УДК 004.932:004.8 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.57

О. М. СУПРУН
кандидат фізико-математичних наук, доцент,
доцент кафедри інтелектуальних кібернетичних систем
Державний університет «Київський авіаційний інститут»
ORCID: 0000-0002-1196-5655

Н. О. ЧІКІНА
кандидат технічних наук, доцент,
професор кафедри вищої математики
Інститут механічної інженерії і транспорту
Національного технічного університету
«Харківський політехнічний інститут»
ORCID: 0000-0002-0643-1771

Я. Я. КРАВЧУК
веб-розробник
ORCID: 0009-0006-1593-9995

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ АНАЛІЗУ ВІДЕОПОТОКУ ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ ПОВІДОМЛЕНЬ

Актуальність дослідження зумовлена стрімким зростанням обсягів відеоданих та ускладненням методів стеганографії, що становить значні ризики для інформаційної безпеки та робить неефективним використання традиційних засобів контролю. Традиційні алгоритми цифрової обробки сигналів не забезпечують достатнього рівня точності та стійкості у виявленні прихованих повідомлень, особливо за наявності шумових перешкод та динамічно змінюваних потоків даних. Це зумовлює потребу впроваджувати інтелектуальні підходи, які поєднують методи комп'ютерного зору, машинного навчання та мультимодального аналізу.

Мета статті – обґрунтувати та розробити інтелектуальні методи аналізу відеопотоку для виявлення прихованих повідомлень, що має забезпечити підвищення захищеності інформаційного середовища та ефективність сучасних алгоритмів штучного інтелекту за умов зростання кіберзагроз.

Методологія дослідження ґрунтується на поєднанні системного аналізу відеопотоку, методів машинного навчання, глибоких нейронних мереж та мультимодальних підходів до обробки даних. Використано принципи інтеграції алгоритмів комп'ютерного зору з класифікаційними моделями, зокрема згортковими та рекурентними мережами, а також механізмами самоуваги трансформерів. Застосовано порівняльний аналіз ефективності різних архітектур, моделювання роботи систем у режимі реального часу та оцінку їхньої стійкості до маніпуляцій.

Результати дослідження полягають у визначенні придатності традиційних та інтелектуальних методів для завдань ідентифікації прихованих сигналів. Доведено, що глибоке навчання та мультимодальні системи забезпечують значно вищу точність і адаптивність порівняно з традиційними підходами. Встановлено, що інтегровані архітектури аналізують просторові, часові й контекстуальні характеристики відео, створюють передумови для підвищення ефективності виявлення прихованих повідомлень у кіберзахисті, прикордонному контролі та моніторингу критичної інфраструктури.

Висновки підтверджують, що застосування інтелектуальних методів аналізу відеопотоку дає змогу долати обмеження традиційних рішень та істотно зміцнює інформаційну безпеку. Водночас виявлено основні проблеми впровадження: значні обчислювальні витрати, дефіцит анотованих мультимодальних даних, низька інтерпретованість результатів і вразливість до adversarial-атак.

Перспективи подальших досліджень пов'язані з розробленням адаптивних архітектур на основі continual learning і federated learning, оптимізацією моделей для енергоефективного функціонування, упровадженням explainable AI для підвищення прозорості роботи алгоритмів, а також зі створенням уніфікованих протоколів інтеграції з іншими засобами кіберзахисту. Очікується, що ці рішення сформують нове покоління інтелектуальних систем відеоаналізу, здатних ефективно реагувати на сучасні та майбутні інформаційні загрози.

Ключові слова: *стеганографія, кіберзахист, комп'ютерний зір, мультимодальний аналіз, глибоке навчання, штучний інтелект, інформаційна безпека.*

O. M. SUPRUN
Candidate of Physical and Mathematical Sciences, Associate Professor,
Associate Professor at the Department of Intelligent Cybernetic Systems
State University "Kyiv Aviation Institute"
ORCID: 0000-0002-1196-5655

N. O. CHIKINA
Candidate of Technical Sciences, Associate Professor,
Professor at the Department of Higher Mathematics
Institute of Education and Science in Mechanical Engineering and Transport
of National Technical University "Kharkiv Polytechnic Institute"
ORCID: 0000-0002-0643-1771

YA. YA. KRAVCHUK
Web Developer
ORCID: 0009-0006-1593-9995

INTELLIGENT METHODS OF VIDEO STREAM ANALYSIS FOR DETECTING HIDDEN MESSAGES

The relevance of this study is determined by the rapid growth of video data volumes and the increasing sophistication of steganographic methods, which pose significant risks to information security and undermine the effectiveness of traditional monitoring tools. Conventional digital signal processing algorithms fail to provide sufficient accuracy and robustness in detecting hidden messages, particularly in the presence of noise interference and dynamically changing data streams. This necessitates the implementation of intelligent approaches that integrate methods of computer vision, machine learning, and multimodal analysis.

The purpose of the article is to substantiate and develop intelligent methods of video stream analysis for detecting hidden messages, thereby enhancing the protection of the information environment and improving the efficiency of modern artificial intelligence algorithms under growing cyber threats.

The research methodology is based on the integration of system analysis of video streams, machine learning techniques, deep neural networks, and multimodal data processing approaches. It applies principles of combining computer vision algorithms with classification models, including convolutional and recurrent networks, as well as transformer-based attention mechanisms. A comparative analysis of the effectiveness of different architectures was carried out, along with real-time system modeling and assessment of their resistance to manipulations.

The results demonstrate the applicability of both traditional and intelligent methods for identifying hidden signals. The study confirms that deep learning and multimodal systems provide significantly higher accuracy and adaptability compared to traditional approaches. It was established that integrated architectures analyze spatial, temporal, and contextual video characteristics, creating prerequisites for improving the detection of hidden messages in cybersecurity, border control, and critical infrastructure monitoring.

The conclusions confirm that the application of intelligent video stream analysis methods overcomes the limitations of traditional solutions and significantly strengthens information security. At the same time, key implementation challenges were identified, including high computational costs, a shortage of annotated multimodal data, low interpretability of results, and vulnerability to adversarial attacks.

Future research prospects are linked to the development of adaptive architectures based on continual learning and federated learning, model optimization for energy-efficient functioning, the introduction of explainable AI to increase algorithm transparency, and the creation of unified protocols for integration with other cybersecurity tools. These advancements are expected to shape a new generation of intelligent video analysis systems capable of effectively responding to current and future information threats.

Key words: *steganography, cybersecurity, computer vision, multimodal analysis, deep learning, artificial intelligence, information security.*

Постановка проблеми

Проблема виявлення прихованих повідомлень у відеопотоці є однією з головних у сучасних дослідженнях з інформаційної безпеки та мультимедійної аналітики, оскільки традиційні методи контролю виявляються малоефективними в умовах зростання обсягів даних та ускладнення технік стеганографії. Інтелектуальні підходи поєднують можливості комп'ютерного зору, машинного навчання та нейронних мереж для ідентифікації прихованих патернів, які не піддаються традиційному аналізу. Такий підхід має значний науковий потенціал, адже орієнтований на розроблення нових алгоритмів розпізнавання прихованих структур у відео, що розширює межі сучасних теорій цифрової обробки сигналів та штучного інтелекту. На практиці це завдання має особливе значення для захисту національної безпеки та критичної інфраструктури, а також для ефективної протидії кіберзлочинності й інформаційним диверсіям. Розроблення ефективних інтелектуальних методів аналізу відеопотоку

здатне підвищити рівень захищеності цифрового середовища. Це вимагає створення інструментів оперативного моніторингу й запровадження технологій превентивного виявлення загроз, що безпосередньо пов'язує цю проблему з актуальними науковими пошуками й стратегічними практичними завданнями.

Аналіз останніх досліджень і публікацій

У наукових розвідках, присвячених інтелектуальним методам аналізу відеопотоку для виявлення прихованих повідомлень, можна виокремити чотири взаємопов'язані напрями. Перший напрям стосується розвитку захисних архітектур і застосування алгоритмів комп'ютерного зору для ідентифікації прихованих патернів. Ю. Горбенко (Y. Horbenko) довів, що застосування конфіденційних обчислень, зокрема захищених енклавів і гомоморфного шифрування, підвищує безпеку інтелектуальних систем аналізу відеопотоку [1]. С. Вань (S. Wan), С. Сюй (X. Xu), Т. Ван (T. Wang) та співавтори представили методи інтелектуального відеоаналізу для виявлення аномальних подій у транспортних системах, які підтверджують ефективність глибинних моделей у реальному часі [2]. Н. Меганатхан (N. Meghanathan), Л. Наяк (L. Nayak) узагальнили алгоритми стеганоаналізу для зображень, аудіо та відео, заклавши методологічну основу для подальших досліджень у сфері виявлення прихованих повідомлень [3]. М. Далал (M. Dalal), М. Джунеджа (M. Juneja) узагальнили методи відеостеганографії – від простих субституцій до адаптивних стратегій на основі машинного навчання [4]. Подальші дослідження необхідно зосередити на інтеграції глибинних моделей та захищених архітектур обчислень для оптимального поєднання продуктивності й безпеки.

Другий напрям пов'язаний із цифровим водяним знакуванням та захистом інформаційних потоків від атак. П. Аберна (P. Aberna), Л. Агіландесварі (L. Agilandeeswari) узагальнили методології цифрового фото- та відеоводяного знакування, виокремивши основні вектори атак і перспективи інтеграції з технологіями стеганографії [5]. На основі аналізу загроз Dark Web С. Назах (S. Nazah), С. Худа (S. Huda), Дж. Абаваджи (J. Abawajy) та співавтори дійшли висновку, що проблеми прихованих каналів посідають головне місце в сучасних стратегіях кіберзахисту [6]. Л. Сонг (L. Song), К. Лікопп (C. Licoppe) у своєму аналізі закриття відеострімів продемонстрували, що послідовність дій у таких потоках може нести ознаки прихованих комунікаційних сигналів [7]. С. Дхаван (S. Dhawan), Р. Гупта (R. Gupta) узагальнили методи стеганографії як інструменту захисту інформаційної безпеки, акцентуючи на порівняльних характеристиках різних підходів [8]. Подальші дослідження мають бути спрямовані на розроблення гібридних моделей, що поєднують watermarking, стеганографію та аналіз поведінкових патернів відеопотоків.

Третій напрям зосереджується на стійкості протоколів комунікацій і загрозах, пов'язаних з інтеграцією стеганографічних алгоритмів у сучасні системи обміну даними. Р. Хуан (R. Huang), Х. Ву (H. Wu), С. Ван (X. Wang) та співавтори довели, що сучасні протоколи миттєвого відеообміну є потенційним каналом прихованих атак, що істотно ускладнює завдання їхнього виявлення [9]. М. Далал (M. Dalal), М. Джунеджа (M. Juneja) у своїй пізнішій роботі систематизували принципи стеганографії та стеганоаналізу в контексті цифрової криміналістики, що відкриває нові перспективи для застосування таких методів у розслідуваннях кіберзлочинів [10]. Н. Субраманіан (N. Subramanian), О. Ельхаррусс (O. Elharrouss), С. Аль-Маадид (S. Al-Maadeed) та співавтори дослідили сучасні досягнення image steganography, виокремивши потенціал глибинних нейромереж у підвищенні стійкості алгоритмів [11]. О. Ф. А. Вагаб (O. F. A. Wahab), А. А. М. Халаф (A. A. M. Khalaf) та співавтори запропонували інтегровану схему приховування даних на основі поєднання RSA-шифрування та компресійної стеганографії, що підвищує рівень захисту [12]. Подальші дослідження в цьому напрямі мають зосереджуватись на формуванні протоколів стійкої комунікації, які інтегрують методи приховування даних із системами захисту від атак.

Четвертий напрям присвячений мультимодальним підходам до обробки та відновлення прихованої інформації в зашифрованих середовищах. З. Сунь (Z. Sun), П. Сарма (P. Sarma), В. Сетарес (W. Sethares) та співавтори показали ефективність мультимодальних методів, які дають змогу поєднувати аналіз текстових, аудіо- та відеопотоків для виявлення прихованих залежностей [13]. Ц. Ю (C. Yu), С. Чжан (X. Zhang) та співавтори розробили метод оборотного приховування даних у зашифрованих зображеннях із багаторівневим ієрархічним вбудовуванням, що сприяє контрольованому збереженню й відновленню прихованої інформації [14]. Цей напрям акцентує на важливості комплексного поєднання мультимодального аналізу й стеганографії у створенні систем, здатних не лише виявляти приховані повідомлення, а й відновлювати їх зі збереженням цілісності даних. Подальші дослідження у цій сфері мають орієнтуватися на стандартизацію мультимодальних протоколів і створення універсальних схем для відновлення даних у зашифрованих відеопотоках.

Попри значні досягнення в інтелектуальному аналізі відеопотоку, низка проблем досі нерозв'язана. Сучасні методи обробки даних демонструють обмежену стійкість до зашумлених та зашифрованих потоків, а також недостатню здатність адаптуватися до нових методів стеганографії. Відчутною проблемою є високі обчислювальні витрати та дефіцит якісних мультимодальних наборів даних, що ускладнює тренування універсальних моделей. Також зберігаються методологічні обмеження, пов'язані з низькою інтерпретованістю алгоритмів і складністю практичної інтеграції в реальні системи кіберзахисту.

У дослідженні запропоновано подолати ці прогалини шляхом поєднання алгоритмів комп'ютерного зору, машинного навчання та мультимодального аналізу для створення більш точних і адаптивних моделей.

Застосування гібридних архітектур, принципів continual та federated learning, а також оптимізованих методів глибинного навчання дасть змогу підвищити стійкість систем і знизити обчислювальні витрати.

Формулювання мети дослідження

Мета статті – обґрунтування та розробка інтелектуальних методів аналізу відеопотоку для виявлення прихованих повідомлень, що забезпечить підвищення рівня інформаційної безпеки й ефективність застосування технологій комп'ютерного зору та штучного інтелекту в умовах сучасних кіберзагроз.

Завдання статті:

1. Дослідити сучасні методи обробки відеопотоку та інтеграцію комп'ютерного зору з машинним навчанням для підвищення точності виявлення прихованої інформації.
2. Проаналізувати потенціал мультимодальних даних для ідентифікації прихованих повідомлень та визначити основні слабкі місця інтелектуальних методів у цій задачі.
3. Сформулювати практичні рекомендації щодо вдосконалення систем аналізу відеопотоку для зміцнення інформаційної безпеки та ефективної протидії кіберзагрозам.

Викладення основного матеріалу дослідження

Аналіз відеопотоку в сучасних умовах – це один із найдинамічніших напрямів розвитку інформаційних технологій, що поєднує комп'ютерний зір, обробку сигналів та алгоритми штучного інтелекту. Методи, що застосовуються для аналізу відео, різняться за рівнем складності та завданнями: від базової детекції руху й класифікації об'єктів до виявлення прихованих структур та стеганографічних повідомлень. Придатність конкретних методів визначається їхньою здатністю працювати в режимі реального часу, стійкістю до завад, масштабованістю та адаптивністю до нових форм приховування даних. З огляду на це доцільним є узагальнення найпоширеніших підходів, які застосовуються в сучасних системах аналізу відеопотоку (табл. 1).

Таблиця 1

Сучасні методи обробки відеопотоку та їхня придатність для виявлення прихованих повідомлень

Метод	Основні характеристики	Сфера застосування	Практичний результат
Традиційні алгоритми цифрової обробки зображень (фільтрація, сегментація, виділення контурів)	Формальні математичні процедури для роботи з кадрами відео	Системи первинного аналізу відео, попередня обробка даних	Швидке виявлення аномалій і базових відхилень у структурі зображення
Машинне навчання (класифікація, метод опорних векторів – Support Vector Machine, дерева рішень)	Навчання моделей на маркованих наборах даних із прикладами прихованої інформації	Системи автоматичного моніторингу та аналізу мультимедійного контенту	Покращення точності розпізнавання прихованих патернів порівняно з класичними методами
Глибоке навчання (Convolutional Neural Networks – CNN, Recurrent Neural Networks – RNN)	Автоматичне виділення ознак, виявлення складних і багаторівневих структур у відеопотоці	Високонавантажені системи кіберзахисту, аналітичні центри з великими масивами даних	Виявлення прихованих повідомлень навіть у зашумленому або зміненому відео, підвищена адаптивність
Мультимодальний аналіз (поєднання відео, звуку, метаданих)	Інтеграція різних типів даних у єдину модель	Системи кіберрозвідки, прикордонний та митний контроль, інформаційна безпека	Комплексне виявлення прихованої інформації, стійкість до маніпуляцій у різних середовищах

Джерело: сформовано авторами на основі [2, p. 4488–4489; 3, p. 45–46; 4, p. 5836–5837; 8, p. 238; 15, p. 4]

Сьогодні ці методи дедалі частіше інтегруються в багаторівневі системи аналізу відеопотоку, що дає змогу переходити від елементарних алгоритмів виявлення аномалій до складних інтелектуальних моделей, здатних виявляти приховані сигнали навіть у високодинамічному середовищі. Традиційні методи цифрової обробки зображень застосовуються як перший етап попередньої фільтрації даних, що дає змогу знизити обчислювальне навантаження на наступні рівні аналізу. Машинне навчання інтегрується в системи моніторингу для автоматичного виявлення закономірностей, наприклад, під час перевірки відеоконтенту на наявність стеганографічних вставок у прикордонному чи митному контролі [8, с. 237–238]. Глибокі нейронні мережі ефективно виявляють приховані повідомлення, замасковані зміною текстури чи кольорової палітри відео. Такі рішення вже використовують у центрах кібербезпеки для протидії диверсіям у медіапросторі. Важливу роль відіграють мультимодальні системи, які одночасно аналізують зображення, звук і метадані: вони успішно застосовуються в кіберрозвідці, де приховані сигнали можуть передаватися, наприклад, незначними шумовими коливаннями у звуковій доріжці чи зміненими параметрами файлів.

Інтеграція технологій комп'ютерного зору та машинного навчання створює окремий клас алгоритмічних підходів, що допомагають значно підвищити точність ідентифікації прихованої інформації у відеопотоці. Якщо традиційні методи працюють з окремими ознаками зображення, то інтегровані архітектури здатні поєднувати просторовий, часовий та контекстуальний аналіз у єдиній моделі. Така синергія сприяє не лише точнішому розпізнаванню прихованих патернів, але й адаптивності до різних форматів відео та сценаріїв застосування. Сучасні дослідження доводять важливість гібридних алгоритмічних рішень, що комбінують можливості згорткових

нейронних мереж для аналізу просторових характеристик, рекурентних мереж для роботи з часовими залежностями та алгоритмів машинного навчання для підсумкової класифікації сигналів (табл. 2).

Таблиця 2

Алгоритмічні підходи інтеграції комп'ютерного зору та машинного навчання

Алгоритмічний підхід	Механізм інтеграції	Приклад використання	Практичний ефект
CNN + SVM (Support Vector Machine)	CNN генерує ознаки, SVM здійснює класифікацію	Автоматизований відеоконтроль на митниці	Висока точність за відносно незначних обчислювальних витрат
CNN–RNN архітектури	Поєднання просторового аналізу кадрів і часової динаміки	Моніторинг транспортних потоків для виявлення прихованих сигналів	Виявлення аномалій у мікродинаміці рухів
Attention-based Transformers + комп'ютерний зір	Застосування механізму самоуваги для пошуку прихованих залежностей	Кібермоніторинг у потокових медіа	Масштабованість та здатність працювати в режимі реального часу
Ensemble-моделі (ансамблі Machine Learning (ML) та Deep Learning (DL))	Комбінація кількох класифікаторів для підвищення стабільності	Аналітичні центри інформаційної безпеки	Зменшення кількості хибнопозитивних результатів

Джерело: сформовано авторами на основі [2, p. 4491–4492; 4, p. 5841–5842; 10, p. 37962–37963; 15, p. 7]

Нині інтеграція комп'ютерного зору та машинного навчання реалізується через гнучкі алгоритмічні архітектури, здатні одночасно аналізувати просторові й часові характеристики відеопотоку. Поєднання CNN із традиційними класифікаторами, зокрема SVM, довело ефективність у прикордонному та митному контролі, де важлива швидкість і відносна простота обчислень. Архітектури CNN–RNN сприяють виявленню прихованих сигналів у динаміці руху об'єктів, що робить їх особливо цінними в транспортних системах і відеоспостереженні високої частоти [2, p. 4493–4494]. Трансформери з їхнім механізмом самоуваги забезпечують обробку великих обсягів потокових даних у реальному часі, що має вирішальне значення для кібермоніторингу та запобігання інформаційним атакам. Ансамблеві моделі, інтегруючи результати кількох алгоритмів, сприяють зниженню рівня хибнопозитивних сигналів, створюючи стабільніші та практично корисні рішення для аналітичних центрів безпеки. Таким чином, на практиці саме інтегровані алгоритмічні підходи формують новий стандарт точності й надійності у виявленні прихованих повідомлень.

Мультимодальний підхід до аналізу відеопотоку ґрунтується на одночасному використанні кількох типів даних, що дає змогу підвищити стійкість та точність виявлення прихованої інформації. На відміну від моделей, які працюють лише з візуальними ознаками, інтеграція звукових доріжок, текстових метаданих та характеристик середовища створює комплексне уявлення про зміст і контекст відео. Такий підхід є особливо актуальним у випадках, коли приховані повідомлення маскуються не у візуальних патернах, а в акустичних або структурних параметрах файлів. Поєднання різних джерел інформації сприяє формуванню більш надійних та адаптивних моделей, здатних працювати в умовах багатовимірних загроз (табл. 3).

Таблиця 3

Можливості використання мультимодальних даних для аналізу відеопотоку

Тип даних	Механізм інтеграції	Приклад використання	Очікуваний результат
Візуальні дані (зображення, кадри відео)	Виділення просторових ознак і поєднання з іншими каналами	Аналіз відео в системах безпеки аеропортів	Виявлення підозрілих змін у структурі кадрів
Аудіодані (звукові доріжки)	Обробка спектральних характеристик та поєднання з відеоаналізом	Контроль трансляцій для пошуку закодованих сигналів у шумі	Виявлення прихованих акустичних повідомлень
Метадані (формат, часові мітки, технічні параметри)	Кореляція службової інформації з візуально-звуковими каналами	Перевірка автентичності відеофайлів у кіберрозслідуваннях	Виявлення аномалій у структурі даних
Інтегровані мультимодальні моделі	Поєднання кількох каналів у єдиній архітектурі (наприклад, multimodal deep learning)	Системи аналітики потокових відео для кібермоніторингу	Підвищення точності та зменшення кількості хибних результатів

Джерело: сформовано авторами на основі [7, p. 6–7; 11, p. 23413–23414; 13, p. 4599–4600; 14]

У сучасних системах аналізу відеопотоку мультимодальність виконує роль визначального чинника підвищення об'єктивності: окремі канали інформації часто дають суперечливі або неповні результати, тоді як їхня інтеграція створює цілісну модель [14]. Візуальний аналіз дає змогу зафіксувати структурні відхилення, аудіоканал виявляє акустичні аномалії, а метадані сигналізують про приховані зміни у файлі. На практиці такий підхід продемонстровано в дослідженнях реального часу потокового мультимодального аналізу для кібербезпеки, де поєднання відео- та аудіоданих дало змогу істотно знизити кількість хибних тривог у моніторингових системах [15, с. 2]. Так, практичне впровадження мультимодальних моделей підтверджує їхню здатність ефективно виявляти приховані повідомлення в складних потоках даних та підвищувати надійність систем реагування.

Практична ефективність застосування інтелектуальних методів аналізу відеопотоку для виявлення прихованих повідомлень обмежується низкою проблем. Однією з головних є надзвичайно високі обчислювальні витрати, оскільки моделі глибинного навчання потребують потужних апаратних ресурсів, а робота з потоковим відео – обробки значних обсягів даних у реальному часі. Це ускладнює масштабування систем і їхнє впровадження в ресурсно обмежених середовищах, наприклад, у прикордонному контролі чи мобільних моніторингових комплексах [2, p. 4490]. Другою важливою проблемою є обмежена стійкість алгоритмів до зашифрованих або спеціально модифікованих відеопотоків, коли приховані повідомлення інтегруються в шумові структури або адаптивно змінюють параметри, щоб обходити виявлення [4, p. 5842–5843; 9, p. 5]. Уразливим місцем залишається здатність моделей адаптуватися до нових методів стеганографії, які еволюціонують швидше, ніж оновлюються алгоритмічні рішення.

Ще однією проблемою є висока залежність від якості даних: навіть невелике стиснення, артефакти кодування чи втрати пакетів під час передавання можуть істотно знизити точність розпізнавання. Це особливо важливо для систем потокового відео у відкритих мережах [7, p. 12–13]. Поширеним обмеженням є також відсутність достатніх обсягів анотованих мультимодальних даних для тренування моделей, що ускладнює досягнення високої узагальнювальної здатності та підвищує ризик помилкових результатів у реальних умовах [6, p. 102023].

У сфері кіберзахисту існує проблема низької інтерпретованості інтелектуальних моделей: навіть після успішного виявлення прихованих повідомлень, неможливість пояснити ознаки, на підставі яких система ухвалила рішення, обмежує довіру до результатів та ускладнює їхнє застосування в судово-експертних процесах [12, p. 1640–1641].

Не менш важливими є ризики масштабного впровадження: централізовані системи є потенційними мішенями для кібератак, а adversarial-атаки підтверджують, що мінімальні зміни у вхідних даних достатні для обходу навіть найсучасніших алгоритмів [5, p. 3055; 14]. Проблемою залишається високе енергоспоживання та вартість утримання складних інфраструктур, що обмежує можливості їхнього застосування в середовищах із жорсткими бюджетними обмеженнями.

Для вдосконалення систем аналізу відеопотоку потрібні адаптивні архітектури, здатні до самооновлення на основі безперервного машинного навчання. Застосування підходів continual learning та few-shot learning дає змогу моделям підтримувати актуальність навіть за умови появи нових методів стеганографії, що мінімізує часовий розрив між загрозою та здатністю системи її розпізнати. Перспективним напрямом є застосування федеративного навчання, що забезпечує обробку даних безпосередньо на периферійних вузлах, зберігаючи конфіденційність і одночасно підвищуючи масштабованість системи. Це особливо важливо для розподілених мереж відеоспостереження, де централізоване зберігання даних є вразливим і ресурсомістким.

Важливим завданням є розвиток енергоефективних моделей глибинного навчання, оптимізованих за допомогою pruning та quantization, що дає змогу істотно знизити обчислювальні витрати без втрати точності. Такі оптимізовані архітектури створюють умови для інтеграції систем у мобільні та портативні платформи, зокрема в безпілотні літальні апарати та переносні комплекси моніторингу. Одночасно постає потреба у впровадженні explainable AI, яке інтерпретує роботу моделей та перетворює її на зрозумілі закономірності чи ознаки. Це підвищує довіру операторів до системи та водночас створює юридично значущу доказову базу під час використання результатів виявлення в правових чи судово-експертних процесах.

Для систематизації отриманих результатів і формування орієнтирів подальших досліджень запропоновано покрокову схему розвитку інтелектуальних мультимодальних систем відеоаналізу. Схема відображає логіку еволюції від концептуальних рішень до практичного впровадження у сфері кіберзахисту. Вона побудована на основі поєднання принципів комп'ютерного зору, машинного навчання та мультимодального аналізу, а також враховує вимоги енергоефективності, інтерпретованості й інтеграційної сумісності. Інноваційність схеми полягає у комплексному підході до обробки даних – відеоаналіз розглядається як елемент багатоканальної системи інформаційної безпеки, що істотно знижує ризик хибнопозитивних результатів і підвищує швидкість реагування на загрози (рис. 1).

На першому етапі відбувається формування концептуальних моделей на основі інтеграції комп'ютерного зору та машинного навчання (CNN, RNN, трансформери), що забезпечує базову точність і здатність виявляти приховані структури у відео. Другий етап передбачає додавання мультимодальних каналів (аудіо, метадані, параметри середовища), завдяки чому зменшується кількість хибнопозитивних сигналів і зростає адаптивність системи. Третій етап полягає у впровадженні енергоефективних моделей через pruning, quantization та edge/federated learning, що знижує обчислювальні витрати й робить можливим мобільне застосування. На четвертому етапі забезпечується інтеграція з іншими засобами кіберзахисту (системами виявлення вторгнень, аналізом трафіку, цифровою криміналістикою), що формує комплексні інфраструктури захисту. Завершальним п'ятим етапом є контекстуальний та explainable аналіз із використанням continual learning і технологій XAI, що забезпечує прозорість прийняття рішень, довіру користувачів і превентивне реагування на загрози. Очікується, що реалізація такої схеми сприятиме створенню нового покоління інтелектуальних систем відеоаналізу, здатних ефективно протидіяти сучасним і майбутнім кіберзагрозам.

Рис. 1. Покрокова схема розвитку мультимодальних систем відеоаналізу

Джерело: власна розробка авторів

Висновки

У дослідженні доведено, що інтелектуальні методи аналізу відеопотоку значно розширюють можливості виявлення прихованих повідомлень завдяки поєднанню комп'ютерного зору, машинного навчання та мультимодальних підходів. Традиційні методи обробки сигналів придатні лише для базового виявлення аномалій, тоді як глибокі нейронні мережі та інтегровані архітектури забезпечують високу точність і адаптивність у динамічних умовах. Гібридні моделі виявилися ефективними, оскільки одночасно враховують просторові, часові й контекстуальні характеристики відео, що робить їх перспективними для застосування в кіберзахисті, прикордонному контролі та моніторингу критичної інфраструктури.

Ідентифіковано основні обмеження: значні обчислювальні витрати, нестійкість до шифрування та навмисних модифікацій, дефіцит якісних датасетів, низька інтерпретованість результатів і високі вимоги до ресурсів. Також виявлено ризики, пов'язані з можливістю adversarial-атак, які знижують довіру до результатів систем.

Подальші дослідження варто зосередити на створенні адаптивних архітектур із механізмами continual learning і federated learning, оптимізації моделей для енергоефективного функціонування, розвитку explainable AI та уніфікації протоколів інтеграції з іншими засобами кіберзахисту. Такий підхід сприятиме формуванню нового покоління інтелектуальних систем відеоаналізу, здатних не лише виявляти приховані повідомлення, а й забезпечувати превентивний захист інформаційного простору.

Список використаної літератури

1. Horbenko Y. Confidential Computing in Front-End: Enhancing Data Security with Secure Enclaves and Homomorphic Encryption. *International Journal of Advanced Multidisciplinary Research and Studies*. 2025. Vol. 5, № 3. P. 308-321. URL: https://www.multiresearchjournal.com/admin/uploads/archives/archive-1747130538.pdf (date of access: 27.09.2025).

2. Wan S., Xu X., Wang T., Gu Z. An Intelligent Video Analysis Method for Abnormal Event Detection in Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*. 2021. Vol. 22, № 7. P. 4487–4495. DOI: https://doi.org/10.1109/TITS.2020.3017505

3. Meghanathan N., Nayak L. Steganalysis algorithms for detecting the hidden information in image, audio and video cover media. *International Journal of Network Security & Its Application (IJNSA)*. 2010. Vol. 2, № 1. P. 43–55. DOI: https://doi.org/10.5121/ijnsa.2010.2104

4. Dalal M., Juneja M. A survey on information hiding using video steganography. *Artificial Intelligence Review*. 2021. Vol. 54. P. 5831–5895. DOI: https://doi.org/10.1007/s10462-021-09988-9

5. Aberna P., Agilandeeswari L. Survey of Digital Video Watermarking Techniques and Attacks. *Wireless Personal Communications*. 2021. Vol. 121. P. 3049–3082. DOI: https://doi.org/10.1007/s11277-021-08430-8

6. Nazah S., Huda S., Abawajy J., Hassan M. M. Evolution of Dark Web Threats: Social Engineering, Phishing and Cybercrime. *IEEE Access*. 2019. Vol. 7. P. 102021–102029. DOI: https://doi.org/10.1109/ACCESS.2019.2931097

7. Song L., Licoppe C. A multimodal approach to the sequential analysis of video streams closures. *Social Interaction. Video-Based Studies of Human Sociality*. 2020. Vol. 3, № 3. P. 1–24. DOI: https://doi.org/10.7146/si.v3i3.120547

8. Dhawan S., Gupta R. Steganography: An Overview. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2012. Vol. 2, № 10. P. 237–240. DOI: https://doi.org/10.1007/s10462-021-09968-0

9. Huang R., Wu H., Wang X., Cheng G., Hu X. Security Analysis of Video Identification Protocols for Instant Messaging Systems. *Security and Communication Networks*. 2018. Vol. 2018. P. 1–11. DOI: https://doi.org/10.1155/2018/3071247

10. Dalal M., Juneja M. Information Hiding Techniques for Steganography and Steganalysis. *Multimedia Tools and Applications*. 2022. Vol. 81. P. 37953–37989. DOI: https://doi.org/10.1007/s11042-022-12722-2.

11. Subramanian N., Elharrouss O., Al-Maadeed S., Bouridane A. Image Steganography: A Review of the Recent Advances. *IEEE Access*. 2021. Vol. 9. P. 23409–23423. DOI: https://doi.org/10.1109/ACCESS.2021.3053998

12. Wahab O. F. A., Khalaf A. A. M., Hussein A. I., Hamed H. F. A. A Secure and High Capacity RSA-Based Video Steganography Technique Using Lempel–Ziv–Welch Algorithm. *Multimedia Tools and Applications*. 2022. Vol. 81. P. 1637–1662. DOI: https://doi.org/10.1007/s11042-021-11693-7

13. Sun Z., Sarma P., Sethares W., Liang Y. Learning Relationships between Text, Audio, and Video via Deep Canonical Correlation for Multimodal Clustering. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2021. Vol. 35, № 5. P. 4596–4604. DOI: https://doi.org/10.1609/aaai.v35i5.16539

14. Yu C., Zhang X., Zhang X., Li G., Tang Z. Reversible Data Hiding in Encrypted Images Based on Multi-Level Hierarchical Embedding. *Signal Processing*. 2021. Vol. 178. Article 107794. DOI: https://doi.org/10.1016/j.sigpro.2020.107794

15. Xiao P., Xiao M., Cai N., Qiu B., Zhou S., Wang H. Adaptive Hybrid Framework for Multiscale Void Inspection of Chip Resistor Solder Joints. *IEEE Transactions on Instrumentation and Measurement*. 2023. Vol. 72. P. 1–12. DOI: https://doi.org/10.1109/TIM.2023.3235435

References

1. Horbenko, Y. (2025). Confidential Computing in Front-End: Enhancing Data Security with Secure Enclaves and Homomorphic Encryption. *International Journal of Advanced Multidisciplinary Research and Studies*, 5(3), 308–321. Retrived from: https://www.multiresearchjournal.com/admin/uploads/archives/archive-1747130538.pdf

2. Wan, S., Xu, X., Wang, T., & Gu, Z. (2021). An Intelligent Video Analysis Method for Abnormal Event Detection in Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*, 22(7), 4487–4495. DOI: https://doi.org/10.1109/TITS.2020.3017505

3. Meghanathan, N., & Nayak, L. (2010). Steganalysis algorithms for detecting the hidden information in image, audio and video cover media. *International Journal of Network Security & Its Application (IJNSA)*, 2(1), 43–55. DOI: https://doi.org/10.5121/ijnsa.2010.2104

4. Dalal, M., & Juneja, M. (2021). A survey on information hiding using video steganography. *Artificial Intelligence Review*, 54, 5831–5895. DOI: https://doi.org/10.1007/s10462-021-09988-9

5. Aberna, P., & Agilandeeswari, L. (2021). Survey of Digital Video Watermarking Techniques and Attacks. *Wireless Personal Communications*, 121, 3049–3082. DOI: https://doi.org/10.1007/s11277-021-08430-8

6. Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2019). Evolution of Dark Web Threats: Social Engineering, Phishing and Cybercrime. *IEEE Access*, 7, 102021–102029. DOI: https://doi.org/10.1109/ACCESS.2019.2931097

7. Song, L., & Licoppe, C. (2020). A multimodal approach to the sequential analysis of video streams closures. *Social Interaction. Video-Based Studies of Human Sociality*, 3(3), 1–24. DOI: https://doi.org/10.7146/si.v3i3.120547

8. Dhawan, S., & Gupta, R. (2012). Steganography: An Overview. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(10), 237–240. DOI: https://doi.org/10.1007/s10462-021-09968-0

9. Huang, R., Wu, H., Wang, X., Cheng, G., & Hu, X. (2018). Security Analysis of Video Identification Protocols for Instant Messaging Systems. *Security and Communication Networks*, 2018, 1–11. DOI: https://doi.org/10.1155/2018/3071247

10. Dalal, M., & Juneja, M. (2022). Information Hiding Techniques for Steganography and Steganalysis. *Multimedia Tools and Applications*, 81, 37953–37989. DOI: https://doi.org/10.1007/s11042-022-12722-2

11. Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. *IEEE Access*, 9, 23409–23423. DOI: https://doi.org/10.1109/ACCESS.2021.3053998

12. Wahab, O. F. A., Khalaf, A. A. M., Hussein, A. I., & Hamed, H. F. A. (2022). A Secure and High Capacity RSA-Based Video Steganography Technique Using Lempel–Ziv–Welch Algorithm. *Multimedia Tools and Applications*, 81, 1637–1662. DOI: https://doi.org/10.1007/s11042-021-11693-7

13. Sun, Z., Sarma, P., Sethares, W., & Liang, Y. (2021). Learning Relationships between Text, Audio, and Video via Deep Canonical Correlation for Multimodal Clustering. *Proceedings of the AAAI Conference on Artificial Intelligence*, 35(5), 4596–4604. DOI: https://doi.org/10.1609/aaai.v35i5.16539

14. Yu, C., Zhang, X., Zhang, X., Li, G., & Tang, Z. (2021). Reversible Data Hiding in Encrypted Images Based on Multi-Level Hierarchical Embedding. *Signal Processing*, 178, Article 107794. DOI: https://doi.org/10.1016/j.sigpro.2020.107794

15. Xiao, P., Xiao, M., Cai, N., Qiu, B., Zhou, S., & Wang, H. (2023). Adaptive Hybrid Framework for Multiscale Void Inspection of Chip Resistor Solder Joints. *IEEE Transactions on Instrumentation and Measurement*, 72, 1–12. DOI: https://doi.org/10.1109/TIM.2023.3235435.

Дата першого надходження рукопису до видання: 21.09.2025
Дата прийнятого до друку рукопису після рецензування: 17.10.2025
Дата публікації: 28.11.2025