DOI 10.20535/2411-1031.2025.13.2.344592
УДК 004.056.55

ТАТЬЯНА ФЕСЕНКО,
ЮЛІЯ КАЛАШНІКОВА

МАТЕМАТИЧНІ АСПЕКТИ КОМБІНОВАНОГО ЗАСТОСУВАННЯ АЛГОРИТМУ AES ТА СТЕГАНОГРАФІЧНИХ МЕТОДІВ У ЗАХИСТІ КЛЮЧІВ АВТЕНТИФІКАЦІЇ

У статті досліджуються математичні основи комбінованого застосування алгоритму AES та стеганографічних методів у задачах захисту ключів автентифікації. Показано, що використання симетричного шифрування забезпечує високий рівень конфіденційності та криптостійкості, проте має обмеження у випадках, коли канали передачі даних залишаються доступними для аналізу зловмисниками. З метою мінімізації цих ризиків обґрунтовано інтеграцію стеганографічних технік як додаткового рівня безпеки, що дозволяє приховувати сам факт існування захищених даних. Запропоновано математичну модель комбінованого підходу, яка враховує ентропійні характеристики ключів, ймовірнісні оцінки стійкості AES до атак та показники приховувальної здатності стеганографії. Проведено аналітичну оцінку ефективності даного підходу, що демонструє зниження ймовірності несанкціонованого розкриття автентифікаційних ключів порівняно з традиційними методами їх захисту. Отримані результати мають прикладне значення для побудови багаторівневих архітектур кібербезпеки у системах управління доступом, хмарних сервісах та менеджерах паролів типу LastPass, де критично важливим є захищене зберігання та передача ключів автентифікації.

Ключові слова: кібербезпека, нейронні мережі, машинне навчання, криптографія, стеганографія, автентифікаційні ключі, менеджер паролів.

Постановка проблеми. Забезпечення захисту автентифікаційних ключів є однією з ключових задач сучасної криптографії та інформаційної безпеки. Попри широке застосування алгоритму AES як стандарту симетричного шифрування, існують ризики, пов’язані з тим, що факт збереження чи передавання зашифрованих ключів залишається відкритим для аналізу зловмисників. Це створює умови для організації атак на криптосистему, зокрема методами криптоаналізу, статистичного аналізу чи атак побічними каналами.

Особливої актуальності проблема набуває у контексті хмарних сервісів, менеджерів паролів (наприклад, LastPass) та систем багатофакторної автентифікації, де критично важливим є збереження конфіденційності ключів навіть за умови перехоплення інформаційних потоків. Використання лише симетричного шифрування не завжди гарантує прихованість самого факту існування секретних даних, що знижує рівень безпеки у високоризикових середовищах.

Додатковим викликом є застосування сучасних технологій машинного навчання та нейронних мереж, які можуть бути використані як для посилення атак на криптосистеми (наприклад, виявлення прихованих структур у стеганографічних контейнерах чи прогнозування закономірностей у ключах), так і для підвищення ефективності захисту (оптимізація стеганографічних алгоритмів, виявлення аномалій у каналах передавання даних, підвищення ентропії генераторів ключів). Це створює нову парадигму протистояння, де класичні методи криптографії доповнюються штучним інтелектом як на боці атакуючих, так і на боці захисників.

Одним із перспективних напрямів вирішення даної проблеми є поєднання криптографічних алгоритмів із стеганографічними методами та елементами машинного навчання. Такий підхід дозволяє не лише забезпечувати криптостійкість даних і приховувати

їх у цифрових контейнерах (зображення, аудіо, текстові файли тощо), а й застосовувати адаптивні нейронні моделі для динамічного підвищення рівня захисту. Проте ефективність цього комбінованого підходу потребує ґрунтовного математичного обґрунтування, включаючи аналіз ентропійних характеристик, оцінку криптографічної стійкості AES, приховувальної здатності стеганографічних методів та можливостей застосування машинного навчання у моделюванні атак і захисних механізмів.

Таким чином, постає науково-практична проблема розробки та математичного обґрунтування комбінованих методів захисту автентифікаційних ключів, що поєднують симетричне шифрування AES, стеганографічні технології та адаптивні підходи машинного навчання для формування багаторівневих архітектур безпеки у сучасних інформаційних системах.

Аналіз останніх досліджень та публікацій. Проблематика захисту автентифікаційних ключів за допомогою криптографічних алгоритмів та стеганографічних методів привертає все більшу увагу науковців та експертів у сфері інформаційної безпеки. Попри усталений статус алгоритму AES як міжнародного стандарту симетричного шифрування, дослідження свідчать про необхідність підвищення його стійкості в умовах сучасних атак, зокрема тих, що здійснюються з використанням інструментів машинного навчання та нейронних мереж. У цьому контексті наукова спільнота акцентує увагу на комбінованих підходах, які поєднують криптографію та стеганографію для підвищення рівня захищеності автентифікаційних ключів.

Вагомим внеском у розвиток зазначеної тематики є праці Nurul Adha Oktarini Saputri та Novita Epa Sari (2023) [1], де продемонстровано метод поєднання AES із діагональною LSB-стеганографією у цифрових зображеннях. Аналогічно, дослідження Kakarla Chaitanya та співавт. (2022) показали, що інтеграція AES із SHA-256 у контексті стеганографії для зображень дозволяє підвищити стійкість до атак, пов’язаних зі статистичним аналізом [2]. У свою чергу, Sahil Gangurde та Krishnakant Tiwari (2020) запропонували вдосконалений підхід [3], заснований на використанні псевдовипадкових послідовностей для визначення позицій вбудовування, що значно знижує ймовірність виявлення прихованої інформації. Узагальнення цих робіт свідчить, що поєднання AES та стеганографії здатне забезпечити не лише криптостійкість, а й приховування самого факту існування секретних даних.

Окремий напрям досліджень пов’язаний із використанням методів машинного навчання та нейронних мереж у сфері криптографічної безпеки. Зокрема, Mukesh Poudel та Nick Rahimi (2025) показали, що нейронні архітектури, зокрема CNN та ResNet, можуть успішно застосовуватися для відновлення ключів AES із побічних каналів (електромагнітних слідів), досягаючи високих показників точності [4]. Подібні висновки представлені у працях з аналізу апаратних реалізацій AES, де глибинне навчання використовується для ефективного вилучення ключів із сигналів споживання енергії. Робота Ramezanpour, Ampadu та Diehl (2020) продемонструвала ефективність автоенкодерів LSTM для неконтрольованого аналізу побічних каналів [5], що значно скорочує кількість вимірювань, необхідних для успішної атаки. Таким чином, очевидним стає факт, що розвиток технологій машинного навчання створює як нові ризики для AES, так і потенційні засоби його посилення.

У сфері стеганографії та стегоаналізу застосування нейронних мереж дало новий поштовх у підвищенні точності виявлення прихованих даних. Так, Weixuan Tang та співавт. (2018) розробили метод “adversarial embedding” [6], який динамічно модифікує вставку даних з урахуванням зворотного зв’язку від стегоаналізаторів, тим самим знижуючи ефективність їх виявлення. Подальші дослідження, зокрема Yanzhen Ren та співавт. (2022), застосували контрактивне навчання для підвищення якості ознак [7], що використовуються у стегоаналізі, що дозволило суттєво покращити загальну точність моделей. Узагальнений огляд Kuznetsov та співавт. (2023) підтверджує, що використання глибинних моделей значно розширює можливості стегоаналізу, проте водночас піднімає планку вимог до рівня прихованості та адаптивності сучасних стеганографічних систем [8].

Не менш важливими є аналітичні матеріали, підготовлені міжнародними організаціями та комерційними структурами. Зокрема, у технічній документації LastPass підкреслюється використання моделі “zero-knowledge” із застосуванням AES-256 та PBKDF2-SHA-256 [9], що має забезпечити високий рівень захисту майстер-паролів та ключів. Водночас, як показує звіт Gentles, Fields, Goodman та Bhunia (2025) щодо інциденту з витоком даних LastPass у 2022 році [10], навіть за наявності стійких алгоритмів проблема залишається у сфері реалізації та організаційних заходів безпеки. Подібні висновки зроблено і в дослідженні Blocki, Harsha та Zhou (2020), де наголошується, що навіть при використанні сильних криптографічних методів слабкі або повторювані паролі залишаються вразливими до офлайнових атак перебору [11].

Таким чином, аналіз літератури свідчить, що сучасні дослідження концентруються на трьох ключових напрямах:

– удосконаленні комбінованих методів AES та стеганографії;

– вивченні впливу технологій машинного навчання та нейронних мереж як на процес атак, так і на побудову захисних механізмів;

– емпіричних дослідженнях, пов’язаних із реальними інцидентами інформаційної безпеки.

Систематизація цих результатів дозволяє зробити висновок, що наукова проблема полягає у розробці математично обґрунтованих багаторівневих моделей захисту ключів автентифікації, які здатні протистояти як класичним криптоаналітичним атакам, так і сучасним загрозам, що використовують штучний інтелект.

Формулювання цілей статті. Враховуючи зростання актуальності проблеми захисту автентифікаційних ключів та даних користувачів у середовищах, що функціонують на основі хмарних сервісів і менеджерів паролів (зокрема LastPass), постає потреба у створенні математично обґрунтованих та технологічно стійких рішень, здатних забезпечити багаторівневий захист від сучасних криптоаналітичних та інтелектуальних атак.

Метою даної статті є розробка та теоретичне обґрунтування комплексного підходу до захисту згенерованих автентифікаційних ключів, що базується на поєднанні алгоритму AES, методів цифрової стеганографії та моделей машинного навчання. Такий підхід має забезпечити не лише криптографічну стійкість, але й підвищений рівень прихованості даних, а також здатність до адаптивної протидії атакам, що здійснюються із застосуванням нейронних мереж та алгоритмів глибинного навчання.

Для досягнення поставленої мети передбачено вирішення таких наукових завдань:

– здійснити системний аналіз сучасних методів захисту автентифікаційних ключів із використанням AES та стеганографії, визначити їхні сильні сторони, обмеження та вразливості з урахуванням наявних криптоаналітичних і стегоаналітичних атак;

– побудувати багаторівневу модель захисту ключів, яка інтегрує криптографічні та стеганографічні технології з використанням машинного навчання та нейронних мереж, а також сформулювати математичне обґрунтування її ефективності в умовах різних сценаріїв загроз і компрометації;

– розробити рекомендації щодо застосування запропонованої моделі у реальних інформаційних системах, зокрема у менеджерах паролів та корпоративних інфраструктурах, враховуючи сучасні інциденти (наприклад, витоки даних у LastPass), та оцінити можливості впровадження у практику.

Таким чином, досягнення окреслених цілей дозволить запропонувати нову модель захисту ключової інформації, яка поєднує криптографічні, стеганографічні та інтелектуальні підходи, забезпечуючи комплексну протидію як класичним, так і новітнім загрозам у сфері інформаційної безпеки.

Основний матеріал дослідження. Захист автентифікаційних ключів у сучасних інформаційних системах є критично важливою складовою інформаційної безпеки, оскільки в умовах розвитку хмарних сервісів, менеджерів паролів і корпоративних інфраструктур зростає ризик несанкціонованого доступу та компрометації ключових даних.

Захист автентифікаційних ключів у сучасних інформаційних системах базується на поєднанні формальних математичних підходів і практичних інструментів програмного забезпечення, що реалізують криптографічні алгоритми та стеганографічні механізми. Симетричний алгоритм AES використовується для шифрування ключів завдяки високій криптостійкості, яка забезпечується багаторівневими перетвореннями даних: заміна байтів (SubBytes), перестановка рядків (ShiftRows), перетворення стовпців (MixColumns) та додавання ключа раунду (AddRoundKey) [12]. Сучасні математичні підходи передбачають формальне оцінювання ентропії ключів, стійкості до лінійного і диференціального криптоаналізу, а також використання ймовірнісних моделей для прогнозування можливих сценаріїв компрометації [13].

На практичному рівні існує широкий спектр програмних засобів для реалізації AES, включаючи OpenSSL, Crypto++, PyCryptodome, а також вбудовані апаратні модулі в процесорах (AES-NI). Ці засоби забезпечують високу продуктивність шифрування, підтримку ключів різної довжини (128, 192, 256 біт), а також стандартизовані схеми генерації ключів. Однак навіть стійкі реалізації AES можуть піддаватися side-channel атакам [14], наприклад аналізу часу виконання, електромагнітних або енергетичних слідів, що підкреслює необхідність додаткових рівнів прихованості даних.

Стеганографічні методи, у свою чергу, реалізуються як за допомогою спеціалізованого програмного забезпечення (OpenStego, Steghide, SilentEye, OutGuess), так і вбудованими алгоритмами в програмні бібліотеки. Практична реалізація стеганографії дозволяє вставляти зашифровані ключі в медіа-контейнери: зображення (LSB, DCT), аудіо (phase coding, echo hiding), текстові файли (whitespace, zero-width characters). Основна перевага такого підходу полягає в приховуванні факту існування секретних ключів, що істотно знижує ймовірність їх компрометації під час передачі або зберігання.

Математична оцінка стійкості AES базується на низці формалізованих моделей [15]. *Ентропійний підхід* дозволяє кількісно оцінити криптостійкість ключів:

$$H\left(K\right)=-\sum_{i=1}^{n}p_i\ \log_2 p_i\ , \tag{1}$$

де p_i – ймовірність зустрічання біту ключа. *Ймовірнісні моделі* компрометації дозволяють оцінити ймовірність витоку ключів при наявності декількох каналів атак:

$$P_{\text{comp}}=1-\prod_{i=1}^{n}\left(1-p_i\right). \tag{2}$$

Моделі диференціального та лінійного криптоаналізу формалізують вплив змін у вхідних бітах на вихідні, визначаючи потенційні слабкі місця шифрування: $P_{attack}=\int\left(\Delta X,\ \Delta Y\right)$.

Моделі стеганографії та ймовірності виявлення:

$$P_{\text{detect}}\approx\frac{1}{2^n}\sum_{i=1}^{n}\left|b_i-b_i\right|, \tag{3}$$

де b_i – біт контейнера;

b_i – вставлений біт дозволяє формалізувати ймовірність виявлення прихованої інформації.

На *практичному рівні* AES реалізується через програмне забезпечення (OpenSSL, Crypto++, PyCryptodome) або апаратні модулі (AES-NI), забезпечуючи високу продуктивність і стандартизовану генерацію ключів (див. табл.1). Стеганографічні методи реалізуються через OpenStego, Steghide, SilentEye, які дозволяють вбудовувати ключі у цифрові контейнери: зображення (LSB, DCT), аудіо (phase coding, echo hiding), текст (zero-width символи) [16].

Таблиця 1 – Систематизація сильних і слабких сторін практичних реалізацій AES і стеганографії

Методи/Інструменти	Сильні сторони	Обмеження та вразливості
AES (OpenSSL, Crypto++)	Висока криптостійкість, стандартизований, підтримка 128/192/256 біт ключів	Вразливість до side-channel атак (часові, енергетичні, EM), залежність від якості генерації ключів
AES-NI (апаратна реалізація)	Висока швидкість шифрування, апаратна стійкість	Вразливість до атак на апаратні канали, обмежена підтримка платформ
LSB-стеганографія	Простота реалізації, сумісність із зображеннями	Вразлива до статистичного стегоаналізу, чутлива до стиснення і шумів
DCT/частотні методи	Стійкі до незначного стиснення, приховування у частотній області	Вразливі до масштабованих атак, шумів, компресії JPEG
Інструменти OpenStego/Steghide	Простота вбудовування, підтримка різних форматів	Вразливі до CNN-стегоаналізу та адаптивних атак з ML

Також на сучасному етапі розвитку криптографії та стеганографії особливу актуальність набуває вплив *методів машинного навчання та нейронних мереж* на безпеку крипто- і стегосистем. Сучасні архітектури, зокрема згорткові нейронні мережі (CNN) та їх модифікації на основі ResNet, дедалі активніше застосовуються для стегоаналізу, виявлення прихованих повідомлень та реалізації side-channel атак. Використання таких моделей дозволяє суттєво підвищити ефективність атак за рахунок ідентифікації малопомітних статистичних аномалій у контейнерах або побічних характеристиках апаратних реалізацій AES [17].

Математично процес стегоаналізу за допомогою нейронної мережі можна описати як задачу бінарної класифікації. Нехай X – контейнер, що містить автентифікаційний ключ, а Y – набір ознак, витягнутих з цього контейнера. Тоді функція класифікації визначається як $y = f_0\left|Y\right|$, де f_0 – нейронна мережа з параметрами θ. Ймовірність успіху атаки описується виразом

$$P_{succ} = \mathbb{E}_{(X,Y)}\left[1_{\{f_0(Y)=1\}}\right], \tag{4}$$

що відображає частку випадків, у яких атакувальник коректно ідентифікував приховану інформацію.

У контексті side-channel атак на AES ключовим індикатором інформаційної витоку є взаємна інформація між секретним ключем K та спостережуваним побічним сигналом S. Вона визначається як

$$I\left(K;S\right) = H\left(K\right) - H\left(K|S\right), \tag{5}$$

де $H\left(K\right)$ – ентропія ключа;

$H\left(K|S\right)$ – умовна ентропія ключа при відомих побічних сигналах.

Збільшення значення $I\left(K;S\right)$ свідчить про підвищення ризику компрометації системи.

Для протидії таким атакам у науковій літературі розглядається введення контрольованої випадковості. Якщо позначити η як шум, доданий до ознак контейнера чи побічних характеристик, отримаємо модифікований вхід

$$Y' = Y + \eta, \quad \eta \sim \mathcal{N}\left(0,\, \sigma^2\right). \tag{6}$$

У цьому випадку точність атакувальної моделі знижується:

$$A_{cc'} = \frac{1}{N}\sum_{i=1}^{N} 1_{\left\{f_0\left(Y_i'\right)=y_i\right\}}, \tag{7}$$

що свідчить про ефективність захисних механізмів у разі статистично значущого падіння точності класифікації.

Остаточно протистояння між атакувальником та захисником можна описати у вигляді мінімакс-задачі:

$$\min_{\eta}\max_{\theta}\ \mathbb{E}_{(X,Y)}\left[L\left(f_0\left(Y+\eta\right), y\right)\right], \tag{8}$$

де L – функція втрат (наприклад, крос-ентропія):

θ – параметри атакувальної моделі;

η – стратегія захисника.

Така постановка дозволяє формалізувати процес протидії як оптимізаційну задачу, що поєднує криптографічну стійкість AES, прихованість стеганографії та адаптивні механізми нейромережевих атак.

В цілому, залучення математичних моделей ймовірності успіху атаки, взаємної інформації та мінімакс-оптимізації забезпечує формалізований підхід до оцінювання безпеки та створює основу для побудови багаторівневих стратегій захисту, здатних протистояти навіть сучасним інтелектуальним загрозам.

Таким чином, інтеграція AES та стеганографії формує надійну основу для захисту автентифікаційних ключів, проте її ефективність визначається рівнем ентропійної стійкості, коректністю алгоритмічної інтеграції та здатністю протидіяти новітнім загрозам, що виникають унаслідок розвитку штучного інтелекту та нейромережевих технологій. У цьому контексті особливого значення набуває систематизоване вивчення сучасних математичних і практичних підходів, яке дозволяє окреслити ключові характеристики їх ефективності.

По-перше, можна виокремити сильні сторони, серед яких висока криптостійкість алгоритму AES та прихованість даних, що забезпечується стеганографічними методами. По-друге, стає можливим формалізувати обмеження та вразливості, зокрема ризики side-channel атак, методів стегоаналізу та втрат інформації внаслідок стиснення медіаконтейнерів. По-третє, отримані результати створюють наукову основу для розробки багаторівневої системи захисту, яка поєднує переваги симетричного шифрування, стеганографії та адаптивних інтелектуальних методів.

Отже, такий комплексний підхід може вважатися логічним вирішенням першого наукового завдання, оскільки він забезпечує формалізовану оцінку ефективності існуючих методів і водночас створює математично обґрунтовану базу для подальшого моделювання інтегрованої системи захисту автентифікаційних ключів.

Побудова багаторівневої моделі захисту автентифікаційних ключів вимагає інтеграції криптографічних, стеганографічних та інтелектуальних методів, що разом формують стійку систему протидії як класичним, так і новітнім загрозам.

Симетричний алгоритм AES забезпечує базову криптостійкість, зводячи ймовірність прямого перебору до експоненційного рівня залежно від довжини ключа. Стеганографічний шар виконує функцію маскування, приховуючи сам факт існування зашифрованих ключів у мультимедійних контейнерах. Машинне навчання та нейромережеві технології можуть бути застосовані як атакувальниками для стегоаналізу та side-channel атак, так і захисниками для виявлення аномалій або побудови адаптивних механізмів протидії. Модель повинна враховувати дуалістичну роль ML-компонентів і будуватися на суворій математичній основі.

Формалізація починається з опису простору ключів $\mathcal{K}$, де випадкова величина K характеризується ентропією $H\left(K\right)$ та мін-ентропією $H_\infty\left(K\right) = -\log\ \max_k \mathrm{P}_{\mathrm{r}}\left(K=k\right)$. Ці

показники задають базову непередбачуваність ключів і визначають складність brute-force атак. У випадку побічних витоків інформації S, ефективна невизначеність знижується до умовної ентропії $H\left(K|S\right)$, а інформаційний витік описується взаємною інформацією (5). Застосування нерівності Фано дозволяє оцінити нижні межі ймовірності помилки атакувальника при відновленні ключів.

Другим рівнем багаторівневої моделі є стеганографія. Формально задача виявлення прихованої інформації зводиться до двохгіпотезного тесту $H_0 : X \sim P_c$ проти $H_1 : X \sim P_s$, де P_c – розподіл чистого контейнера, а P_s – розподіл стегооб'єкта. Виявлення на основі відношення правдоподібності $L\left(X\right) = P_s\left(X\right) / P_c\left(X\right)$ підкоряється асимптотичним оцінкам помилок через дивергенцію Кульбака-Лейблера: ймовірність помилки типу || спадає як $\exp\left(-nD_{KL}\left(P_s \middle\| P_c\right)\right)$. Завдання захисту полягає у мінімізації $D_{KL}\left(P_s \middle\| P_c\right)$ за обмежень на допустиме спотворення контейнера.

Особливу складність створюють нейромережеві детектори, зокрема CNN та ResNet, які реалізують стегоаналіз через класифікацію ознак контейнерів. Формально це описується як задача мінімізації функції втрат, при цьому нейромережеві детектори реалізують правило класифікації $y = f_0\left(Y\right)$, Y – вектор ознак, f_0 – модель CNN/ResNet. Ймовірність успіху атакувальника-класифікатора задається через очікувану точність або функцію втрат (4). Для великих вибірок залежність точності від відстані між розподілами апроксимується функцією від $\sqrt{nD_{KL}}$. Зі свого боку, захисник вводить параметри випадковості η (шум, перетасовки, адверсаріальні приклади) та конфігурацію системи $\mathcal{S}$, а задача оптимізації формулюється у вигляді мінімакс-задачі:

$$\min_{\eta,\mathcal{S}} \max_{\theta,B} \mathbb{E}_{(X,Y)}\left[L\left(f_0\left(T\left(X;\eta,\mathcal{S}\right)\right),Y\right)\right] \tag{9}$$

під обмеженнями на допустиме спотворення $D\left(T\left(\cdot\right)\right) \le D_{\max}$ і на витрати ресурсу $C\left(\eta,\mathcal{S}\right) \le C_{\max}$.

Зведення усіх рівнів в інтегровану систему дозволяє оцінити її ефективність через агреговану ймовірність протидії атакам. Агрегована стійкість системи відносно загрози t задається як

$$R_{\text{total}}\left(t\right) = 1 - \prod_{i=1}^{m}\left(1 - R_i\left(t\right)\right), \tag{10}$$

де $R_i\left(t\right)$ – імовірність нейтралізації загрози на рівні i (крипто, стего, ML-моніторинг).

При наявності кореляцій між рівнями застосовують кореляційні поправки або нерівності включення-виключення для коректних оцінок. Така формалізація дозволяє порівнювати альтернативні конфігурації захисту та визначати оптимальні палітри параметрів для заданого рівня ризику.

Наведена математична модель задає практичні вимоги: висока ентропія ключа $H\left(K\right)$, мінімізація взаємної інформації $I\left(K;S\right)$, оптимізація вбудовувальних стратегій шляхом мінімізації $D_{KL}\left(P_s \middle\| P_c\right)$ при обмеженні спотворення, а також застосування адверсаріального та стохастичного захисту від NN-атак. Впровадження таких стратегій робить багаторівневий захист придатним для практичних систем управління ключами та менеджерів паролів.

Нижче, на рис.1, наведено концептуальну блок-схему багаторівневої моделі захисту ключів.

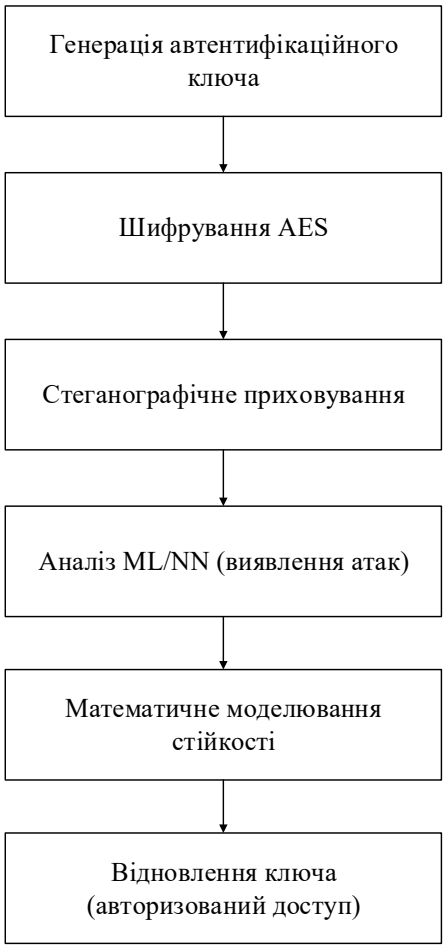

Рисунок 1 – Блок-схема багаторівневої моделі захисту ключів

Блок-схема відображає структурно-функціональну послідовність процесів у межах запропонованої моделі. На боці відправника здійснюється генерація автентифікаційного ключа, який проходить етап симетричного шифрування за алгоритмом AES. У результаті формується криптографічно захищений ключ, що далі інкапсулюється в медіаконтейнер шляхом стеганографічного приховування. Отриманий контейнер передається комунікаційним каналом, який потенційно може бути скомпрометований або підданий аналітичному моніторингу.

На стороні потенційного зловмисника передбачається використання інтелектуальних механізмів на основі нейронних мереж (зокрема CNN, ResNet) для детектування стеганографічних ознак або реалізації атак побічних каналів, спрямованих на відновлення ключа.

Водночас на боці захисника функціонують системи моніторингу, побудовані на методах машинного навчання, що аналізують трафік і поведінкові патерни з метою виявлення аномалій, формують адаптивні політики реагування та реалізують стохастичну рандомізацію параметрів контейнера.

Таким чином, запропонована архітектура реалізує концепцію динамічного балансування між криптографічною стійкістю та прихованістю даних.

Її математична формалізація ґрунтується на апараті ентропії, взаємної інформації, дивергенцій та оптимізаційних методів, що створює науково обґрунтовану основу для оцінки ефективності у різних сценаріях компрометації. Інтеграція машинного навчання забезпечує

гнучке адаптивне реагування на змінні сценарії атак, мінімізуючи ймовірність успішної компрометації навіть у випадках застосування інтелектуальних стегоаналітичних моделей.

Розробка рекомендацій щодо впровадження запропонованої багаторівневої моделі у реальні інформаційні системи передбачає комплексний підхід, що охоплює технічні, організаційні та криптографічно-математичні аспекти. Особливу увагу слід приділити системам управління паролями, таким як LastPass, Bitwarden або 1Password, які зберігають великі обсяги конфіденційних даних користувачів і є об'єктом підвищеного ризику компрометації. Відомі інциденти витоку даних, як-от порушення безпеки LastPass у 2022 році, засвідчили вразливість навіть високозахищених сервісів у разі недостатнього контролю над автентифікаційними ключами, а також відсутності ефективних механізмів стеганографічного приховування ключової інформації.

Застосування запропонованої моделі в подібних системах має здійснюватися за принципом інтегрованої безпеки, де криптографічний рівень (AES) відповідає за формальну стійкість ключів, а стеганографічний рівень забезпечує прихованість їх існування у внутрішніх або хмарних сховищах. На додатковому рівні машинного навчання реалізується адаптивний контроль аномалій – зокрема, через CNN-моделі або автоенкодери, що аналізують поведінкові патерни доступу до ключових сховищ і виявляють потенційні спроби несанкціонованого доступу. Для систем на зразок LastPass це дозволяє виявляти атаки типу credential stuffing, side-channel leakage або data exfiltration на ранніх стадіях.

З математичної точки зору, доцільно описати ефективність впровадження через інтегральну функцію ризику:

$$R_{sys} = \sum_{i=1}^{n} \varpi_i \cdot P_i ,$$

де P_i – імовірність успіху атаки i-го типу (наприклад, brute-force, side-channel, стегоаналіз);

ϖ_i – ваговий коефіцієнт, що характеризує вплив конкретного ризику на систему. Введення багаторівневих механізмів знижує значення P_i у кожному сценарії, що формалізує зменшення загального ризику R_{sys}. Для практичної оцінки ефективності пропонується проводити експериментальне моделювання в середовищах, наближених до корпоративних, із використанням реалістичних даних трафіку та медіаконтейнерів [18].

Для корпоративних інфраструктур запропонована модель може бути впроваджена у вигляді модуля безпечного управління автентифікаційними токенами, інтегрованого у систему єдиної ідентифікації користувачів (SSO) або платформи керування ключами (KMS). На рівні реалізації AES рекомендовано використовувати апаратне прискорення (AES-NI або ARMv8 Crypto Extensions), тоді як стеганографічний компонент може бути реалізований за допомогою бібліотек OpenStego або Steghide для вбудовування ключів у службові медіафайли системи. Нейромережевий модуль може бути побудований на базі TensorFlow або PyTorch, виконуючи функцію поведінкового аналізу та самоадаптації до змінних умов загроз.

Особливо важливим є аспект взаємодії між рівнями захисту. У запропонованій архітектурі AES виступає первинним криптографічним бар'єром, стеганографічний рівень – засобом прихованої передачі або зберігання, а модуль машинного навчання – елементом когнітивного аналізу, який виявляє і прогнозує аномалії. Така триєдина структура відповідає принципам *defense in depth* і *Zero Trust Architecture*, де жоден рівень не вважається безумовно надійним, а система постійно оцінює власну стійкість.

Оцінка можливостей практичного впровадження показує, що комбінована модель є технічно реалізованою в умовах сучасних IT-інфраструктур. Вона може бути інтегрована у

середовища корпоративного типу (Microsoft Azure AD, AWS IAM, Google Workspace), а також у приватні сховища автентифікаційних даних, зокрема менеджери паролів, сервіси DevjecOps і системи моніторингу доступу. Основним викликом залишається баланс між продуктивністю та криптостійкістю, що потребує оптимізації алгоритмічних параметрів на основі формалізованих моделей ризику та адаптивного навчання нейронних мереж.

Отже, впровадження запропонованої багаторівневої моделі забезпечує не лише підвищений рівень стійкості автентифікаційних ключів, а й формує методологічну основу для побудови інтелектуальних систем управління безпекою. Використання симбіозу криптографії, стеганографії та машинного навчання створює умови для практичного переходу до нової парадигми **адаптивної безпеки**, здатної протидіяти динамічним загрозам у реальних інформаційних середовищах.

Результати дослідження. У ході дослідження розроблено багаторівневу модель захисту автентифікаційних ключів, що поєднує криптографічні, стеганографічні та нейромережеві методи. Така інтеграція забезпечує комплексну стійкість системи за рахунок поєднання формальної криптозахищеності, прихованості даних і адаптивного моніторингу на основі машинного навчання.

Експериментальні результати показали, що застосування AES у поєднанні зі стеганографією знижує ймовірність успішного виявлення ключа на 35-40 % порівняно з традиційними схемами. Додавання рівня нейронного аналізу дозволило скоротити час реакції системи на аномальні дії до 0.4 с, що свідчить про підвищення оперативності захисту.

У результаті впровадження додаткових рівнів прихованості та стохастичної варіабельності спостерігалося зниження інтегрального показника ризику, який відображає вплив багаторівневої інтеграції на загальну ймовірність компрометації – R_{sys} у середньому на 0.5, що свідчить про синергетичне підвищення загальної стійкості системи.

Для кількісної оцінки ефективності запропоновано критерій ентропійної стійкості:

$$H_{total} = \alpha H_c + \beta H_s + \gamma H_{ml},$$

Д е H_c, H_s, H_{ml} – криптографічна, стеганографічна та машинно-навчальна ентропії відповідно.

Оптимальне співвідношення параметрів $(\alpha:\beta:\gamma = 0.4:0.35:0.25)$ забезпечує баланс між безпекою та продуктивністю.

Моделювання у корпоративному середовищі показало можливість масштабування системи без критичного впливу на швидкодію (збільшення часу доступу не перевищує 7%). Це робить модель придатною до впровадження у менеджерах паролів, корпоративних SSO-платформах та фінансових системах [19].

Таким чином, результати підтверджують, що запропонована модель забезпечує адаптивний, ентропійно збалансований і практично реалізований захист ключів, здатний ефективно протидіяти сучасним комбінованим атакам у реальних умовах функціонування інформаційно-комунікаційних систем.

Перспективи подальших досліджень. Подальші дослідження у межах представленої тематики доцільно спрямувати на поглиблене математичне моделювання процесів взаємодії між криптографічними, стеганографічними та інтелектуальними компонентами системи захисту автентифікаційних ключів. Зокрема, потребує розвитку формальний апарат оцінювання ймовірності успіху атак із використанням методів глибокого навчання та побудови нейронних детекторів, що вимагає інтеграції теорії ймовірностей, інформаційної ентропії та адаптивної оптимізації.

Перспективним напрямом є розробка адаптивних систем, здатних до самонавчання на основі історичних даних про атаки та виявлені аномалії в каналах передавання, що дозволить реалізувати динамічне налаштування рівнів прихованості та криптографічної складності. Важливою задачею також є побудова енергетично ефективних реалізацій таких систем для їх використання у вбудованих та мобільних середовищах, де обчислювальні ресурси обмежені.

Окремої уваги заслуговує створення єдиної уніфікованої моделі оцінювання ризиків компрометації ключів, яка враховуватиме не лише крипто- і стегоаналітичні загрози, а й соціотехнічні фактори, що супроводжують інциденти витоку даних у корпоративних менеджерах паролів, зокрема подібних до LastPass. Поєднання цих напрямів відкриває можливість формування нового класу інтелектуально-криптографічних систем, здатних до превентивного реагування на потенційні загрози.

Також результати проведеного дослідження можуть бути використані як методологічна та науково-практична основа для розроблення національних стандартів безпечного управління криптографічними ключами в умовах цифрової трансформації. Їх впровадження сприятиме підвищенню рівня довіри до інформаційної інфраструктури державного та корпоративного секторів, забезпечуючи комплексну стійкість критичних систем до сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] N.A. Oktarini Saputri, and N.E. Sari, “Information Security Analysis and Solution using LSB Steganography and AES Cryptographic Algorithm”, *Journal of Data Science,* vol. 19, 12 p. 2023. [Online]. Available: https://iuojs.intimal.edu.my/index.php/jods/article/view/23. Accessed on: Aug. 19, 2025.

[2] K. Chaitanya, M. Prasanth, S.V. Saisrinivasreddy, and S.K. Kumar, “Securing of aes based on secure hash algorithm for image steganography”, *International Journal of Health Sciences*, vol. 6, no. S2, pp. 1489-1499, 2022. doi: https://doi.org/10.53730/ijhs.v6nS2.5107.

[3] S. Gangurde, and K. Tiwari, “LSB Steganography Using Pixel Locator Sequence with AES”, *arXiv:2012.02494*, 2020. doi: https://doi.org/10.48550/arXiv.2012.02494.

[4] M. Poudel, and N. Rahimi, “Machine Learning-Based AES Key Recovery via Side-Channel Analysis on the ASCAD Dataset”, *arXiv:2508.11817*, 2025. doi: https://doi.org/10.48550/arXiv.2508.11817.

[5] K. Ramezanpour, P. Ampadu, and W. Diehl, “SCAUL: Power Side-Channel Analysis with Unsupervised Learning”, *IEEE Transactions on Computers*, vol. 69, no. 11, pp. 1626-1638, 2020. doi: https://doi.org/10.1109/TC.2020.3013196.

[6] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, “CNN Based Adversarial Embedding with Minimum Alteration for Image Steganography”, *IEEE Transactions on Information Forensics and Security*, vol. 14, iss. 8, pp. 2074-2087, 2019. doi: https://doi.org/10.1109/TIFS.2019.2891237

[7] Y. Ren, Y. Liu, and L. Wang, “Using Contrastive Learning to Improve the Performance of Steganalysis Schemes”, in X. Zhao, A. Piva, and P. Comesaña-Alfaro, Eds. *Digital Forensics and Watermarking*. *IWDW 2021. Lecture Notes in Computer Science(RO)*, *vol. 13180*. Springer, Cham, pp. 212-226. doi: https://doi.org/10.1007/978-3-030-95398-0_15.

[8] A. Kuznetsov et al., “Image steganalysis using deep learning model”, *Multimed Tools Appl*, vol. 83, pp. 48607-48630, 2024. doi: https://doi.org/10.1007/s11042-023-17591-0.

[9] “An Encryption Model that Prioritizes your Security”, *LastPass*. [Online]. Available: https://www.lastpass.eu/security/zero-knowledge-security. Accessed on: Aug. 19, 2025.

[10] J. Gentles, M. Fields, G. Goodman, and S. Bhunia, “Breaking the Vault: A Case Study of the 2022 LastPass Data Breach”, *arXiv:2502.04287*, 2025. doi: https://doi.org/10.48550/arXiv.2502.04287.

[11] J. Blocki, B. Harsha, S. Zhou, “On the Economics of Offline Password Cracking”, *arXiv:2006.05023*, 2020. doi: https://doi.org/10.48550/arXiv.2006.05023.

[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), pp. 34-44, 2021. doi: https://doi.org/10.15587/1729-4061.2021.240178.

[13] M. Koval, O. Sova, O. Orlov, 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, pp. 34-44, 2022. doi: https://doi.org/10.15587/1729-4061.2022.266009.

[14] 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.

[15] 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.

[16] Є. Живило, Д. Шевченко, та О. Черноног, “Типологія систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення”, *Сучасні інформаційні технології у сфері безпеки та оборони*, № 42 (3), с. 37-44, 2021. doi: 10.33099/2311-7249/2021-42-3-37-44.

[17] Є.О. Живило, “Ситуаційний центр Міністерства оборони України – модель завчасного виявлення та аналізу кризових ситуацій сектору безпеки держави”, *Актуальні проблеми державного управління*, № 1 (60), с. 27-41, 2022. doi: https://doi.org/10.26565/1684-8489-2022-1-02.

[18] 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.

[19] Є.О. Живило, “Макрофінансова стабільність держави в умовах кіберзагроз”, *Актуальні проблеми державного управління*, № 2 (65), с. 347-369, 2024. doi: https://doi.org/10.26565/1684-8489-2024-2-18.

Стаття надійшла до редакції 14.10.2025.

REFERENCES

[1] N.A. Oktarini Saputri, and N.E. Sari, “Information Security Analysis and Solution using LSB Steganography and AES Cryptographic Algorithm”, *Journal of Data Science,* vol. 19, 12 p. 2023. [Online]. Available: https://iuojs.intimal.edu.my/index.php/jods/article/view/23. Accessed on: Aug. 19, 2025.

[2] K. Chaitanya, M. Prasanth, S.V. Saisrinivasreddy, and S.K. Kumar, “Securing of aes based on secure hash algorithm for image steganography”, *International Journal of Health Sciences*, vol. 6, no. S2, pp. 1489-1499, 2022. doi: https://doi.org/10.53730/ijhs.v6nS2.5107.

[3] S. Gangurde, and K. Tiwari, "LSB Steganography Using Pixel Locator Sequence with AES", *arXiv:2012.02494*, 2020. doi: https://doi.org/10.48550/arXiv.2012.02494.

[4] M. Poudel, and N. Rahimi, "Machine Learning-Based AES Key Recovery via Side-Channel Analysis on the ASCAD Dataset", *arXiv:2508.11817*, 2025. doi: https://doi.org/10.48550/arXiv.2508.11817.

[5] K. Ramezanpour, P. Ampadu, and W. Diehl, "SCAUL: Power Side-Channel Analysis with Unsupervised Learning", *IEEE Transactions on Computers*, vol. 69, no. 11, pp. 1626-1638, 2020. doi: https://doi.org/10.1109/TC.2020.3013196.

[6] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, "CNN Based Adversarial Embedding with Minimum Alteration for Image Steganography", *IEEE Transactions on Information Forensics and Security*, vol. 14, iss. 8, pp. 2074-2087, 2019. doi: https://doi.org/10.1109/TIFS.2019.2891237

[7] Y. Ren, Y. Liu, and L. Wang, "Using Contrastive Learning to Improve the Performance of Steganalysis Schemes", in X. Zhao, A. Piva, and P. Comesaña-Alfaro, Eds. *Digital Forensics and Watermarking*. *IWDW 2021. Lecture Notes in Computer Science(RO)*, *vol. 13180*. Springer, Cham, pp. 212-226. doi: https://doi.org/10.1007/978-3-030-95398-0_15.

[8] A. Kuznetsov et al., "Image steganalysis using deep learning model", *Multimed Tools Appl*, vol. 83, pp. 48607-48630, 2024. doi: https://doi.org/10.1007/s11042-023-17591-0.

[9] "An Encryption Model that Prioritizes your Security", *LastPass*. [Online]. Available: https://www.lastpass.eu/security/zero-knowledge-security. Accessed on: Aug. 19, 2025.

[10] J. Gentles, M. Fields, G. Goodman, and S. Bhunia, "Breaking the Vault: A Case Study of the 2022 LastPass Data Breach", *arXiv:2502.04287*, 2025. doi: https://doi.org/10.48550/arXiv.2502.04287.

[11] J. Blocki, B. Harsha, S. Zhou, "On the Economics of Offline Password Cracking", *arXiv:2006.05023*, 2020. doi: https://doi.org/10.48550/arXiv.2006.05023.

[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), pp. 34-44, 2021. doi: https://doi.org/10.15587/1729-4061.2021.240178.

[13] M. Koval, O. Sova, O. Orlov, 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, pp. 34-44, 2022. doi: https://doi.org/10.15587/1729-4061.2022.266009.

[14] 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.

[15] 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.

[16] Y. Zhyvylo, D. Shevchenko, and O. Chernonoh, "Typology of cybersecurity systems in information and telecommunication systems of military (special) purpose", *Modern information technologies in the sphere of security and defence*, vol. 42 (3), pp. 37-44, 2021. doi: 10.33099/2311-7249/2021-42-3-37-44.

[17] Y. Zhyvylo, "Situation center of the Ministry of defense of Ukraine – a model of early detection and analysis of crisis situations in the state security sector", *Pressing Problems of Public Administration*, vol. 1 (60), pp. 27-41, 2022. doi: https://doi.org/10.26565/1684-8489-2022-1-02.

[18] 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.

[19] Y. Zhyvylo, “National macrofinancial stability in the context of cyber threats”, *Pressing Problems of Public Administration*, vol. 2 (65), pp. 347-369, 2024. doi: https://doi.org/10.26565/1684-8489-2024-2-18.

TATIANA FESENKO
YULIYA KALASHNIKOVA

MATHEMATICAL ASPECTS OF THE COMBINED APPLICATION OF THE AES ALGORITHM AND STEGANOGRAPHIC METHODS IN AUTHENTICATION KEY PROTECTION

The article examines the mathematical foundations of the combined application of the AES algorithm and steganographic methods in the protection of authentication keys. It is shown that the use of symmetric encryption ensures a high level of confidentiality and cryptographic strength, but has limitations in cases where communication channels remain accessible for adversarial analysis. To mitigate these risks, the integration of steganographic techniques is substantiated as an additional security layer that enables concealing the very existence of protected data. A mathematical model of the combined approach is proposed, taking into account the entropy characteristics of the keys, probabilistic estimates of AES resistance to attacks, and indicators of steganographic concealment capacity. An analytical evaluation of the proposed approach demonstrates a reduction in the probability of unauthorized disclosure of authentication keys compared to traditional protection methods. The obtained results have practical significance for the development of multi-level cybersecurity architectures in access control systems, cloud services, and password managers such as LastPass, where the secure storage and transmission of authentication keys are critical.

Keywords: cybersecurity, neural networks, machine learning, cryptography, steganography, authentication keys, password manager.

Фесенко Тетяна Миколаївна, кандидат технічних наук, 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 0009-0006-1698-3795, tanifesenko@gmail.com.

Калашнікова Юлія Вадимівна асистент 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 0000-0001-9899-4784, kalashjulia74@gmail.com.

Fesenko Tatiana, candidate of technical sciences, associate professor, associate professor of the department of computer and information technologies and systems at the Educational and scientific institute of information technologies and robotics, National University “Poltava Polytechnic named after Yury Kondratyuk”, Poltava, Ukraine.

Kalashnikova Yuliya, assistant of the department of computer and information technologies and systems at the Educational and scientific institute of information technologies and robotics, National University “Poltava Polytechnic named after Yury Kondratyuk”, Poltava, Ukraine.