CRYPTOLOGY

DOI 10.20535/2411-1031.2025.13.2.344591
УДК 004.056.55:004.89:519.876.5

ЄВГЕН ЖИВИЛО,
ЮРІЙ КУЧМА

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ІНТЕЛЕКТУАЛЬНО-КРИПТОГРАФІЧНОГО ЗАХИСТУ АВТЕНТИФІКАЦІЙНИХ КЛЮЧІВ

У статті обґрунтовано науково-методичні засади математичного моделювання інтелектуально-криптографічних систем превентивного реагування на загрози компрометації автентифікаційних ключів. Запропоновано узагальнену концептуальну модель, що інтегрує криптографічні механізми симетричного шифрування (зокрема алгоритм AES), стеганографічні методи приховування криптографічних параметрів та інтелектуальні модулі прогнозування атак, сформовані на базі методів глибокого навчання. Розроблений математичний апарат ґрунтується на синтезі положень теорії ймовірностей, інформаційної ентропії та адаптивної оптимізації, що забезпечує кількісну оцінку ризиків компрометації та формування динамічних стратегій реагування в умовах змінних загроз. Особливу увагу приділено формалізації процесів адаптивного налаштування рівня криптографічної складності та ступеня прихованості залежно від результатів інтелектуального аналізу трафіку й виявлення аномалій у каналах передавання даних. Розглянуто підходи до побудови енергетично та обчислювально ефективних реалізацій таких систем для вбудованих і мобільних середовищ із обмеженими ресурсами. Отримані результати закладають наукове підґрунтя для розроблення нового класу інтелектуально-криптографічних систем, здатних до самонавчання, адаптивного управління параметрами безпеки та превентивного реагування на потенційні загрози компрометації автентифікаційних даних у динамічному інформаційному просторі.

Ключові слова: кібербезпека, нейронні мережі, математичне моделювання, інтелектуально-криптографічна система, превентивне реагування, автентифікаційні ключі, ентропійний аналіз, адаптивна оптимізація, глибоке навчання.

Постановка проблеми. Сучасні системи автентифікації та управління криптографічними ключами перебувають під постійним тиском з боку зростаючої кількості кіберзагроз, зокрема цілеспрямованих атак, спрямованих на компрометацію ключової інформації. Традиційні криптографічні підходи, попри високу математичну стійкість, виявляються недостатньо ефективними у динамічних середовищах, де характер атак швидко змінюється, а канали передавання даних піддаються стегоаналітичному аналізу з боку зловмисників. Додаткової складності набуває проблема у зв’язку з поширенням вбудованих, мобільних та енергообмежених пристроїв, у яких реалізація повноцінних криптографічних механізмів часто неможлива без компромісів між рівнем захисту та продуктивністю.

У межах сучасної парадигми інформаційної безпеки дедалі більшої актуальності набуває концепція превентивного реагування, що передбачає не лише виявлення та блокування атак, а й їхнє прогнозування на основі інтелектуального аналізу поведінкових і статистичних характеристик інформаційних потоків. Застосування методів машинного та глибокого навчання у криптографічних системах відкриває можливості для побудови самонавчальних архітектур, здатних динамічно змінювати рівень прихованості, ентропійну складність та параметри шифрування залежно від оціненого рівня ризику компрометації.

Водночас відсутність формалізованих математичних моделей, які б описували взаємодію між криптографічними, стеганографічними та інтелектуальними компонентами в єдиному теоретичному полі, ускладнює системний підхід до побудови таких рішень. Недостатньо

розробленим залишається також апарат кількісного оцінювання ймовірності успіху атак із використанням методів глибокого навчання, що обмежує можливості аналітичного прогнозування ризиків.

Таким чином, постає науково-практична проблема математичного моделювання інтелектуально-криптографічних систем превентивного реагування, спрямованого на формування узагальненого апарату аналізу, оцінювання та оптимізації параметрів безпеки в умовах динамічних загроз. Її розв'язання створить передумови для розроблення нового класу адаптивних систем захисту, здатних до самонавчання, передбачення потенційних атак і мінімізації ризиків компрометації автентифікаційних ключів у складних інформаційних середовищах.

Аналіз останніх досліджень та публікацій. Предметна область комбінування криптографічних та стеганографічних технік із інтелектуальними модулями аналізу швидко еволюціонує на перетині прикладної математики, теорії інформації та машинного навчання. Історично методологічний фундамент стеганографії і стегоаналізу закладено класичними працями, що сформулювали стохастичні та статистичні підходи до виявлення вбудованих повідомлень у цифрових об'єктах; ці підходи залишаються релевантними як теоретична база для подальшої формалізації ймовірнісних моделей стего-сигналу [1].

Паралельно відбувається інтенсивний розвиток глибинних нейронних архітектур як у ролі механізмів приховування (neural steganography), так і у ролі детекторів (neural steganalysis). Наскрізні архітектурні рішення, зокрема HiDDeN, продемонстрували життєздатність методів, що навчаються безпосередньо на задачі вбудовування й відновлення інформації в спостережуваних сигналах, одночасно змінюючи класичні припущення про статичні моделі помилок і шуму в каналі. Розвиток архітектур детекторів (SRNet, Yedroudj-Net та ін.) показав підвищення ефективності виявлення за рахунок глибоких представлень, але також виокремив проблему формалізації статистичних гарантій та здатності моделей зберігати ефективність у разі варіацій параметрів каналу та динамічних атак [2].

У криптографічному менеджменті ключів та нормативної практики помітну роль відіграють спеціальні рекомендації щодо керування ключовим матеріалом, які надають орієнтири для визначення життєвого циклу ключів, політик ротації та процедури оцінювання ризику. Зокрема, рекомендації NIST із менеджменту ключів формалізують класи процедур і метрик, що є необхідними для інтеграції в адаптивні системи контролю та автоматизованого прийняття рішень щодо криптографічних параметрів. Поєднання таких нормативних підходів із методами кількісного оцінювання ризику є важливим кроком для практичної реалізації інтелектуально-криптографічних систем [3].

Аналітичні звіти міжнародних та національних агенцій служать контекстною опорою для технічних досліджень, оскільки вони ілюструють динаміку загроз та пріоритетні сценарії компрометації. Звіти ENISA з формування «Threat Landscape» підкреслюють зростаючу роль адаптивних та соціотехнічних векторів атак, що стимулює потребу у превентивних інструментах із прогнозною аналітикою. Аналогічно, матеріали CERT-UA та суміжних національних служб фіксують локалізовані сценарії атак і надають дані про реальні інциденти, які доцільно залучати як емпіричні набори для навчання й апробації детекторів та ризик-моделей [4].

У науковій літературі та прикладних звітах виокремлюються кілька системних прогалин, що вимагають математично обґрунтованих рішень. По-перше, відсутність уніфікованого стохастичного апарату для одночасного опису ймовірності компрометації ключів, характеристик стего-помилок та поведінкових ознак аномалій трафіку унеможливлює формальну агрегацію ризику; це відкриває шлях до розробки багатовимірних марківських, ієрархічних баєсових чи спряжених стохастичних моделей. По-друге, неформалізована «адаптивна криптографічна вартість» – показник, що пов'язує обчислювальні/енергетичні

витрати з очікуваним підвищенням стійкості, що ускладнює багатокритеріальні оптимізаційні задачі в ресурсно-обмежених середовищах (IoT, мобільні пристрої) [5]. По-третє, існує нагальна потреба в аналітичних інструментах для кількісної оцінки робастності нейронних детекторів (зокрема, теоретичних меж помилок першого й другого роду) у змінених канальних умовах; для цього необхідне застосування методу великих відхилень та концентраційних нерівностей [1].

Синтез теоретичних і практичних напрацювань вимагає міждисциплінарного підходу: поєднання прикладної теорії ймовірностей, ентропійного аналізу, методів оптимізації та сучасних технік машинного навчання (глибинні архітектури, онлайн-навчання, детектори аномалій). Це передбачає як теоретичне доведення властивостей запропонованих моделей (конвергенція адаптивних процедур, гарантії зниження ризику), так і створення реплікованих бенчмарків: наборів атак, симульованих каналів із реалістичними перетвореннями та енергетичних профілів апаратних платформ. Крім того, для забезпечення прикладної цінності необхідно співвіднести наукові висновки з вимогами та рекомендаціями стандартизуючих органів, що визначатиме прийнятні пороги ризику для впровадження адаптивних механізмів у промислових системах [3].

Отже, огляд літератури й аналітичних звітів підтверджує необхідність подальшого математичного опрацювання та експериментальної апробації інтелектуально-криптографічних підходів: розроблення узагальнених стохастичних моделей ризику, формалізація метрик «адаптивної криптографічної вартості», теоретичне обґрунтування робастності нейронних детекторів і конструювання енерго-ефективних алгоритмів для вбудованих систем. Виконання цих завдань створить надійну наукову основу для практичної реалізації превентивних систем захисту автентифікаційних ключів [1], [3].

Метою даної статті є розроблення та обґрунтування математичної моделі інтелектуально-криптографічної системи превентивного реагування на загрози компрометації автентифікаційних ключів, яка забезпечує інтеграцію криптографічних, стеганографічних та інтелектуальних компонент у єдиному адаптивному середовищі захисту даних.

Для досягнення поставленої мети передбачено вирішення таких наукових взаємопов’язаних завдань:

аналітико-концептуальне завдання, що полягає у систематизації сучасних підходів до криптографічного та стеганографічного захисту та критичному аналізі методів глибокого навчання для виявлення, прогнозування та попередження атак на автентифікаційні механізми, із акцентом на формуванні теоретичних критеріїв ефективності детекторів і алгоритмів приховання, що забезпечують основу для математичної формалізації адаптивних систем;

математико-моделювальне завдання, яке полягає у підготовці формалізованого апарату для опису взаємодії криптографічних, стеганографічних та інтелектуальних компонентів системи шляхом побудови багатовимірних стохастичних моделей, що дозволяють кількісно оцінювати ймовірність компрометації ключів, розраховувати інформаційну ентропію каналів передачі та оптимізувати параметри системи за допомогою адаптивних процедур з урахуванням історичних даних про атаки та виявлені аномалії;

інженерно-прикладне завдання котре полягає у розробленні архітектурних рішень та моделей енергетично й обчислювально ефективної реалізації системи для вбудованих і мобільних середовищ з обмеженими ресурсами, із акцентом на механізмах адаптивного налаштування рівня криптографічної складності та ступеня прихованості залежно від результатів інтелектуального аналізу трафіку й виявлення аномалій у каналах передачі, що забезпечує динамічне балансування між безпекою та ресурсною ефективністю.

Отже, досягнення окреслених цілей дозволить реалізувати зазначені завдання та створити науково обґрунтовану основу для формування нового покоління інтелектуально-

криптографічних систем, здатних до самонавчання, превентивного реагування та мінімізації ризиків компрометації автентифікаційних ключів у динамічному інформаційному середовищі.

Основний матеріал дослідження. У сучасних інформаційних системах захист автентифікаційних ключів є критичною задачею, що потребує комплексного підходу, інтегруючого криптографічні, стеганографічні та інтелектуальні методи. Першим етапом дослідження є аналітико-концептуальна складова, яка спрямована на систематизацію сучасних підходів до криптографічного та стеганографічного захисту, а також критичний аналіз методів глибокого навчання для виявлення, прогнозування та попередження атак на автентифікаційні механізми. З математичної точки зору це передбачає формалізацію системи як сукупності компонентів

$$C = \{C_1, C_2, ..., C_n\}, \tag{1}$$

де $C_1, ..., C_k$ – криптографічні модулі;

$C_{k+1}, ..., C_m$ – стеганографічні методи приховування ключів;

$C_{m+1}, ..., C_n$ – інтелектуальні детектори атак.

Ефективність кожного компонента оцінюється через функцію корисності:

$$U(C_i) = \omega_1 P_{\text{detect}} - \omega_2 P_{\text{false}} + \omega_3 H(C_i), \tag{2}$$

де P_{detect} – ймовірність коректного виявлення загрози;

P_{false} – ймовірність хибного спрацювання;

$H(C_i)$ – ентропія каналу передачі;

$\omega_1, \omega_2, \omega_3$ – вагові коефіцієнти, що відображають пріоритетність окремих критеріїв. Такий підхід дозволяє кількісно оцінювати ефективність детекторів та алгоритмів приховання, що є основою для побудови адаптивних систем [6].

Для формалізації прогнозування атак застосовується **стохастичний підхід**, де ймовірність компрометації ключів $R(t)$ у часі t визначається як:

$$\begin{aligned} R(t) &= 1 - \prod_{i=1}^{n} \left(1 - P_{\text{comp}}(C_i, t)\right) \\ P_{\text{comp}}(C_i, t) &= f\left(\lambda(t), X(t), U(C_i)\right) \end{aligned}, \tag{3}$$

де $\lambda(t)$ – інтенсивність атак;

$X(t)$ – параметри каналу передачі;

$f(\cdot)$ – функція, що інтегрує вплив усіх компонентів системи.

Така стохастична модель дозволяє формалізувати рівень ризику компрометації та враховувати взаємозв'язок між ефективністю захисту та характеристиками каналу.

Інтелектуальні модулі прогнозування атак, побудовані на методах глибокого навчання, оцінюють ймовірності аномалій у каналах передачі ключів і впливають на параметри криптографічного та стеганографічного захисту. Формально, адаптивне регулювання можна описати через оптимізаційну задачу:

$$\max_{\theta} = \sum_{i=1}^{n} U(C_i, \theta) - \alpha \cdot \sum_{i=1}^{n} C_{\text{res}}(C_i, \theta), \tag{4}$$

де θ – вектор параметрів адаптації;

$C_{\text{res}}(C_i, \theta)$ – обчислювальні та енергетичні витрати;

α – коефіцієнт ваги ресурсної ефективності.

Розв'язання цієї задачі забезпечує динамічне балансування між рівнем безпеки та ресурсними обмеженнями.

Особлива увага сконцентрована на інтеграції криптографічних та стеганографічних методів через комбіновану трансформацію ключа:

$$\mathrm{K_s} = \mathcal{g}\left(\mathrm{E(K)},\ \mathrm{S(K)}, \theta\right), \tag{5}$$

де $\mathrm{E(K)}$ – криптографічне шифрування ключа (AES);

$\mathrm{S(K)}$ – стеганографічне приховання;

θ – параметри адаптивного налаштування, що визначають рівень прихованості та складності шифрування залежно від стану системи та виявлених аномалій.

Таким чином, аналітико-концептуальна складова дослідження формує математичний фундамент для подальшої розробки адаптивної інтелектуально-криптографічної системи, де криптографічні та стеганографічні компоненти взаємодіють із інтелектуальними модулями, забезпечуючи превентивне реагування на загрози компрометації автентифікаційних ключів та кількісну оцінку ризиків у динамічному інформаційному середовищі.

В основі математико-моделювального етапу дослідження лежить необхідність побудови єдиного формалізованого апарату, здатного описати складну взаємодію між криптографічними, стеганографічними та інтелектуальними компонентами системи. Такий підхід дозволяє не лише кількісно оцінювати ризики компрометації, але й забезпечити підґрунтя для адаптивного керування безпекою в умовах динамічних загроз та обмежених обчислювальних ресурсів. Відповідно, метою цього етапу є математична формалізація процесів, що визначають інтегровану поведінку системи в часі, з урахуванням її стохастичної природи, інформаційної ентропії та факторів енергетичної ефективності.

В рамках концептуальної передумови моделювання пропонується інформаційно-захисну систему розглядать як комплексну динамічну структуру, у якій криптографічні алгоритми $(\mathcal{C})$, стеганографічні методи $(\mathcal{G})$ та інтелектуальні механізми аналізу $(\mathcal{I})$ взаємодіють у спільному часовому та просторовому полі.

Таку систему можна представити як вектор станів

$$\mathcal{S}(\mathrm{t}) = \left\{\mathcal{C}(\mathrm{t}),\ \mathcal{G}(\mathrm{t}),\ \mathcal{I}(\mathrm{t})\right\}, \tag{6}$$

де кожна складова функціонує у стохастичному середовищі, описуваному набором випадкових параметрів $\xi(\mathrm{t})$, які визначають інтенсивність атак, рівень шуму в каналах, ентропійну насиченість даних тощо.

Таким чином, дослідження спирається на парадигму стохастичного моделювання, у межах якої поведінка системи є результатом взаємодії детермінованих процесів (алгоритмічних процедур) і випадкових збурень (зовнішніх атак або внутрішніх флуктуацій).

Фундаментом для аналізу ефективності захисту є ймовірнісна оцінка ризику компрометації ключів. Вважаємо, що для трьох незалежних підсистем – криптографічної $\left(P_C\right)$, стеганографічної $\left(P_G\right)$ та інтелектуальної $\left(P_I\right)$ – інтегральна ймовірність компрометації визначається як:

$$P_{\mathrm{comp}}(t) = 1 - \prod_{\iota \in \{C,G,I\}} \left(1 - P_\iota(t)\right). \tag{7}$$

Однак у реальних умовах між підсистемами спостерігається некорельована або частково корельована поведінка, що вимагає введення коефіцієнтів міжкомпонентної залежності $\rho_{\iota j}$:

$$P_{\mathrm{comp}}(t) = 1 - \prod_{\iota=1}^{3}\left(1 - P_\iota(t)\right) + \sum_{\iota<1} \rho_{\iota j} P_\iota(t) P_j(t). \tag{8}$$

Таке структурування дозволяє формалізувати синергетичні ефекти, коли взаємодія криптографічних і стеганографічних механізмів сприяє взаємному підсиленню загальної стійкості системи, що має ключове значення для побудови адаптивних структур захисту.

Наступним етапом є оцінювання інформаційної ентропії каналів передавання, яка визначає рівень непередбачуваності даних і, відповідно, потенційну стійкість до криптоаналізу. Динамічна ентропія сигналу у момент часу визначається:

$$H_t\left(X\right)=-\sum_{\iota=1}^{n}\rho_\iota\left(t\right)\log_2\rho_\iota\left(t\right) \tag{9}$$

де $\rho_\iota\left(t\right)$ – ймовірність появи ι-го символьного стану.

Для стеганографічних каналів доцільно використовувати умовну ентропію:

$$H\left(X\middle|S\right)=-\sum_{\iota,j}^{n}\rho\left(\boldsymbol{x}_\iota,\boldsymbol{\mathcal{S}}_j\right)\log_2\rho_\iota\left(\boldsymbol{x}_\iota\middle|\boldsymbol{\mathcal{S}}_j\right), \tag{10}$$

де $\boldsymbol{\mathcal{S}}$ – сукупність прихованих сигналів.

Метою є досягнення максимальної умовної ентропії при збереженні допустимого рівня надлишковості, тобто

$$\begin{gathered}\frac{\partial H\left(X\middle|S\right)}{\partial S}=0\\ H\left(X\middle|S\right)\to\max\end{gathered}, \tag{11}$$

що забезпечує мінімальну ймовірність виявлення стеганографічних структур.

Цей показник використовується як частина багатокритеріальної оптимізації, що визначає компроміс між безпекою, прихованістю та обчислювальною вартістю.

Інтелектуальний компонент системи формує адаптивну модель поведінки атакувального середовища.

В основі лежить байєсівська формула оновлення апостеріорних ймовірностей:

$$P\left(A\middle|D\right)=\frac{P\left(D\middle|A\right)P\left(A\right)}{P\left(D\right)}, \tag{12}$$

де A_t – подія атаки, а D_t – сукупність детектованих аномалій.

Інтенсивність атак λ_t описується пуассонівським процесом:

$$P\left(k\text{ атак за }t\right)=\frac{\left(\lambda_t t\right)^k e^{-\lambda_t t}}{k!}, \tag{13}$$

а її поточне значення коригується на основі результатів глибинного навчання, яке моделює залежність між поведінкою атакувальних агентів і динамікою вразливостей системи.

Таким чином, система постійно оновлює свої апостеріорні оцінки ризику, використовуючи адаптивні нейронні процедури у реальному часі, що забезпечує самонавчальний характер безпекового середовища.

Для інтеграції криптографічної, стеганографічної та інтелектуальної підсистем застосовується багатокритеріальний підхід оптимізації у вигляді цільової функції:

$$\min_\theta J\left(\theta\right)=\alpha_1 R\left(\theta\right)+\alpha_2 C_{\text{comp}}\left(\theta\right)-\alpha_3 H\left(\theta\right), \tag{14}$$

де $R\left(\theta\right)$ – очікуваний ризик компрометації;

$C_{\text{comp}}\left(\theta\right)$ – витрати обчислювальних ресурсів;

$H\left(\theta\right)$ – ентропійна стійкість каналу;

α_i – вагові коефіцієнти, що визначають пріоритети системи.

Для забезпечення стійкої адаптації виконується умова монотонного зниження функціоналу:

$$\frac{dJ(\theta)}{dt} \le 0\,,\ \forall t\,, \tag{15}$$

що гарантує асимптотичну стабільність процесу навчання системи.

У разі використання стохастичних градієнтних методів навчання цей критерій виконує роль локального принципу Ляпунова, що забезпечує збіжність параметрів навіть за наявності стохастичного шуму в даних.

Для повного опису взаємодії компонентів система моделюється через рівняння стохастичної динаміки:

$$\frac{d\mathrm{X}(t)}{dt} = \mathrm{A}(t)\mathrm{X}(t) + B(t)U(t) + \mathrm{W}(t), \tag{16}$$

де $\mathrm{X}(t)$ – вектор станів системи (рівень криптографічної складності, ентропійна насиченість, інтенсивність атак);

$U(t)$ – вектор керувань (параметри адаптації);

$\mathrm{W}(t)$ – стохастичні впливи зовнішнього середовища.

Система є стійкою, якщо $\rho\left(A(t)\right) < 0$, тобто власні значення матриці переходів мають від'ємну дійсну частину. Це гарантує асимптотичну збіжність станів системи до стійкої траєкторії навіть при зовнішніх збуреннях.

Таким чином, побудована математична модель забезпечує формалізацію процесів взаємодії між криптографічними, стеганографічними та нейронними компонентами системи, дозволяючи кількісно оцінювати ймовірність компрометації автентифікаційних ключів і визначати ентропійну стійкість каналів передачі.

Запропонований підхід створює можливість здійснювати адаптивне керування параметрами безпеки з урахуванням історичних даних про атаки та динаміку виявлених аномалій, забезпечуючи при цьому оптимальний баланс між рівнем криптографічного захисту, ступенем прихованості та енергетичною ефективністю. У сукупності ці властивості формують теоретико-аналітичний фундамент для подальшого переходу до інженерно-прикладного рівня, де реалізуються архітектурні, алгоритмічні та програмно-апаратні рішення інтелектуально-криптографічної системи превентивного реагування.

Інженерно-прикладна складова дослідження спрямована на практичну імплементацію розроблених математичних принципів у вигляді архітектурно завершеної системи, оптимізованої для роботи у вбудованих та мобільних середовищах із обмеженими ресурсами. Основна мета цього етапу полягає у створенні технічно узгодженої інфраструктури, здатної динамічно балансувати між рівнем безпеки, обчислювальною складністю та енергоспоживанням. При цьому ключову роль відіграють механізми адаптивного налаштування параметрів криптографічних і стеганографічних процесів залежно від поточних умов середовища та результатів інтелектуального аналізу трафіку.

Запропонована архітектура системи представлена на структурній схемі (рис. 1), де відображено взаємодію між трьома рівнями – сенсорним, аналітико-регуляторним і криптографічно-адаптивним. Потоки даних і сигнали керування реалізовані у вигляді двонаправлених зв'язків, що забезпечують замкнене контурне керування безпековими параметрами в реальному часі.

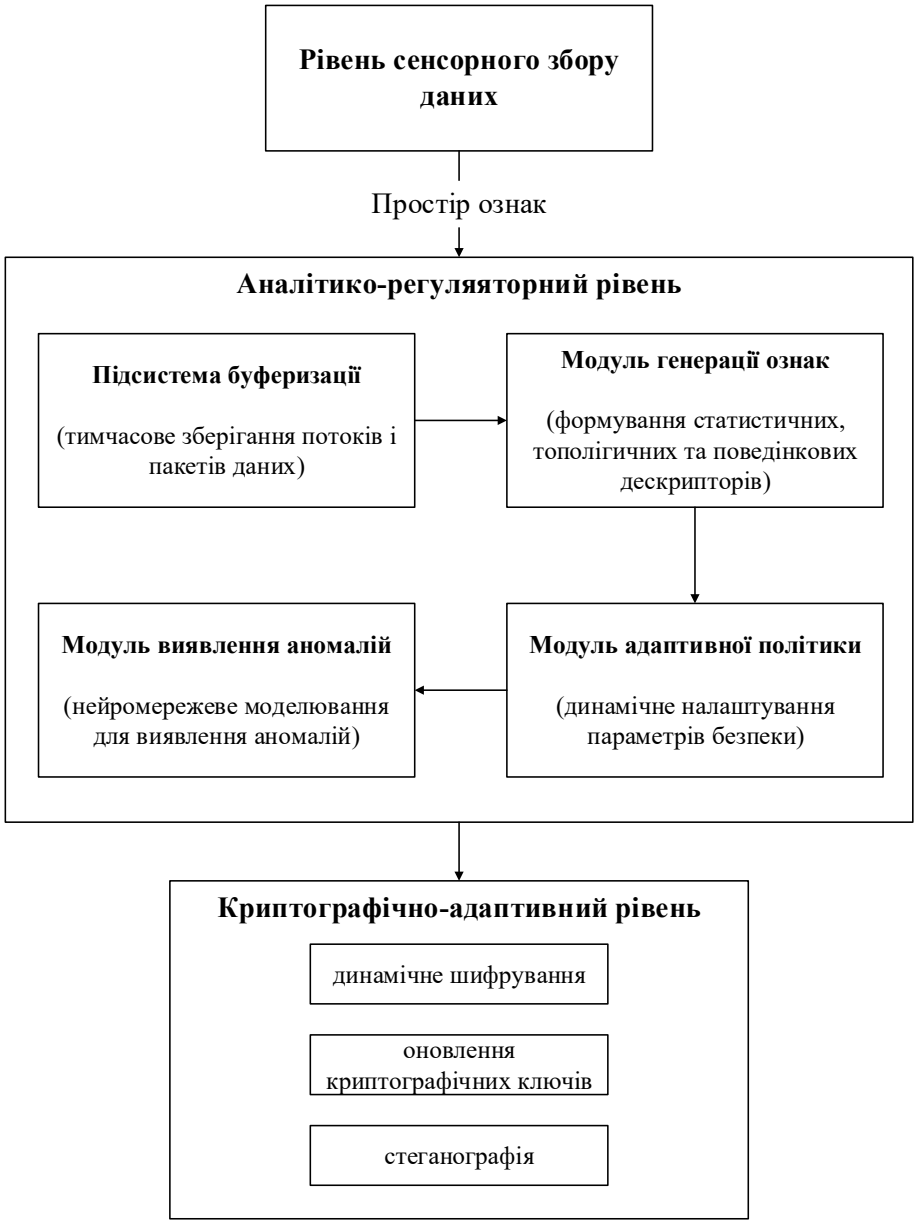

Рис. 1 – Структурна схема трирівневої архітектури інтелектуально-криптографічної системи

Як зазначається, інженерно-прикладна реалізація інтегрує результати попередніх математичних та аналітико-концептуальних етапів дослідження, формуючи єдине функціональне середовище, здатне до самоадаптації, прогнозування та динамічної оптимізації параметрів безпеки в реальному часі.

Така інтеграція формує синергетичний зв’язок між теоретичними моделями та прикладними механізмами управління ризиками, забезпечуючи цілісність процесу аналізу, прогнозування та реагування на кіберзагрози. Завдяки цьому створюється науково обґрунтована основа для розроблення енергетично та обчислювально ефективних криптографічних систем нового покоління. Запропонований підхід відкриває можливості практичної реалізації таких систем у мобільних, вбудованих і розподілених обчислювальних середовищах, де традиційні методи криптозахисту є надмірно ресурсоємними та не забезпечують достатнього рівня адаптивності до динамічних змін профілю загроз.

Отже система передбачає трирівневу архітектуру, що поєднує функціональну розподіленість і гнучкість управління потоками даних у режимі реального часу, а саме:

Рівень сенсорного збору даних – забезпечує оброблення потоків інформації з датчиків, мобільних пристроїв або вузлів IoT-інфраструктури (температурні сенсори, GPS-трекери, смарт-камери, BLE-браслети тощо) [7]. На цьому рівні здійснюється первинна фільтрація сигналів та виявлення аномалій із застосуванням легковагових алгоритмів, таких як EWMA (Exponentially Weighted Moving Average) або Z-score detection, що дозволяє зменшити навантаження на аналітико-регуляторний рівень. Додатково виконуються процедури усунення шумів, ідентифікації та заповнення пропущених значень та нормалізації даних у форматах, придатних для подальшої обробки (наприклад, JSON або CBOR).

Рівень використовує протоколи MQTT, CoAP або AMQP для енергоефективної передачі даних у центральний вузол. У системах із високою затримкою, а також в умовах обмежених ресурсів може застосовуватись DTN (Delay Tolerant Networking) з метою мінімізації пропускного навантаження.

У результаті формується атрибутний простір $\mathrm{X} = \{x_1, x_2, ..., x_n\}$. Попередня обробка описується як:

$$\Phi\left(X_t(t)\right) = \mathrm{Norm}\left(\mathrm{Filter}\left(X_t(t)\right)\right), \tag{17}$$

де Filter – функція згладжування шуму;

Norm – нормалізація до уніфікованої шкали $[0,1]$

В подальшому вектор сенсорних спостережень передається до аналітичного модуля для подальшого інтелектуального аналізу.

Аналітико-регуляторний рівень – виконує ідентифікацію, класифікацію та прогнозування загроз на основі методів машинного навчання. Тут функціонує модуль глибокого аналізу трафіку, який використовує моделі виду

$$f_\theta(\mathrm{X}) = y,\ y \in [0,1],$$

де y – оцінка ймовірності виникнення аномальної активності [8].

На цьому рівні реалізується система адаптивних тригерів, що формує регулюючі сигнали до криптографічного рівня залежно від динаміки виявлених аномалій. У разі зростання ризику компрометації модель ініціює підвищення рівня шифрування або застосування стеганографічних приховувальних процедур.

Аналітико-регуляторний рівень є центральною ланкою системи, що забезпечує інтелектуальний аналіз потокових даних, виявлення відхилень у поведінці системних компонентів та формування керуючих впливів на криптографічно-адаптивний рівень. Його робота базується на принципах оперативної обробки даних (stream-processing), глибинного навчання та адаптивного управління ризиками.

1. **Обробка потокових даних у реальному часі**. На цьому етапі реалізується високопродуктивна обробка потокових даних у режимі реального часу з використанням технологій stream-processing, таких як Apache Kafka Streams або Apache Flink. Потоки даних $D_t = \{d_1, d_2, ..., d_m\}$ обробляються з урахуванням часової послідовності надходження, що дозволяє здійснювати контекстно-залежний аналіз подій і виявляти кореляційні залежності між подіями в системі.

2. **Детекція аномалій засобами глибокого навчання**. Механізм виявлення аномалій базується на застосуванні моделей глибоких нейронних мереж [9], зокрема:

– *Autoencoder* – для реконструкції нормальної поведінки та оцінювання відхилень через помилку відновлення:

$$\varepsilon_t = \left\| X_t - X_t \right\|^2, \tag{18}$$

де X_t – вхідний вектор атрибутів;

X_t – його реконструкція.

– *LSTM* (Long Short-Term Memory) – для аналізу часових послідовностей мережевих подій та виявлення довготривалих залежностей.

– *GNN* (Graph Neural Networks) – для моделювання топологічних зв'язків між вузлами мережі при аналізі структурованого трафіку.

Критерієм виявлення аномалії є перевищення похибки реконструкції або відхилення ймовірності нормальної поведінки від допустимого порогу:

$$\varepsilon_t > \theta \quad \Rightarrow \quad X_t \in \Omega_{\text{anom}}, \tag{19}$$

де Ω_{anom} – множина виявлених аномалій.

3. **Прогнозування атак у часовій перспективі**. Для оцінювання ймовірності появи атак у майбутньому часовому інтервалі використовується стохастична модель прогнозування:

$$P\left(A_{t+k} \middle| X_t\right), \tag{20}$$

де $P\left(A_{t+k} \middle| X_t\right)$ – умовна ймовірність виникнення атаки через k часових кроків, виходячи зі стану системи $\left|X_t\right.$ у момент часу t.

Ця модель дозволяє не лише виявляти поточні загрози, а й передбачати можливі сценарії атак, що формує основу для проактивного управління безпекою.

4. **Адаптивне регулювання криптографічного навантаження**. Реалізація адаптивного керування безпековими параметрами здійснюється через модуль Security Controller, який реалізує політику прийняття рішень у вигляді відображення:

$$\pi : f\left(X_t\right) \to C_t, \tag{21}$$

де $f\left(X_t\right)$ – функція оцінювання ризику на основі поточного стану системи;

C_t – вектор криптографічних параметрів, що включає рівень шифрування, довжину ключів та ступінь стеганографічного приховування.

В цілому технічна архітектура аналітико-регуляторного рівня передбачає багатокомпонентну організацію обчислювальних процесів, у якій підсистема буферизації даних (Data Buffering Subsystem) виконує функцію тимчасового зберігання потоків і пакетів даних для їх подальшої пакетної або мікропакетної обробки; модуль генерації ознак (Feature Extraction Engine) забезпечує формування статистичних, топологічних та поведінкових дескрипторів мережевого трафіку, що створюють багатовимірний простір атрибутів для аналітичної моделі; модуль виявлення аномалій (Anomaly Detection Engine) реалізує нейромережеве моделювання на основі обчислювальних графів TensorFlow або PyTorch, забезпечуючи високоточну детекцію нетипових патернів у часових рядах і мережевих графах; натомість модуль адаптивної політики (Adaptive Policy Module) здійснює динамічне налаштування параметрів безпеки шляхом розв'язання оптимізаційних задач за допомогою стохастичного градієнтного методу або алгоритмів підкріплювального навчання (Q-learning), що гарантує стійку адаптацію системи до змін середовища та характеру атак.

Математичне формулювання процесу прийняття рішень в адаптивній системі захисту базується на принципі динамічної оптимізації, що забезпечує раціональний баланс між рівнем криптографічної складності та споживанням обчислювальних ресурсів у реальному часі. У контексті ресурсно-обмежених середовищ така оптимізація є критично важливою, оскільки перевищення допустимого порогу навантаження може призвести до деградації продуктивності або втрати здатності системи реагувати на атаки вчасно.

Формалізовано процес прийняття рішень визначається через задачу мінімізації очікуваних витрат при збереженні заданого рівня безпеки, що виражається наступною оптимізаційною моделлю:

$$C_t^* = \arg \min_{C_t \in C} \mathbb{E}\left[\alpha R(C_t) - \beta S(C_t) \middle| f(X_t) \right], \quad (22)$$

де $R(C_t)$ – функція витрат ресурсів (енергетичних, обчислювальних або часових), що залежать від обраної криптографічної конфігурації C_t;

$S(C_t)$ – функція очікуваної ефективності захисту, яка відображає ймовірність успішного запобігання атакам за поточних умов;

$\mathbb{E}[\cdot]$ –математичне сподівання, яке усереднює результати за історичними даними щодо атак, аномалій і навантаження системи;

α та β – вагові коефіцієнти, що визначають пріоритетність між мінімізацією ресурсних витрат і максимізацією рівня безпеки відповідно.

У практичній реалізації ця модель інтегрується в модуль адаптивної політики (Adaptive Policy Module), який виконує безперервне оновлення параметрів C_t згідно з результатами моніторингу та прогнозування ризиків. Функція ризику $f(X_t)$ може бути представлена як нейронна апроксимація, що оцінює поточний стан системи на основі векторів ознак X_t, сформованих з показників трафіку, рівня ентропії, коефіцієнтів кореляції та статистики відхилень.

Таким чином, прийняття рішень у системі відбувається не детерміновано, а адаптивно-стохастично, з урахуванням історичного контексту, мінливості атакувального середовища та внутрішніх обмежень на ресурси. Це дозволяє забезпечити динамічне балансування між безпекою та ефективністю, коли рівень криптографічної складності, довжина ключів і параметри стеганографічного приховування коригуються автоматично залежно від поточних умов і прогнозованого рівня загроз.

Отже, система забезпечує динамічне балансування між рівнем безпеки та енергетично-обчислювальною ефективністю, адаптуючись до змін середовища та рівня загроз у режимі реального часу.

Криптографічно-адаптивний рівень – реалізує механізми динамічного вибору параметрів шифрування, довжини ключів k та ступеня прихованості s відповідно до функції ризику

$$R(\mathrm{t}) = \alpha P_c(t) + \beta E(t), \quad (23)$$

де $P_c(t)$ – оцінка ймовірності компрометації;

$E(t)$ – енергоспоживання системи, а коефіцієнти α;

β – визначають вагомість безпеки та енергоефективності.

Залежно від поточного значення $R(\mathrm{t})$ – система виконує автоматичне налаштування криптографічного профілю, що забезпечує компроміс між безпекою й продуктивністю.

Головна мета рівня – підтримка оптимального балансу між рівнем криптографічної стійкості та енергетичною ефективністю [10].

Основні функціональні можливості криптографічно-адаптивного рівня полягають у реалізації гнучкої та інтелектуально керованої політики захисту, спрямованої на забезпечення стійкості системи до змінного спектра загроз при збереженні обчислювальної ефективності. На цьому рівні відбувається динамічне налаштування алгоритмів шифрування (AES, ChaCha20, RSA, ECC) відповідно до поточного рівня ризику, що визначається на основі аналітичних даних про трафік, частоту аномалій та поведінкові патерни потенційних атак. Такий підхід дозволяє системі в режимі реального часу змінювати криптографічну політику – наприклад, підвищувати стійкість при фіксації зростання активності ворожих вузлів або знижувати криптографічне навантаження при відсутності загроз.

Одним із ключових механізмів є оновлення ключів за принципом “Context-Aware Key Rotation”, що передбачає автоматичну зміну криптографічних ключів залежно від контексту обчислень, часу життя сесії або рівня довіри до комунікаційного каналу [11]. Це дозволяє мінімізувати ризики компрометації ключів та підвищує ентропійну стійкість криптографічної підсистеми.

Важливою складовою також є інтеграція стеганографічного шару, який забезпечує приховування службових та аутентифікаційних метаданих у легітимному мережевому трафіку. Такий підхід ускладнює пасивний аналіз даних з боку зловмисників, оскільки сигнатури службових пакетів маскуються в інформаційному шумі [12], що істотно підвищує прихованість системи.

Для зменшення обчислювальних витрат і забезпечення роботи в умовах обмежених ресурсів застосовується апаратне прискорення криптографічних операцій за допомогою технологій ARM Crypto Extensions та Intel AES-NI [13], що дозволяє оптимізувати швидкість шифрування/дешифрування без зниження рівня безпеки.

У сукупності ці механізми формують адаптивно-криптографічне ядро системи, здатне забезпечити стійкість до атак різного рівня складності, дотримуючись при цьому принципів енергоефективності та автономності функціонування в мобільних і вбудованих середовищах.

Формалізована модель зміни криптографічної складності описує динаміку адаптації системи в часі відповідно до поточного стану загроз і ресурсних обмежень. Процес оновлення параметрів визначається рекурентним співвідношенням

$$C_{t+1} = C_t + \eta \cdot \nabla J\left(C_t\right), \tag{24}$$

де $J\left(C_t\right) = \alpha R\left(C_t\right) - \beta S\left(C_t\right)$ – цільова функція оптимізації, яка відображає баланс між витратами ресурсів $R\left(C_t\right)$ та ефективністю захисту $S\left(C_t\right)$;

η – коефіцієнт адаптації, що визначає швидкість коригування криптографічних параметрів.

Таким чином, система динамічно змінює рівень криптографічної складності залежно від оцінки поточного стану безпеки: при зростанні ризику система збільшує рівень шифрування (підвищуючи β), а при зниженні загроз – оптимізує витрати ресурсів (зменшуючи α). Такий підхід базується на принципах стохастичної оптимізації та може бути реалізований через методи градієнтного спуску або адаптивного Q-learning, що забезпечує стабільну збіжність до оптимального стану C_t^*.

Завдяки такій модульній структурі система здатна підтримувати динамічну рівновагу між безпекою та ефективністю, забезпечуючи контекстно-залежне оновлення параметрів без втрати продуктивності, що є критично важливим для вбудованих і мобільних середовищ із обмеженими обчислювальними ресурсами.

Інтеграція між рівнями системи є ключовим аспектом її функціональної узгодженості та забезпечення цілісності процесів захисту даних. Взаємодія між сенсорним, аналітико-регуляторним та криптографічно-адаптивним рівнями реалізується через уніфіковану подієву шину (Event Bus), що підтримує асинхронний обмін повідомленнями, дозволяючи системі ефективно масштабуватися та мінімізувати затримки обробки сигналів. Така архітектура сприяє декуплінгу компонентів, зменшуючи міжмодульну залежність і підвищуючи надійність системи в умовах змінного навантаження та непередбачуваних подій.

Формально процес інтеграції можна подати як композицію операторів, що відображає послідовну обробку, аналіз і криптографічну адаптацію вхідних даних:

$$Y_t = \Psi_{\text{crypto}}\left(\Theta_{\text{AI}}\left(\Phi_{\text{sensor}}\left(X_t\right)\right)\right), \tag{25}$$

де Φ_{sensor} – оператор первинної обробки, який виконує нормалізацію, фільтрацію шумів та перетворення даних у структуровану форму;

Θ_{AI} – оператор інтелектуальної аналітики, що застосовує методи глибокого навчання для виявлення аномалій та оцінювання рівня загроз;

Ψ_{crypto} – механізм динамічної криптографічної адаптації, який оптимізує параметри шифрування, ключової ротації та прихованості відповідно до поточного стану системи.

У такій моделі інформаційні потоки передаються згідно з принципами оперативного програмування, де кожна подія ініціює оновлення стану наступного рівня. Це дозволяє досягти синхронізації між математичною моделлю ризику, нейронною аналітикою та криптографічним модулем, забезпечуючи замкнений контур керування безпекою в реальному часі.

Результати цього дослідження. У результаті проведеного дослідження було розроблено цілісну концепцію побудови адаптивної системи захисту інформації для ресурсно-обмежених середовищ, що інтегрує криптографічні, стеганографічні та інтелектуальні компоненти в єдину архітектуру. Отримані результати відображають послідовне виконання трьох взаємопов'язаних етапів – аналітико-концептуального, математико-моделювального та інженерно-прикладного, кожен із яких сформував власний науково-технічний внесок у створення системи.

Загалом, отримані результати підтверджують можливість реалізації енергетично й обчислювально ефективної системи адаптивного захисту, здатної до самооптимізації в умовах змінного середовища та обмежених ресурсів [14]. Запропонована модель створює основу для подальших експериментальних досліджень, а також для інтеграції у промислові та мобільні інформаційно-комунікаційні інфраструктури.

Перспективи подальших досліджень. Подальші дослідження зосереджуватимуться на розширенні теоретико-методологічної бази адаптивних систем захисту через інтеграцію технологій штучного інтелекту, постквантової криптографії та механізмів самонавчання. Особливу увагу буде приділено розробленню квантово-резистентних криптографічних протоколів і гібридних моделей глибокого навчання, здатних динамічно прогнозувати та запобігати атакам у реальному часі. Перспективним напрямом є також використання розподілених реєстрів (блокчейн, DAG) для забезпечення довіреного обміну даними та прозорості змін параметрів безпеки.

У прикладному аспекті доцільним є дослідження енергетично оптимізованих архітектур із розподілом обчислювальних навантажень між периферійними та хмарними вузлами, а також створення цифрових двійників безпеки (Digital Twins) для моделювання поведінки систем у змінних умовах загроз. Подальший розвиток цього напряму сприятиме формуванню інтелектуально-автономних систем кіберзахисту нового покоління, здатних до самоадаптації, прогнозування та самостійної оптимізації, що забезпечить підвищення рівня довіри, стійкості та енергоефективності інформаційних інфраструктур.

СПИСОК ВИКОРМСТАНИХ ДЖЕРЕЛ

[1] J. Fridrich, and M. Goljan, "Practical Steganalysis of Digital Images – State of the Art", in *Proc. SPIE 4675, Security and Watermarking of Multimedia Contents IV*, San Jose, California, USA, 2002. doi: https://doi.org/10.1117/12.465263.

[2] J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "HiDDeN: Hiding Data With Deep Networks", in *Proc. Part XV, Computer Vision – ECCV 2018: 15th Eur. Conf.*, Munich, Germany, 2018, pp. 682-697. doi: https://doi.org/10.1007/978-3-030-01267-0_40.

[3] E. Barker, *NIST Special Publication 800-57 Part 1 Revision 5. Recommendation for Key Management: Part 1 – General*. USA: NIST, 2020. doi: https://doi.org/10.6028/NIST.SP.800-57pt1r5.

[4] ENISA Threat Landscape 2024, Sep. 2024. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf. Accessed on: May 23, 2025.

[5] І. Ромашко, та Ю. Калашнікова, "Cisco SecureX та Zero Trust: сучасні підходи до кіберзахисту", *Наука і техніка сьогодні*, № 9 (50), с. 1475-1489, 2025. doi: https://doi.org/10.52058/2786-6025-2025-9(50)-1475-1489.

[6] S. Kashkevich, A. Shyshatskyi, O. Dmytriieva, Y. Zhyvylo, G. Plekhova, and S. Neronov, "The development of management methods based on bio-inspired algorithms" in *Information and control systems: modelling and optimizations*. *Collective monograph*, A. Shyshatskyi, Ed. Kharkiv, Ukraine: Technology Center PC, 2024, pp. 35-69p. doi: http://doi.org/10.15587/978-617-8360-04-7.

[7] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) Communication Protocols: Review", in *Proc. IEEE 8th International Conference on Information Technology (ICIT),* 2017, Amman, Jordan, pp. 685-690. doi: https://doi.org/10.1109/ICITECH.2017.8079928.

[8] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami "Practical Black-Box Attacks against Machine Learning", in *Proc. Asia Conference on Computer and Communications Security (ASIA CCS '17)*, 2017, Abu Dhabi, UAE, pp. 506-519. doi: https://doi.org/10.1145/3052973.3053009.

[9] M. Koval, O. Sova, O. Orlov, A. Shyshatskyi, Y. Artabaiev, O. Shknai, A. Veretnov, O. Koshlan, Y. Zhyvylo, and I. Zhyvylo, "Improvement of complex resource management of special-purpose communication systems", *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9 (119): Information and controlling system, pp. 34-44, 2022. doi: https://doi.org/10.15587/1729-4061.2022.266009.

[10] E. Barker, *NIST Special Publication 800-175B. Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*. USA: NIST, 2016. doi: http://dx.doi.org/10.6028/NIST.SP.800-175B.

[11] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 20th Ann. ed*. USA: John Wiley & Sons, Inc., 2015.

[12] Q.A. Mahdi et al., "Development of a method of structural-parametric assessment of the object state", *Eastern-European Journal of Enterprise Technologies,* vol. 5, no. 4 (113): Mathematics and Cybernetics – applied aspects, pp. 34-44, 2021. doi: https://doi.org/10.15587/1729-4061.2021.240178.

[13] Ye. Zhyvylo, and V. Kuz, "Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences", *Theoretical and Applied Cybersecurity: scientific journal*, vol. 5, no. 2, pp. 68-80, 2023. doi: https://doi.org/10.20535/tacs.2664-29132023.2.280377.

[14] Є. Живило, та Д. Шевченко, "Оцінка ризиків кібербезпеки та контролю конфіденційності в інформаційних системах державного управління", *Зб. наук. пр. ВІ КНУ імені Тараса Шевченка*, № 75, с. 66-76, 2022. doi: https://doi.org/10.17721/2519-481X/2022/75-07.

Стаття надійшла до редакції 14.10.2025.

REFERENCES

[1] J. Fridrich, and M. Goljan, "Practical Steganalysis of Digital Images – State of the Art", in *Proc. SPIE 4675, Security and Watermarking of Multimedia Contents IV*, San Jose, California, USA, 2002. doi: https://doi.org/10.1117/12.465263.

[2] J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "HiDDeN: Hiding Data With Deep Networks", in *Proc. Part XV, Computer Vision – ECCV 2018: 15th Eur. Conf.*, Munich, Germany, 2018, pp. 682-697. doi: https://doi.org/10.1007/978-3-030-01267-0_40.

[3] E. Barker, *NIST Special Publication 800-57 Part 1 Revision 5. Recommendation for Key Management: Part 1 – General*. USA: NIST, 2020. doi: https://doi.org/10.6028/NIST.SP.800-57pt1r5.

[4] ENISA Threat Landscape 2024, Sep. 2024. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf. Accessed on: May 23, 2025.

[5] I. Romashko, and Yu. Kalashnikova, "Cisco SecureX and Zero Trust: modern approaches to cyber defense", *Science and technology today*, no. 9 (50), pp. 1475-1489, 2025. doi: https://doi.org/10.52058/2786-6025-2025-9(50)-1475-1489.

[6] S. Kashkevich, A. Shyshatskyi, O. Dmytriieva, Y. Zhyvylo, G. Plekhova, and S. Neronov, "The development of management methods based on bio-inspired algorithms" in *Information and control systems: modelling and optimizations*. *Collective monograph*, A. Shyshatskyi, Ed. Kharkiv, Ukraine: Technology Center PC, 2024, pp. 35-69p. doi: http://doi.org/10.15587/978-617-8360-04-7.

[7] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) Communication Protocols: Review", in *Proc. IEEE 8th International Conference on Information Technology (ICIT),* 2017, Amman, Jordan, pp. 685-690. doi: https://doi.org/10.1109/ICITECH.2017.8079928.

[8] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami "Practical Black-Box Attacks against Machine Learning", in *Proc. Asia Conference on Computer and Communications Security (ASIA CCS '17)*, 2017, Abu Dhabi, UAE, pp. 506-519. doi: https://doi.org/10.1145/3052973.3053009.

[9] M. Koval, O. Sova, O. Orlov, A. Shyshatskyi, Y. Artabaiev, O. Shknai, A. Veretnov, O. Koshlan, Y. Zhyvylo, and I. Zhyvylo, "Improvement of complex resource management of special-purpose communication systems", *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9 (119): Information and controlling system, pp. 34-44, 2022. doi: https://doi.org/10.15587/1729-4061.2022.266009.

[10] E. Barker, *NIST Special Publication 800-175B. Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*. USA: NIST, 2016. doi: http://dx.doi.org/10.6028/NIST.SP.800-175B.

[11] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 20th Ann. ed*. USA: John Wiley & Sons, Inc., 2015.

[12] Q.A. Mahdi et al., "Development of a method of structural-parametric assessment of the object state", *Eastern-European Journal of Enterprise Technologies,* vol. 5, no. 4 (113): Mathematics and Cybernetics – applied aspects, pp. 34-44, 2021. doi: https://doi.org/10.15587/1729-4061.2021.240178.

[13] Ye. Zhyvylo, and V. Kuz, "Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences", *Theoretical and Applied Cybersecurity: scientific journal*, vol. 5, no. 2, pp. 68-80, 2023. doi: https://doi.org/10.20535/tacs.2664-29132023.2.280377.

[14] Ye. Zhyvylo, and D. Shevchenko, “Cybersecurity Risk Assessment and Privacy Control in Government Information Systems”, *Coll. of scien. works of the Taras Shevchenko National University of Kyiv*, no. 75, pp. 66-76, 2022. doi: https://doi.org/10.17721/2519-481X/2022/75-07.

YEVHEN ZHYVYLO,
YURII KUCHMA

MATHEMATICAL MODELING OF INTELLECTUAL AND CRYPTOGRAPHIC PROTECTION OF AUTHENTICATION KEYS

The article substantiates the scientific and methodological foundations of mathematical modeling of intellectual-cryptographic systems for preventive response to authentication key compromise threats. A generalized conceptual model is proposed, integrating symmetric encryption mechanisms (in particular, the AES algorithm), steganographic methods for concealing cryptographic parameters, and intelligent attack prediction modules based on deep learning techniques. The developed mathematical framework is grounded in the synthesis of probability theory, information entropy, and adaptive optimization principles, enabling quantitative assessment of compromise risks and the formation of dynamic response strategies under variable threat conditions. Special attention is given to formalizing adaptive adjustment processes of cryptographic complexity levels and degrees of concealment, depending on the results of intelligent traffic analysis and anomaly detection in data transmission channels. Approaches to building energy- and computation-efficient implementations of such systems for embedded and mobile environments with limited resources are also examined. The obtained results establish the scientific basis for developing a new class of intellectual-cryptographic systems capable of self-learning, adaptive security parameter management, and preventive response to potential authentication data compromise threats in a dynamic information environment.

Keywords: cybersecurity, neural networks, mathematical modeling, intellectual-cryptographic system, preventive response, authentication keys, entropic analysis, adaptive optimization, deep learning.

Живило Євген Олександрович, кандидат наук з державного управління, доцент, доцент кафедри комп’ютерних та інформаційних технологій і систем навчально-наукового інституту інформаційних технологій та робототехніки, Національний університет “Полтавська політехніка імені Юрія Кондратюка”, Полтава, Україна, ORCID 0000-0003-4077-7853, zhivilka@i.ua.

Кучма Юрій Володимирович, кандидат технічних наук, доцент, завідувач кафедри комп’ютерних систем ТОВ ПВНЗ “Університет сучасних технологій”, Київ, Україна, ORCID 0009-0002-5498-4271, krabatua@gmail.com.

Zhyvylo Yevhen candidate of sciences in public administration, associate professor, associate professor of the department of computer and information technologies and systems, Educational and scientific institute of information technologies and robotics, National University “Poltava Polytechnic named after Yury Kondratyuk”, Poltava, Ukraine.

Kuchma Yurii candidate of technical sciences, associate professor, head of the department of computer systems of the Limited Liability Company Private Higher Education Institution “University of Modern Technologies”, Kyiv, Ukraine.