зміни.

Для оцінки якості зображення після вбудовування цифрового водяного знака було використано іншу метрику – PSNR (Peak Signal-to-Noise Ratio). Ця метрика визначає відношення максимальної потужності сигналу (пікового значення) до потужності шуму, що вноситься під час обробки, та обчислюється за формулою:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX^2}{MSE}\right), \tag{9}$$

де MAX – максимальне значення пікселю, MSE – середньоквадратичне відхилення [5].

На основі отриманих результатів було встановлено, що зі зростанням порогу вбудовування T спостерігається поступове зниження показника PSNR для всіх типів зображень. PNG-зображення (P1, P2) демонструють значно вищу стійкість до спотворень, ніж JPEG-зображення (P3–P6), що обумовлено менш агресивною природою формату PNG.

Це свідчить про доцільність використання форматів без втрат при вбудовуванні ЦВЗ, особливо у випадках, коли важливо зберегти високу якість візуального сприйняття. В ході аналізу вбудовування виконувалося в середньочастотні компоненти блоків зображення з індексами [4,1] та [3,2]. Результати дослідження впливу порогу вбудовування на якість зображень показана на рисунку 6.

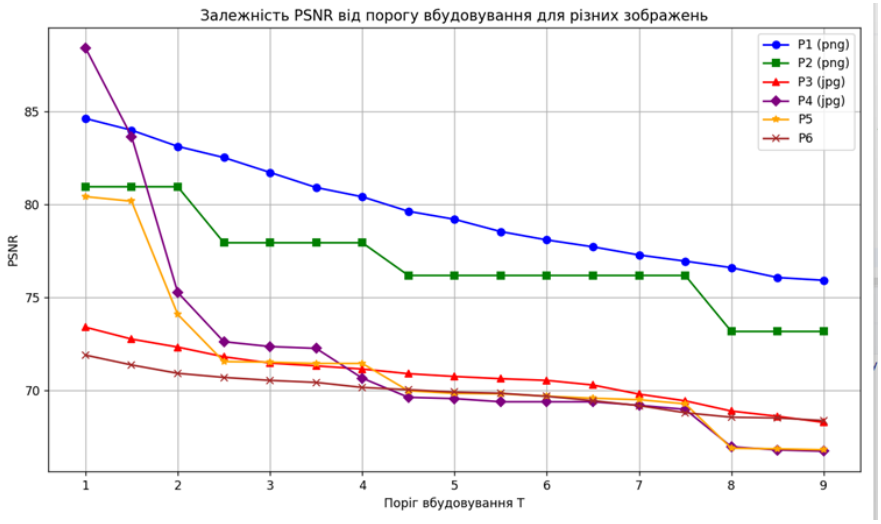


Рис. 6. Графік залежності якості ЦВЗ від порогу вбудовування

Для реалізації розробленого алгоритму у веб-застосунку було обрано порогове значення *T*, що дорівнює 4. Для оцінки розробленого алгоритму були використані вже описані метрики PSNR, SNR, а також метрика SSIM (structural similarity index measure).

Результати оцінювання ефективності реалізації запропонованого алгоритму демонструють достатньо високу якість відеофайлів після вбудовування цифрового водяного знака (див. таблицю 2).

Таблиця 2.

Результати оцінки ефективності реалізації запропонованого алгоритму

Номер відеофайлу	PSNR	SNR	SSIM
1	45,30	29,23	0,9887
2	41,71	32,21	0,9796
3	43,47	21,73	0,9754
4	41,58	31,57	0,9841
5	39,91	29,29	0,9771

Значення PSNR перевищують 39 дБ, SSIM – понад 0.97, що свідчить про незначні візуальні спотворення, а рівень SNR у більшості випадків становить понад 29 дБ, що вказує на збереження акустичної якості.

Висновки. У цій статті розглянуто застосування цифрових водяних знаків для захисту мультимедійних файлів. Проаналізовано сучасні методи вбудовування ЦВЗ у просторовій та частотній областях, а також окреслено переваги застосування дискретного косинусного перетворення для підвищення стійкості та непомітності водяного знака. Запропоновано алгоритм вбудовування ЦВЗ у відеофайл, що використовує як стеганоконтейнер кадри та аудіодоріжку, реалізований шляхом модифікації частотних компонентів за методом Коха-Жао у частотній області, отриманій внаслідок застосування ДКП.

Особливістю запропонованого підходу є використання одного текстового ключа для генерації ЦВЗ за допомогою HMAC-SHA256, а також для формування псевдовипадкової вибірки блоків для модифікації. Результати експериментальної оцінки за метриками PSNR, SSIM та SNR свідчать про допустиме погіршення якості відео після вбудовування, що дозволяє зробити висновок про непомітність цифрового водяного знака для кінцевого користувача.

Водночас питання стійкості вбудованого ЦВЗ до типових атак, таких як стиснення, масштабування, зміна формату тощо, потребує окремого аналізу. У

подальших дослідженнях доцільно провести розширене тестування алгоритму з метою оцінки його надійності та стійкості в умовах реальних загроз.

Реалізація алгоритму у вигляді веб-застосунку підтверджує його практичну придатність і потенціал для подальшого вдосконалення та адаптації до різних типів мультимедійного контенту.

Список літератури

1. Зубко І. С., Мартовицький В. О., Пунченко А. В., Карачевцев Д. Д. Огляд методів нанесення цифрових водяних знаків для захисту зображень. *Системи управління, навігації та зв'язку.* 2024. № 3. С. 121–125. DOI: 10.26906/SUNZ.2024.3.121.
2. Kadhim, I. J., Premaratne, P., Alwan, Z. A. Invisible Video Watermarking Based on Frame Selection and LSB Embedding. *International Journal of Intelligent Engineering and Systems*. 2024. Vol.17, №3. P.41-53. DOI: 10.22266/ijies2024.0630.04
3. Md. Asikuzzaman, M. Pickering. An Overview of Digital Video Watermarking. *IEEE Transactions on Circuits and Systems for Video Technology*. 2017. P. 1-24. DOI: 10.1109/TCSVT.2017.2712162
4. Салієва О., Грицак А., Гуменюк В., Білик О. Удосконалення стеганографічного методу вбудовування крихких водяних знаків для підвищення захищеності потокового відео від несанкціонованої модифікації. *Вимірювальна та обчислювальна техніка в технологічних процесах.* 2023. № 75. С. 197–205. DOI: https://doi.org/10.31891/2219-9365-2023-75-23.
5. A. Al-Gindy, A. Omar, O. Mashal, Y. Shaker, E. Alhogaraty, S. Moussa. A new watermarking scheme for digital videos using DCT. *Open Computer Science*.2022. P. 248-259. DOI: 10.1515/comp-2022-0238.
6. Zhou M., Kuchuk N., Grynov D. A robust method for embedding and extracting watermarks in video using discreate cosine transform. *Control, Navigation and Communication Systems*. 2024. № 3. P. 166-169. DOI: 10.26906/SUNZ.2024.3.166.
7. Ramakrishnan S. Digital image and video watermarking and steganography. London : IntechOpen, 2019. 75 p.
8. Jabbar K.K., Tuieb M.B. Compare between DCT and DWT for digital watermarking in color image. *Information and Knowledge Management.* 2015. Vol. 5, No. 7. P. 22–32.
9. Kanhe A., Gnanasekaran A. Robust image-in-audio watermarking technique based on DCT-SVD transform. *EURASIP Journal on Audio, Speech, and Music Processing*. 2018. №16. 12 p. DOI: 10.1186/s13636-018-0139-3.
10. Шостак Н. В. Аналіз характеристик алгоритмів вбудовування цифрового водяного знаку на тлі атак і завад у каналах зв'язку. *Проблеми телекомунікацій.* 2019. № 1 (24). С. 34–50. DOI: https://doi.org/10.30837/pt.2019.1.03.

AN ALGORITHM FOR EMBEDDING A DIGITAL WATERMARK INTO AUDIO AND VIDEO COMPONENTS OF A MULTIMEDIA FILE

K.S. Chabanenko, N.I. Kushnirenko, V. Podufalov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: chabanenkoksenia3@gmail.com, kushnirenko@op.edu.ua

This article examines the application of digital watermarks as an effective means of protecting multimedia files. It describes the main watermarking methods, including the spatial approach of least significant bit replacement, as well as frequency-domain techniques such as discrete Fourier transform (DFT), discrete wavelet transform (DWT), and discrete cosine transform (DCT). An algorithm for embedding a digital watermark into a video file is proposed, which utilizes both the video frames and the audio track of the input file as a container for hidden information. The algorithm is based on the Koch–Zhao method for modifying frequency coefficients obtained through DCT, as well as on the cryptographic HMAC-SHA256 function for generating the digital watermark based on the user-specified message key. The implementation sequence is described: splitting the video file into frames and audio blocks, generating a block selection pattern based on the length of the message key and the total number of blocks, frequency-domain transformation of the selected segments, and finally, formation and embedding of the mark. The embedding is performed only into fragments with ordinal numbers that are multiples of a parameter computed based on the key length and the total number of blocks. The developed algorithm has been implemented as a web application, which allows both embedding and verification of the digital watermark. The image and audio quality after embedding were assessed using PSNR, SSIM, and SNR metrics. Experimental results confirmed the preservation of a high level of visual and auditory perception. The proposed algorithm has promising practical applications in systems for copyright protection, content integrity monitoring, and digital identification of multimedia data. At the same time, given the current stage of testing, it is advisable to conduct additional experimental studies to assess its robustness, scalability, and efficiency under various application conditions.
Keywords: steganography, digital watermark, discrete cosine transform, HMAC, multimedia data, information protection.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 15, номер 3, 2025. Одеса – 165 с., іл.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 15, No. 3, 2025. Odesa – 165 p.

Засновник: Національний університет «Одеська політехніка»

Зареєстровано Міністерством юстиції України 04.04.2011р.
Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Національного університету «Одеська політехніка», (протокол № 3 від 30.09.2025р.)

Адреса редакції: Національний університет «Одеська політехніка»,

1, Шевченка проспект, Одеса 65044 Україна

Web: www.immm.op.edu.ua (immm.opu.ua)

Email: immm.ukraine@gmail.com