№ 2(56)
2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online
УДК 004.056.5:004.7:004.8

https://doi.org/10.52058/2786-6025-2026-2(56)-1909-1928

Костюк Юлія Володимирівна доктор філософії (PhD), доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, Київський столичний університет імені Бориса Грінченка, м. Київ, https://orcid.org/0000-0001-5423-0985

Рзаєва Світлана Леонідівна кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук, Київський столичний університет імені Бориса Грінченка, м. Київ, https://orcid.org/0000-0002-7589-2045

Рзаєв Дмитро Олександрович старший викладач кафедри інформатики та системології, Київський національний економічний університет імені Вадима Гетьмана, м. Київ, https://orcid.org/0000-0002-7149-4971

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ ВИЯВЛЕННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Стрімка цифровізація бізнес-процесів і зростання масштабів мережевої взаємодії зумовлюють постійне збільшення обсягів трафіку та ускладнення кіберзагроз у комп'ютерних мережах. Сучасні атаки характеризуються автоматизацією, високою швидкістю реалізації та маскуванням під легітимну активність, що знижує результативність традиційних сигнатурних засобів, які залежать від повноти та актуальності баз шаблонів. Додатковим викликом є неможливість ручного аналізу великих масивів мережевих даних і наявність складних кореляцій між параметрами трафіку, які не завжди враховуються класичними алгоритмічними підходами.

У статті обґрунтовано доцільність застосування методів машинного навчання для автоматизованого аналізу мережевого трафіку та підвищення ефективності виявлення інцидентів інформаційної безпеки в умовах динамічного мережевого середовища.

Метою дослідження є розроблення структурної моделі інтелектуальної системи виявлення інцидентів на основі мережевого трафіку та експериментальне оцінювання її ефективності порівняно з традиційними підходами. Запропонована архітектура включає джерела вхідних даних (пакетний рівень, потокові записи та журнали подій мережевих засобів і серверів), модуль збору та консолідації, попередню обробку (очищення, агрегацію, нормалізацію),

ISSN 2786-6025 Online

формування інформативного набору ознак і модуль машинного аналізу для класифікації або виявлення аномалій.

Логіка прийняття рішення реалізує визначення класу події та ініціює процедури реагування: сповіщення оператора, автоматичне блокування/обмеження трафіку, оновлення політик безпеки.

Для забезпечення керованості та відтворюваності результатів передбачено журналювання подій у сховищі, аудит і контур зворотного зв'язку для перенавчання моделей.

Експериментальна частина охоплює порівняння поширених алгоритмів класифікації (Logistic Regression, Decision Tree, SVM, Random Forest) на розміченій вибірці мережевого трафіку з поділом даних на тренувальну та тестову підмножини. Якість моделей оцінено за стандартними метриками Accuracy, Precision, Recall, F1-score, а також за ROC-аналізом, що відображає компроміс між правильними виявленнями та хибнопозитивними спрацюваннями за різних порогів. Отримані результати демонструють перевагу ансамблевого підходу Random Forest, який забезпечив найвищі значення показників якості та найкращу здатність відокремлювати інциденти від нормального трафіку.

Додатково встановлено скорочення середнього часу виявлення інцидентів на 15–20 % порівняно із сигнатурним підходом, що підвищує оперативність реагування та зменшує ризики реалізації наслідків атак. Практична цінність роботи полягає у формуванні структурованої моделі інтелектуального моніторингу трафіку та обґрунтуванні вибору алгоритмів для задач раннього виявлення інцидентів у мережевих середовищах із високою динамікою.

Ключові слова: мережевий трафік, інцидент інформаційної безпеки, виявлення вторгнень, машинне навчання, класифікація, аномалії, формування ознак, попередня обробка даних, моніторинг мережі, журналювання подій.

Kostiuk Yuliia PhD in Computer Science Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok, Borys Grinchenko Kyiv Metropolitan University, Kyiv, https//orcid.org/0000-0001-5423-0985

Rzaeva Svitlana Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Science, Borys Grinchenko Kyiv Metropolitan University, Kyiv, https//orcid.org/0000-0002-7589-2045

Rzaev Dmytro Senior Lecturer of the Department of Informatics and Systemology Vadym Hetman Kyiv National University of Economics, Kyiv, https://orcid.org/0000-0002-7149-4971

№ 2(56)
2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online

INTELLIGENT NETWORK TRAFFIC ANALYSIS FOR INFORMATION SECURITY INCIDENT DETECTION

Abstract. The rapid digitalization of business processes and the expansion of network interactions lead to a continuous increase in traffic volumes and the growing complexity of cyber threats in computer networks. Modern attacks are characterized by automation, high execution speed, and disguise as legitimate activity, which reduces the effectiveness of traditional signature-based tools that depend on the completeness and timeliness of signature databases. An additional challenge is the impossibility of manual analysis of large-scale network data and the presence of complex correlations between traffic parameters that are not always captured by classical algorithmic approaches. The paper substantiates the feasibility of applying machine learning methods for automated network traffic analysis and improving the efficiency of information security incident detection in dynamic network environments.

The purpose of the study is to develop a structural model of an intelligent incident detection system based on network traffic and to experimentally evaluate its effectiveness compared to traditional approaches. The proposed architecture includes data sources (packet-level data, flow records, and logs from network devices and servers), a data collection and consolidation module, preprocessing (cleaning, aggregation, normalization), feature extraction, and a machine learning module for classification or anomaly detection. The decision-making logic determines the class of an event and initiates response procedures, including operator notification, automated traffic blocking or rate limiting, and security policy updates. To ensure controllability and reproducibility of results, event logging in a storage system, auditing, and a feedback loop for model retraining are implemented.

The experimental part involves a comparative analysis of widely used classification algorithms (Logistic Regression, Decision Tree, SVM, Random Forest) on a labeled network traffic dataset with a train-test split. Model performance is evaluated using standard metrics such as Accuracy, Precision, Recall, F1-score, as well as ROC analysis reflecting the trade-off between true positive and false positive rates under different thresholds. The results demonstrate the superiority of the ensemble-based Random Forest approach, which achieved the highest quality indicators and the best capability to distinguish security incidents from normal traffic. Additionally, a reduction in the average incident detection time by 15–20% compared to the signature-based approach was observed, which enhances response efficiency and reduces the risk of attack consequences. The practical value of the study lies in the development of a structured model for intelligent traffic monitoring and the justification of algorithm selection for early incident detection in highly dynamic network environments.

ISSN 2786-6025 Online
Keywords: network traffic, information security incident, intrusion detection, machine learning, classification, anomaly detection, feature extraction, data preprocessing, network monitoring, event logging.

Постановка проблеми. Стрімкий розвиток інформаційних технологій та цифровізація бізнес-процесів зумовлюють постійне зростання обсягів мережевого трафіку в комп'ютерних мережах. Одночасно з цим ускладнюється структура кіберзагроз, з'являються нові типи атак, що характеризуються високою швидкістю реалізації, маскуванням під легітимну активність та використанням автоматизованих інструментів.

Традиційні підходи до виявлення інцидентів інформаційної безпеки, що базуються на сигнатурному аналізі, передбачають зіставлення мережевого трафіку з відомими шаблонами атак. Однак ефективність таких систем обмежується наявністю відповідних сигнатур у базі даних. У випадку нових або модифікованих атак, а також при використанні технік приховування шкідливої активності, сигнатурні засоби можуть не забезпечувати належного рівня виявлення.

Додатковою проблемою є значний обсяг даних, що генеруються сучасними мережами. Ручний аналіз таких даних є практично неможливим, а традиційні алгоритмічні підходи часто не враховують складні кореляційні зв'язки між параметрами трафіку [1-2, 11]. У результаті виникає ризик несвоєчасного виявлення інцидентів або формування великої кількості хибних спрацювань.

Таким чином, постає науково-прикладна проблема підвищення ефективності виявлення інцидентів інформаційної безпеки шляхом автоматизованого аналізу мережевого трафіку з використанням інтелектуальних методів [9, 15]. Необхідним є розроблення підходу, який дозволить:

- аналізувати великі масиви мережевих даних у режимі, наближеному до реального часу [1, 11];
- виявляти як відомі, так і нові типи атак [5, 13];
- зменшити кількість хибнопозитивних та хибнонегативних результатів [4, 15];
- адаптувати систему до змін характеристик мережевого середовища.

Вирішення зазначеної проблеми можливе шляхом застосування методів машинного навчання для формування моделей нормальної та аномальної поведінки мережевого трафіку [1, 7, 9]. Це обумовлює необхідність дослідження можливостей інтелектуального аналізу трафіку та розроблення структури відповідної системи виявлення інцидентів.

Аналіз останніх досліджень і публікацій. Упродовж останніх років дослідження у сфері виявлення інцидентів інформаційної безпеки на основі

ISSN 2786-6025 Online

аналізу мережевого трафіку характеризуються активним впровадженням методів машинного навчання та глибокого навчання. Науковці зосереджують увагу не лише на підвищенні точності детектування атак, але й на забезпеченні адаптивності моделей, їх стійкості до змін мережевого середовища та можливості інтерпретації результатів.

Зокрема, у роботах 2023 року значна увага приділяється використанню глибоких нейронних мереж для аналізу великих обсягів трафіку. Дослідження M. Keshk [1] демонструє доцільність поєднання методів машинного навчання з пояснюваними механізмами аналізу, що дозволяє не лише виявляти аномалії, а й пояснювати причини прийнятого рішення системою. Автор підкреслює, що прозорість алгоритмів є критично важливою для практичного впровадження інтелектуальних систем виявлення вторгнень.

У свою чергу, W. Hu [2] зосереджується на проблемі формування інформативного набору ознак для підвищення точності класифікації мережевих подій. Дослідження доводить, що якість попередньої обробки та виділення характеристик трафіку істотно впливає на результативність алгоритмів глибокого навчання. Таким чином, ефективність системи виявлення інцидентів значною мірою залежить не лише від вибору моделі, а й від структури вхідних даних.

Подальший розвиток тематики представлено у роботі P. M. Corea [3], де здійснено порівняльний аналіз класичних алгоритмів машинного навчання для задач бінарної та багатокласової класифікації мережевих атак. Автор доводить, що ансамблеві методи, зокрема Random Forest, демонструють стабільно високі показники точності та повноти виявлення інцидентів. Водночас наголошується на необхідності стандартизації протоколів тестування та оцінювання моделей.

У дослідженнях 2025 року простежується тенденція до інтеграції адаптивних і пояснюваних механізмів у системи виявлення атак. Так, V. Z. Mohale [4] обґрунтовує важливість використання XAI-підходів для підвищення довіри до інтелектуальних IDS, що особливо актуально в умовах критичних інфраструктур. Робота демонструє, що пояснюваність рішень дозволяє зменшити кількість хибнопозитивних спрацювань та оптимізувати процес реагування. Додатково V. Pai [5] розглядає проблему адаптивного виявлення аномалій у змінних мережевих середовищах, підкреслюючи необхідність побудови моделей, здатних коригувати свої параметри відповідно до динаміки трафіку. Автор акцентує увагу на складності детектування атак, які маскуються під легітимну активність користувачів.

Систематичний огляд сучасних XAI-підходів для IDS, зокрема в контексті Industry 5.0 та протидії adversarial-атакам, представлено у роботі N. Khan [15], де наголошується на необхідності поєднання високої точності детектування з прозорістю та стійкістю моделей до маніпулятивних впливів.

ISSN 2786-6025 Online

Узагальнення проаналізованих праць свідчить, що сучасні дослідження спрямовані на підвищення точності та адаптивності інтелектуальних систем аналізу мережевого трафіку, проте залишаються відкритими питання зменшення кількості хибних спрацювань, забезпечення стабільності моделей у різних мережевих середовищах та оптимізації процесу попередньої обробки даних [4-5, 15]. Це підтверджує актуальність подальших досліджень у напрямі розроблення структурованої інтелектуальної системи моніторингу мережевого трафіку для ефективного виявлення інцидентів інформаційної безпеки.

Мета статті – обґрунтувати доцільність застосування методів машинного навчання для аналізу мережевого трафіку, розробити структуру інтелектуальної системи виявлення інцидентів інформаційної безпеки та оцінити її ефективність у порівнянні з традиційними сигнатурними підходами.

Методи дослідження. У процесі дослідження було застосовано комплекс теоретичних та експериментальних методів, спрямованих на аналіз можливостей інтелектуального виявлення інцидентів інформаційної безпеки на основі мережевого трафіку.

На теоретичному етапі використано методи аналізу та узагальнення наукових джерел з метою визначення сучасних підходів до виявлення мережевих атак, класифікації інцидентів та вибору алгоритмів машинного навчання для задач аналізу трафіку. Порівняльний аналіз дозволив визначити переваги та обмеження сигнатурних, поведінкових і гібридних систем виявлення вторгнень.

Для побудови інтелектуальної моделі було використано методи машинного навчання, що передбачають навчання класифікаторів на основі історичних даних мережевої активності [1, 11, 13]. Дослідження охоплювало етапи збору, підготовки та аналізу даних. На етапі збору використовувалися мережеві журнали та потоки трафіку, що містили приклади як нормальної активності, так і атак типу DoS, сканування портів та підбору паролів.

Попередня обробка даних включала очищення набору від шумових записів, усунення пропусків, нормалізацію числових параметрів та кодування категоріальних ознак [2-3, 7-9]. Особливу увагу приділено формуванню інформативного набору характеристик трафіку, зокрема кількості пакетів за певний інтервал часу, середнього розміру пакета, частоти з’єднань, тривалості сесій та кількості невдалих спроб автентифікації.

У межах експериментального дослідження застосовано такі алгоритми класифікації: Logistic Regression, Decision Tree, Random Forest, Support Vector Machine та k-Nearest Neighbors.

Навчання моделей здійснювалося на тренувальній вибірці, після чого проводилося тестування на незалежному наборі даних для оцінювання узагальнювальної здатності моделей.

ISSN 2786-6025 Online

Оцінювання ефективності моделей здійснювалося за допомогою стандартних метрик класифікації: Accuracy, Precision, Recall та F1-score [7, 9, 11]. Для зменшення ризику переобучення використовувався поділ вибірки на тренувальну та тестову частини, а також застосовувався метод перехресної перевірки.

Таким чином, обрані методи дослідження забезпечили можливість комплексної оцінки ефективності інтелектуального аналізу мережевого трафіку та визначення доцільності використання алгоритмів машинного навчання для виявлення інцидентів інформаційної безпеки.

Виклад основного матеріалу. Сучасні комп'ютерні мережі є ключовим елементом функціонування інформаційних систем підприємств, державних установ, фінансових організацій та об'єктів критичної інфраструктури [7, 15]. Забезпечення їх стабільної та безпечної роботи безпосередньо впливає на економічну безпеку, безперервність бізнес-процесів і захист інформаційних ресурсів. Водночас стрімке зростання обсягів мережевого трафіку, розвиток хмарних технологій, мобільних сервісів та розподілених інформаційних систем призводять до ускладнення структури мережевої взаємодії та збільшення кількості потенційних вразливостей.

Паралельно з розвитком інформаційних технологій еволюціонують і кіберзагрози. Сучасні атаки характеризуються високим рівнем автоматизації, використанням бот-мереж, методів приховування шкідливої активності та маскування під легітимний трафік. Зловмисники застосовують комбіновані сценарії атак, що ускладнює їх своєчасне виявлення традиційними засобами захисту. У таких умовах особливої актуальності набуває проблема ефективного виявлення інцидентів інформаційної безпеки на ранніх етапах їх реалізації.

Традиційні системи виявлення атак, що базуються на сигнатурному аналізі, здійснюють зіставлення мережевих подій із відомими шаблонами загроз [7]. Хоча такі системи демонструють високу ефективність для ідентифікації відомих атак, вони мають обмежені можливості щодо виявлення нових або модифікованих сценаріїв вторгнення [9]. Крім того, сигнатурний підхід потребує постійного оновлення баз даних і не враховує динамічних змін у поведінці мережевих користувачів. Альтернативою є поведінковий підхід, який передбачає формування профілю нормального функціонування мережі та виявлення відхилень від нього [11, 13, 16]. Саме на цьому принципі ґрунтується застосування методів штучного інтелекту та машинного навчання, що дозволяють аналізувати великі обсяги мережевих даних, виявляти приховані закономірності та автоматично класифікувати події як нормальні або аномальні.

Інтелектуальний аналіз мережевого трафіку створює можливість підвищення точності виявлення інцидентів, зменшення кількості хибнопозитивних

ISSN 2786-6025 Online

спрацювань та адаптації системи захисту до змін характеристик мережевого середовища. У зв'язку з цим актуальним є дослідження методів машинного навчання, здатних забезпечити ефективну класифікацію мережевих подій та підтримку прийняття рішень у процесі реагування на інциденти.

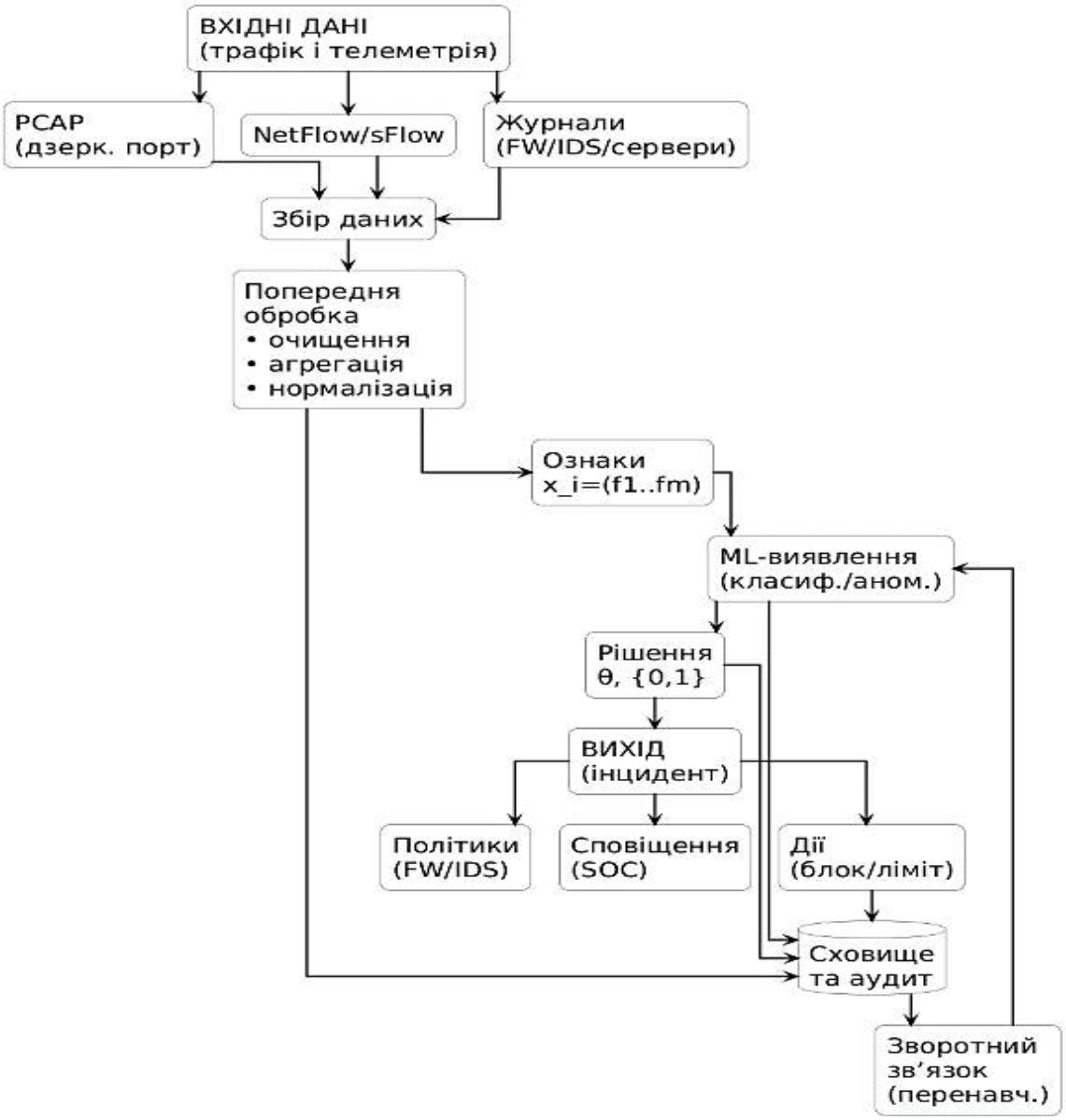

Рис. 1. Загальна структурна модель інтелектуальної системи аналізу мережевого трафіку для виявлення інцидентів інформаційної безпеки
Джерело: побудовано авторами

На рис. 1 подано структурну модель інтелектуальної системи аналізу мережевого трафіку для виявлення інцидентів інформаційної безпеки. У верхній частині схеми показано джерела вхідних даних: пакетний трафік

ISSN 2786-6025 Online

(PCAP), потокові записи (NetFlow/sFlow) та журнали подій міжмережевих екранів, IDS і серверів. Усі ці дані надходять до модуля збору, де відбувається їх консолідація та підготовка до обробки. Наступним етапом є попередня обробка, яка включає очищення, агрегацію та нормалізацію даних. Після цього формується набір ознак, що відображають характеристики мережевої активності та використовуються модулем машинного навчання для класифікації або виявлення аномалій. На основі результатів аналізу приймається рішення про наявність або відсутність інциденту. У разі виявлення загрози система ініціює відповідні дії: формування сповіщення для оператора, автоматичне блокування або обмеження трафіку, а також оновлення політик безпеки. Усі події та результати зберігаються у сховищі для забезпечення аудиту. Дані зі сховища можуть використовуватися для перенавчання моделі, що формує зворотний зв'язок і забезпечує адаптацію системи до нових типів атак та змін у мережевому середовищі.

Для формалізації процесу виявлення інцидентів інформаційної безпеки розглянемо мережевий трафік як множину спостережень [6-7, 9]:

$$X = \{x_1, x_2, \dots, x_n\}, \quad (1)$$

де x_i – вектор ознак i-го мережевого з'єднання або потоку. Таке представлення дозволяє перейти від сирих мережевих даних до формалізованої моделі, придатної для подальшого машинного аналізу.

Кожен вектор ознак формується у вигляді:

$$x_i = (f_1, f_2, \dots, f_m), \quad (2)$$

де f_1 – кількість пакетів за інтервал часу, f_2 – середній розмір пакета, f_3 – частота встановлення з'єднань, f_4 – тривалість сесії, f_5 – кількість невдалих спроб автентифікації тощо. Таким чином, процес виявлення інцидентів зводиться до задачі класифікації багатовимірних векторів ознак [11]. Таке представлення забезпечує можливість уніфікації різнорідних характеристик мережевого трафіку та приведення їх до числового формату, придатного для застосування алгоритмів машинного навчання. Крім того, формування множини векторів ознак створює основу для побудови математичної моделі класифікації, що дозволяє автоматизувати процес виявлення інцидентів інформаційної безпеки.

На рис. 2 представлено структурну модель формування вектора ознак на основі трирівневого аналізу мережевого трафіку [2, 13]. Вхідними даними є

ISSN 2786-6025 Online

мережеві пакети, потоки та журнали подій, які надходять до системи для подальшої обробки. Процес побудований за трьома паралельними гілками. Перша гілка (packet-level) формує ознаки на рівні окремих пакетів, враховуючи їх розмір, інтервали між надходженням та службові прапорці протоколів. Друга гілка (flow-level) оперує агрегованими характеристиками потоків або сесій, такими як тривалість з'єднання, обсяг переданих даних та інтенсивність трафіку. Третя гілка (behavioral-level) відображає поведінкові характеристики, зокрема частоту активності, повторюваність дій та історичні шаблони мережевої взаємодії. Після виділення параметрів у кожній гілці здійснюється їх нормалізація для забезпечення узгодженості масштабів та коректності подальшого машинного аналізу. Далі всі групи ознак інтегруються в єдиний узгоджений вектор, який використовується як вхід для моделей машинного навчання. Запропонована трирівнева структура дозволяє поєднати миттєві характеристики трафіку, агреговані статистики з'єднань та довгострокові поведінкові патерни, що підвищує інформативність вхідних даних і стійкість системи до складних та модифікованих сценаріїв атак.

Рис. 2. Схема формування вектора ознак
для інтелектуального аналізу мережевого трафіку
Джерело: побудовано авторами

ISSN 2786-6025 Online

Задача виявлення інцидентів зводиться до побудови функції класифікації:

$$F : X \to Y, \tag{3}$$

де $Y = \{0,1\}$, 0 – нормальний трафік, 1 – інцидент безпеки.

Тобто кожному вектору ознак мережевого з'єднання ставиться у відповідність один із двох класів залежно від характеру його поведінки. Побудова такої функції передбачає навчання моделі на основі попередньо розмічених даних, що містять приклади як нормального трафіку, так і атак [4, 15-16].

Якість сформованої функції класифікації безпосередньо визначає здатність системи своєчасно виявляти інциденти та мінімізувати кількість хибних спрацювань.

Для алгоритму Logistic Regression ймовірність належності об'єкта до класу інцидентів визначається як [3, 7]:

$$P(y = 1|x) = \frac{1}{1+e^{-(w^T x+b)}}, \tag{4}$$

де w – вектор вагових коефіцієнтів, b – зміщення. Формула описує сигмоїдну функцію, яка перетворює лінійну комбінацію ознак у значення ймовірності в інтервалі від 0 до 1.

Вектор вагових коефіцієнтів www відображає значущість кожної ознаки у процесі прийняття рішення, а параметр b визначає зсув гіперплощини класифікації.

Під час навчання моделі значення w та b оптимізуються таким чином, щоб мінімізувати похибку класифікації на тренувальній вибірці.

На рис. 3 зображено сигмоїдну функцію, що використовується в алгоритмі Logistic Regression для обчислення ймовірності належності мережевого з'єднання до класу інцидентів інформаційної безпеки. По осі абсцис відкладено лінійну комбінацію ознак $z = w^T x + b$, а по осі ординат – відповідну ймовірність $P(y = 1|x)$. Горизонтальна лінія відповідає пороговому значенню θ, яке визначає правило класифікації: якщо значення функції перевищує θ, трафік відноситься до класу інцидентів, інакше – до нормального класу [11-12].

Візуалізація демонструє нелінійний характер перетворення ознак у ймовірність та наочно пояснює механізм прийняття рішення моделлю.

ISSN 2786-6025 Online

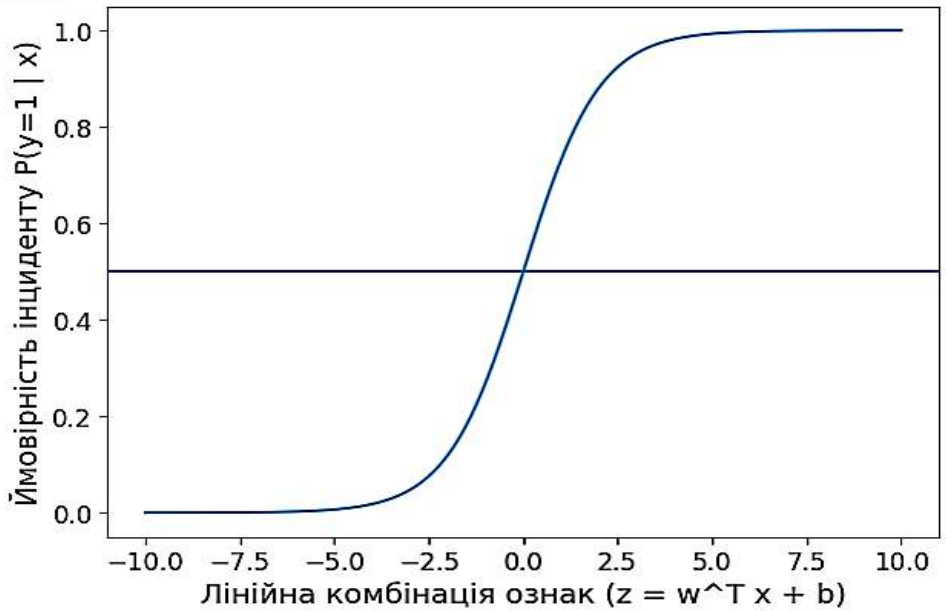

Рис. 3. Графік сигмоїдної функції Logistic Regression з порогом прийняття рішення θ

Джерело: побудовано авторами

Фінальне рішення приймається за пороговим правилом [15]:

$$\hat{y} = \begin{cases} 1, & \text{якщо } P(y=1|x) \geq \theta \\ 0, & \text{інакше} \end{cases}, \quad (5)$$

де θ – порогове значення. Порогове значення θ визначає межу, при перевищенні якої об'єкт класифікується як інцидент інформаційної безпеки.

Вибір цього параметра суттєво впливає на баланс між кількістю хибнопозитивних та хибнонегативних результатів: зменшення θ підвищує чутливість моделі, але може збільшити кількість помилкових спрацювань. Таким чином, оптимальне значення порога обирається з урахуванням вимог до рівня безпеки та допустимого ризику пропуску атак.

З метою підвищення стійкості моделі до шуму та нелінійних залежностей використано ансамблевий метод Random Forest [7, 13]:

$$F(x) = \frac{1}{T}\sum_{t=1}^{T} h_t(x), \quad (6)$$

де T – кількість дерев, $h_t(x)$ – результат t-го дерева. Такий підхід передбачає побудову множини незалежних дерев рішень на різних підвибірках навчальних даних із випадковим вибором ознак. Кожне дерево формує власне

ISSN 2786-6025 Online

рішення щодо належності об'єкта до певного класу, а сукупний результат визначається шляхом агрегування їх відповідей. Завдяки усередненню результатів зменшується вплив випадкових коливань у даних, що підвищує загальну точність і стійкість моделі до перенавчання.

Фінальне рішення визначається більшістю голосів [13]:

$$\hat{y} = mode\{h_1(x), h_2(x), \dots, h_T(x)\}, \quad (7)$$

Ансамблевий підхід дозволяє зменшити варіативність окремих моделей і підвищити узагальнювальну здатність класифікатора.

Функція $mode$ у формулі (7) означає вибір класу, який отримав найбільшу кількість голосів серед усіх побудованих дерев рішень. Такий механізм агрегування рішень дозволяє компенсувати помилки окремих слабких моделей та забезпечує більш стабільний результат класифікації. У результаті знижується чутливість системи до окремих аномальних спостережень і підвищується надійність виявлення інцидентів у різних умовах функціонування мережі.

Для оцінювання ефективності запропонованої моделі класифікації використовується матриця помилок (confusion matrix), що відображає співвідношення між фактичними та передбаченими результатами класифікації [15]. Такий підхід дозволяє детально проаналізувати типи помилок, які допускає модель, та оцінити її поведінку в умовах реальних мережевих сценаріїв.

Таблиця 1

Матриця помилок класифікації

	Передбачено інцидент (1)	**Передбачено норму (0)**
Фактично інцидент (1)	TP (True Positive)	FN (False Negative)
Фактично норма (0)	FP (False Positive)	TN (True Negative)

У табл. 1 показано чотири можливі результати класифікації. Показник TP відображає кількість правильно виявлених інцидентів, тоді як TN характеризує кількість правильно визначених нормальних з'єднань. Значення FP відповідає хибнопозитивним спрацюванням, а FN – пропущеним інцидентам, що є найбільш критичним типом помилки у сфері інформаційної безпеки. Саме на основі цих показників обчислюються основні метрики ефективності моделі

На основі матриці помилок обчислюються основні метрики якості класифікації. Загальна точність визначається як [10, 12]:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}, \quad (8)$$

ISSN 2786-6025 Online

Ця метрика характеризує частку правильно класифікованих спостережень серед усіх прикладів. Однак показник $Accuracy$ є інформативним лише за умови відносної збалансованості класів у вибірці [12, 14]. У задачах виявлення інцидентів, де кількість нормального трафіку може суттєво перевищувати кількість атак, доцільно додатково використовувати інші метрики, що враховують співвідношення помилок різних типів.

Точність (Precision) обчислюється як:

$$Precision = \frac{TP}{TP+FP}, \quad (9)$$

Precision показує, яка частка передбачених інцидентів є дійсно інцидентами. Високе значення цієї метрики означає низький рівень хибнопозитивних спрацювань, тобто вона відображає частку правильних спрацювань серед усіх передбачених інцидентів. Високе значення показника $Precision$ є особливо важливим у середовищах із великим обсягом мережевого трафіку [6, 8], де надмірна кількість хибнопозитивних спрацювань може призвести до перевантаження служби інформаційної безпеки [10]. Таким чином, ця метрика дозволяє оцінити надійність системи з точки зору коректності її попереджень про інциденти.

Повнота (Recall) визначається як:

$$Recall = \frac{TP}{TP+FN}, \quad (10)$$

$Recall$ визначає здатність моделі виявляти всі наявні інциденти. Низьке значення цієї метрики свідчить про значну кількість пропущених атак [12]. Високе значення $Recall$ свідчить про ефективність системи у виявленні більшості інцидентів інформаційної безпеки, що є критично важливим для мінімізації ризиків [10, 14].

Водночас надмірне підвищення цієї метрики може супроводжуватися зростанням кількості хибнопозитивних спрацювань, тому її доцільно аналізувати у взаємозв'язку з показником $Precision$.

Комплексна оцінка здійснюється за допомогою F1-міри:

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision+Recall}, \quad (11)$$

ISSN 2786-6025 Online

F1-міра є гармонійним середнім між Precision та Recall і використовується для комплексної оцінки моделі в умовах дисбалансу класів [10, 14]. Використання гармонійного середнього дозволяє врахувати взаємозв'язок між повнотою та точністю, зменшуючи вплив їх значного розбалансування. F1-міра є особливо доцільною у задачах виявлення інцидентів інформаційної безпеки [6, 8], де важливо одночасно мінімізувати як пропущені атаки, так і хибнопозитивні спрацювання.

У задачах виявлення інцидентів інформаційної безпеки особливе значення має мінімізація показника FN (пропущених атак), оскільки навіть одиничний невиявлений інцидент може призвести до суттєвих втрат [14]. Водночас надмірне зростання FP призводить до перевантаження систем реагування та зниження довіри до інтелектуальної моделі [10, 12]. Тому при оцінюванні ефективності класифікаторів доцільно використовувати комплекс метрик, зокрема $Precision$, $Recall$ та $F1$.

Моделювання виконувалося на вибірці мережевого трафіку, що містила 60 % нормальних з'єднань та 40 % атак. Такий розподіл дозволив забезпечити достатню кількість прикладів обох класів для навчання та об'єктивного оцінювання моделі. Дані були поділені у співвідношенні 70 % – для тренування та 30 % – для тестування, що дало можливість перевірити узагальнювальну здатність алгоритмів на незалежній вибірці. Результати експериментального оцінювання наведено в табл. 2.

Таблиця 2

Порівняльні результати алгоритмів класифікації

Алгоритм	Accuracy	Precision	Recall	F1-score
Logistic Regression	0.87	0.84	0.82	0.83
Decision Tree	0.89	0.86	0.85	0.85
SVM	0.91	0.88	0.87	0.87
Random Forest	0.94	0.92	0.90	0.91

Як видно з табл. 2, усі досліджені алгоритми демонструють прийнятний рівень точності виявлення інцидентів інформаційної безпеки [12]. Водночас найвищі показники за всіма метриками отримано для алгоритму Random Forest, що свідчить про його кращу здатність враховувати складні залежності між параметрами мережевого трафіку. Отримані результати підтверджують доцільність використання ансамблевих методів для задач аналізу та класифікації мережевих інцидентів.

На рис. 4 представлено ROC-криві для алгоритмів Logistic Regression, Decision Tree, SVM та Random Forest. Крива відображає залежність між часткою хибнопозитивних спрацювань (FPR) та часткою правильно виявлених

ISSN 2786-6025 Online

інцидентів (TPR) при зміні порогового значення класифікації. Найбільшу площу під кривою (AUC) демонструє алгоритм Random Forest, що підтверджує його кращу здатність відокремлювати інциденти безпеки від нормального трафіку. Результати графічно узгоджуються з показниками F1-score, наведеними у табл. 2, і підтверджують доцільність використання ансамблевого підходу для задач інтелектуального аналізу мережевого трафіку.

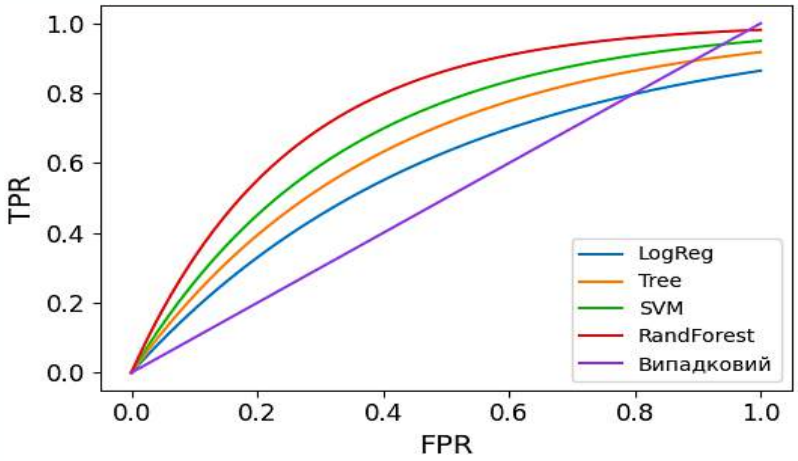

Рис. 4. Криві робочої характеристики приймача (ROC) для алгоритмів класифікації
Джерело: побудовано авторами

Інцидент вважається зафіксованим у момент часу t, якщо:

$$F(h_t) = 1, \tag{12}$$

Тобто у момент надходження нового вектора ознак система здійснює його класифікацію та приймає рішення щодо наявності загрози [10, 12, 14]. У випадку, якщо значення функції дорівнює одиниці, формується сигнал про інцидент та ініціюється процедура реагування відповідно до політики безпеки.

Час реагування системи визначається як:

$$T_{resp} = t_{detect} - t_{start}, \tag{13}$$

де t_{start} – початок атаки, t_{detect} – момент виявлення. Зменшення значення T_{resp} є одним із ключових показників ефективності інтелектуальної системи виявлення інцидентів. Чим менший інтервал між початком атаки та моментом її детектування, тим нижчою є ймовірність реалізації негативних наслідків для інформаційної системи.

ISSN 2786-6025 Online

Моделювання показало зменшення середнього часу виявлення інциденту на 15–20 % порівняно із сигнатурним підходом, що підтверджує практичну ефективність інтелектуального аналізу трафіку.

Отримані результати свідчать про доцільність застосування методів машинного навчання для оперативного виявлення мережевих загроз у динамічному середовищі.

Таким чином, інтелектуальний аналіз трафіку забезпечує не лише підвищення точності класифікації, але й скорочення часу реагування на інциденти інформаційної безпеки.

Висновки. У статті розв'язано науково-прикладну задачу підвищення ефективності виявлення інцидентів інформаційної безпеки шляхом інтелектуального аналізу мережевого трафіку. Обґрунтовано обмеження сигнатурних підходів в умовах появи нових і модифікованих атак та зростання обсягів даних, а також показано доцільність застосування методів машинного навчання для автоматизованого формування моделей нормальної та аномальної мережевої поведінки.

Запропоновано структуровану модель інтелектуальної системи моніторингу трафіку, що охоплює збір даних (пакетний, потоковий та журнальний рівні), попередню обробку, формування вектора ознак, модуль ML-виявлення, прийняття рішення та підсистему реагування із збереженням подій для аудиту й забезпечення адаптивного зворотного зв'язку.

Для задачі класифікації мережевого трафіку використано порівняльний експеримент із застосуванням Logistic Regression, Decision Tree, SVM та Random Forest, а якість моделей оцінено за метриками Accuracy, Precision, Recall, F1-score і ROC-аналізом.

Експериментальні результати підтверджують, що найкращі показники виявлення інцидентів забезпечує ансамблевий метод Random Forest (Accuracy = 0.94, Precision = 0.92, Recall = 0.90, F1-score = 0.91), що узгоджується з ROC-кривими та свідчить про кращу здатність моделі відокремлювати інциденти від нормального трафіку.

Додатково встановлено, що інтелектуальний підхід забезпечує зменшення середнього часу виявлення інциденту на 15–20 % порівняно із сигнатурним аналізом, що є критичним для мінімізації наслідків атак у реальних мережевих середовищах.

Подальші дослідження доцільно спрямувати на розширення набору ознак за рахунок часових та поведінкових характеристик, використання глибокого навчання для виявлення складних багатокрокових атак, підвищення інтерпретованості рішень (XAI) для зменшення хибнопозитивних спрацювань, а також апробацію підходу на багатодоменних даних реальних мереж із урахуванням дрейфу розподілів трафіку.

ISSN 2786-6025 Online

Література:

1. M. Keshk, N. Koroniotis, N. Pham, N. Moustafa, B. Turnbull, and A. Y. Zomaya, "An explainable deep learning-enabled intrusion detection framework in IoT networks," *Information Sciences*, vol. 639, Art. no. 119000, 2023. https://doi.org/10.1016/j.ins.2023.119000

2. W. Hu, L. Cao, Q. Ruan, and Q. Wu, "Research on anomaly network detection based on self-attention mechanism," *Sensors*, vol. 23, no. 11, p. 5059, 2023. https://doi.org/10.3390/s23115059

3. P. M. Corea, Y. Liu, J. Wang, S. Niu, and H. Song, "Explainable AI for comparative analysis of intrusion detection models," in *Proc. IEEE Int. Mediterranean Conf. Communications and Networking (MeditCom)*, 2024, pp. 585–590.

4. V. Mohale and I. Obagbuwa, "Evaluating machine learning-based intrusion detection systems with explainable AI: Enhancing transparency and interpretability," *Frontiers in Computer Science*, vol. 7, 2025. https://doi.org/10.3389/fcomp.2025.1520741

5. V. Pai et al., "Adaptive network anomaly detection using machine learning approaches," *EURASIP Journal on Information Security*, vol. 2025, Art. no. 29, 2025. https://doi.org/10.1186/s13635-025-00216-4

6. Y. Kostiuk et al., "Protection of information and secure data exchange in wireless mobile networks with authentication and key exchange protocols," *Cybersecurity: Education, Science, Technique*, vol. 1, no. 25, pp. 229–252, 2024. https://doi.org/10.28925/2663-4023.2024.25.229252

7. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, Art. no. 102419, 2019. https://doi.org/10.1016/j.jisa.2019.102419

8. Y. Kostiuk et al., "Ensuring cybersecurity and performance of data transmission in wireless networks," *Information Security*, vol. 30, no. 3, pp. 365–375, 2024. https://doi.org/10.17721/ISTS.2024.8.5-16

9. Z. Li, W. Fang, C. Zhu, G. Song, and W. Zhang, "Toward deep learning-based intrusion detection system: A survey," in *Proc. 6th Int. Conf. Big Data Engineering (BDE)*, 2024, pp. 25–32. https://doi.org/10.1145/3688574.3688578

10. Y. Kostiuk et al., "Tool-based information security protection against hidden threats in cloud infrastructure," *Cybersecurity: Education, Science, Technique*, vol. 4, no. 28, pp. 633–655, 2025. https://doi.org/10.28925/2663-4023.2025.28.857

11. K. Prabu and P. Sudhakar, "A hybrid deep learning approach for enhanced network intrusion detection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, p. 1915, 2024. https://doi.org/10.11591/ijeecs.v33.i3.pp1915-1923

12. Y. Kostiuk et al., "Specific features of network attacks implementation via TCP/IP protocols," *Cybersecurity: Education, Science, Technique*, vol. 1, no. 29, pp. 571–597, 2025. https://doi.org/10.28925/2663-4023.2025.29.915

13. D. Ke, "Network intrusion detection based on feature selection and transformer," in *Proc. Int. Conf. Intelligent Communication and Computer Engineering (ICICCE)*, 2023, pp. 23–28. https://doi.org/10.1109/ICICCE61720.2023.00010

14. Y. Kostiuk et al., "Intelligent control and protection systems in cyber-physical and cloud-based Smart Grid environments," *Cybersecurity: Education, Science, Technique*, vol. 2, no. 30, pp. 125–156, 2025. https://doi.org/10.28925/2663-4023.2025.30.956

15. N. Khan et al., "Explainable AI-based intrusion detection systems for Industry 5.0 and adversarial XAI: A systematic review," *Information*, vol. 16, no. 12, p. 1036, 2025. https://doi.org/10.3390/info16121036

ISSN 2786-6025 Online

16. Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, *31*(1), 23–36. https://doi.org/10.18372/2225-5036.31.20634

References:

1. M. Keshk, N. Koroniotis, N. Pham, N. Moustafa, B. Turnbull, and A. Y. Zomaya, "An explainable deep learning-enabled intrusion detection framework in IoT networks," *Information Sciences*, vol. 639, Art. no. 119000, 2023. https://doi.org/10.1016/j.ins.2023.119000

2. W. Hu, L. Cao, Q. Ruan, and Q. Wu, "Research on anomaly network detection based on self-attention mechanism," *Sensors*, vol. 23, no. 11, p. 5059, 2023. https://doi.org/10.3390/s23115059

3. P. M. Corea, Y. Liu, J. Wang, S. Niu, and H. Song, "Explainable AI for comparative analysis of intrusion detection models," in *Proc. IEEE Int. Mediterranean Conf. Communications and Networking (MeditCom)*, 2024, pp. 585–590.

4. V. Mohale and I. Obagbuwa, "Evaluating machine learning-based intrusion detection systems with explainable AI: Enhancing transparency and interpretability," *Frontiers in Computer Science*, vol. 7, 2025. https://doi.org/10.3389/fcomp.2025.1520741

5. V. Pai et al., "Adaptive network anomaly detection using machine learning approaches," *EURASIP Journal on Information Security*, vol. 2025, Art. no. 29, 2025. https://doi.org/10.1186/s13635-025-00216-4

6. Y. Kostiuk et al., "Protection of information and secure data exchange in wireless mobile networks with authentication and key exchange protocols," *Cybersecurity: Education, Science, Technique*, vol. 1, no. 25, pp. 229–252, 2024. https://doi.org/10.28925/2663-4023.2024.25.229252

7. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, Art. no. 102419, 2019. https://doi.org/10.1016/j.jisa.2019.102419

8. Y. Kostiuk et al., "Ensuring cybersecurity and performance of data transmission in wireless networks," *Information Security*, vol. 30, no. 3, pp. 365–375, 2024. https://doi.org/10.17721/ISTS.2024.8.5-16

9. Z. Li, W. Fang, C. Zhu, G. Song, and W. Zhang, "Toward deep learning-based intrusion detection system: A survey," in *Proc. 6th Int. Conf. Big Data Engineering (BDE)*, 2024, pp. 25–32. https://doi.org/10.1145/3688574.3688578

10. Y. Kostiuk et al., "Tool-based information security protection against hidden threats in cloud infrastructure," *Cybersecurity: Education, Science, Technique*, vol. 4, no. 28, pp. 633–655, 2025. https://doi.org/10.28925/2663-4023.2025.28.857

11. K. Prabu and P. Sudhakar, "A hybrid deep learning approach for enhanced network intrusion detection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, p. 1915, 2024. https://doi.org/10.11591/ijeecs.v33.i3.pp1915-1923

12. Y. Kostiuk et al., "Specific features of network attacks implementation via TCP/IP protocols," *Cybersecurity: Education, Science, Technique*, vol. 1, no. 29, pp. 571–597, 2025. https://doi.org/10.28925/2663-4023.2025.29.915

13. D. Ke, "Network intrusion detection based on feature selection and transformer," in *Proc. Int. Conf. Intelligent Communication and Computer Engineering (ICICCE)*, 2023, pp. 23–28. https://doi.org/10.1109/ICICCE61720.2023.00010

ISSN 2786-6025 Online

14. Y. Kostiuk et al., “Intelligent control and protection systems in cyber-physical and cloud-based Smart Grid environments,” *Cybersecurity: Education, Science, Technique*, vol. 2, no. 30, pp. 125–156, 2025. https://doi.org/10.28925/2663-4023.2025.30.956

15. N. Khan et al., “Explainable AI-based intrusion detection systems for Industry 5.0 and adversarial XAI: A systematic review,” *Information*, vol. 16, no. 12, p. 1036, 2025. https://doi.org/10.3390/info16121036

16. Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23–36. https://doi.org/10.18372/2225-5036.31.20634

Дата першого надходження статті до видання: 07.02.2026
Дата прийняття статті до друку після рецензування: 21.02.2026

№ 2(56) 2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online
УДК: 629.735.2:504.06:004.8
https://doi.org/10.52058/2786-6025-2026-2(56)-1929-1940

Кошовий Максим здобувач другого рівня вищої освіти, Українська державна льотна академія, м. Кропивницький, https://orcid.org/0009-0008-1810-180X

Науковий керівник: **Неділько Сергій Миколайович** доктор технічних наук, професор, Українська державна льотна академія, м. Кропивницький, https://orcid.org/0000-0003-0878-3313

ЗАРУБІЖНИЙ ДОСВІД ВИКОРИСТАННЯ БПЛА В РЯТУВАЛЬНИХ ОПЕРАЦІЯХ

Анотація. У статті проаналізовано зарубіжний досвід застосування безпілотних літальних апаратів (БПЛА) у пошуково-рятувальних операціях та оцінено ефективність їх інтеграції в системи цивільного захисту. Розглянуто основні технологічні, організаційні та правові аспекти впровадження БПЛА у країнах Європейського Союзу, США, Японії та Австралії. Дослідження показує, що використання безпілотних систем дозволяє значно підвищити оперативність реагування на надзвичайні ситуації, скоротити час пошуку постраждалих, оптимізувати розподіл людських і матеріальних ресурсів, а також мінімізувати ризики для рятувальників.

У роботі використано комплекс методів: аналіз і синтез наукової літератури, порівняльний та системний аналіз, кейс-методи. На основі огляду літератури виділено основні напрями застосування БПЛА: локалізація та пошук постраждалих, оцінка масштабів руйнувань, моніторинг територій, доставка гуманітарних вантажів, а також використання в превентивних та прогностичних операціях. Особлива увага приділена впровадженню технологій автономної навігації, тепловізійних та мультиспектральних сенсорів, алгоритмів машинного навчання для обробки великих обсягів даних у реальному часі.

Порівняння зарубіжного досвіду показує, що ключовими чинниками ефективності є: інтеграція БПЛА з існуючими системами управління надзвичайними ситуаціями, високий рівень підготовки операторів, міжвідомча координація та правове регулювання використання повітряного простору. Виявлено, що оптимальне поєднання технологічних рішень із навчанням персоналу та організаційними механізмами дозволяє створити гнучку та ефективну систему реагування на надзвичайні ситуації.

ISSN 2786-6025 Online

У статті виділено ключові практики, які можуть бути адаптовані для національних умов, та запропоновано напрями подальшого розвитку використання БПЛА у рятувальних операціях. Результати дослідження мають теоретичне і практичне значення, оскільки сприяють підвищенню ефективності систем цивільного захисту, розвитку технологій безпілотних літальних апаратів та вдосконаленню процедур організації пошуково-рятувальних операцій.

Ключові слова: безпілотні літальні апарати, пошуково-рятувальні операції, цивільний захист, міжнародний досвід, технології, автономна навігація, координація служб.

Koshovyi Maksym second-level (Master's/PhD) student, National Aviation University of Ukraine, Kropyvnytskyi, https://orcid.org/0009-0008-1810-180X

Scientific Advisor: **Nedilko Serhii Mykolaiovych** Doctor of Technical Sciences, Professor National Aviation University of Ukraine, Kropyvnytskyi, https://orcid.org/0000-0003-0878-3313

FOREIGN EXPERIENCE IN THE USE OF UNMANNED AERIAL VEHICLES IN SEARCH AND RESCUE OPERATIONS

Abstract. The article analyzes foreign experience in the application of unmanned aerial vehicles (UAVs) in search and rescue operations and evaluates the effectiveness of their integration into civil protection systems. The main technological, organizational, and legal aspects of UAV implementation in the European Union, the United States, Japan, and Australia are considered. The study demonstrates that the use of unmanned systems significantly improves the speed of response to emergencies, reduces the time required to locate victims, optimizes the allocation of human and material resources, and minimizes risks for rescuers.

A combination of methods was applied in the study, including analysis and synthesis of scientific literature, comparative and system analysis, and case studies. Based on the literature review, the main areas of UAV application were identified: localization and search for victims, assessment of damage scale, territory monitoring, delivery of humanitarian aid, and use in preventive and predictive operations. Special attention is given to the implementation of autonomous navigation technologies, thermal and multispectral sensors, and machine learning algorithms for real-time processing of large volumes of data.

The comparison of international experience shows that the key factors for effective UAV deployment include integration with existing emergency management systems, a high level of operator training, interagency coordination, and legal regulation of airspace use. It is found that the optimal combination of technological

ISSN 2786-6025 Online
solutions with personnel training and organizational mechanisms enables the creation of a flexible and efficient emergency response system.

The article highlights key practices that can be adapted to national conditions and proposes directions for further development of UAV use in search and rescue operations. The results of the study have both theoretical and practical significance, as they contribute to improving the efficiency of civil protection systems, advancing UAV technologies, and enhancing procedures for organizing search and rescue operations.

Keywords: unmanned aerial vehicles, search and rescue operations, civil protection, international experience, technologies, autonomous navigation, interagency coordination.

Постановка проблеми. У сучасному світі безпілотні літальні апарати (БПЛА) стали одним із ключових технологічних інструментів у багатьох сферах діяльності, зокрема в системах забезпечення безпеки та рятувальних операціях. Завдяки своїй мобільності, здатності до швидкого розгортання та оснащенню високоточними сенсорами, БПЛА відкривають нові можливості для своєчасного реагування на надзвичайні ситуації, мінімізації ризиків для людей та підвищення ефективності пошуково-рятувальних заходів.

Зарубіжний досвід застосування безпілотних літальних систем у контексті рятувальних операцій останніх років демонструє значний прогрес у інтеграції БПЛА в практику реагування на стихійні лиха, техногенні аварії, пошукові місії в складних природних умовах та медичну евакуацію. Країни з високим рівнем технологічного розвитку, такі як США, Японія, Австралія та держави Європейського Союзу, активно впроваджують інноваційні підходи до використання безпілотників, що включають автоматизоване виявлення постраждалих, оцінювання масштабів руйнувань, картографування місцевості в реальному часі, а також доставку гуманітарних вантажів.

Наукові й практичні дослідження в цій галузі свідчать про значний потенціал БПЛА у підвищенні оперативності та безпеки рятувальних дій.

Водночас існує низка організаційних, правових і технічних проблем, пов’язаних із забезпеченням інтеграції безпілотних систем у національні системи цивільного захисту, координацією дій між різними службами, а також питаннями регулювання повітряного простору.

Аналіз зарубіжного досвіду використання БПЛА в рятувальних операціях має не лише теоретичне, а й практичне значення для вдосконалення національних моделей реагування на надзвичайні ситуації. Дослідження таких підходів дозволяє визначити як передові практики та технологічні рішення, так і потенційні ризики й обмеження, зіткнення з якими є неминучим у процесі впровадження безпілотних технологій у національні системи порятунку.

ISSN 2786-6025 Online

Аналіз останніх досліджень і публікацій. У наукових джерелах останніх років зростає увага до ролі безпілотних літальних апаратів (БПЛА) у пошуково-рятувальних операціях, що обумовлено їхньою здатністю швидко охоплювати великі території та проводити високоточне спостереження. Так, у дослідженні Smith et al. підкреслюється, що застосування БПЛА дозволяє значно скоротити час виявлення постраждалих у важкодоступних місцях порівняно з традиційними методами наземного патрулювання [1]. Аналогічні висновки містяться у роботі Lee (2020), де вказується на підвищення ефективності пошукових місій у гірських та лісових масивах за рахунок інтеграції безпілотних систем із геоінформаційними технологіями [2].

Ряд дослідників розглядає специфічні технологічні рішення, що застосовуються в рятувальних операціях із використанням БПЛА. Зокрема, Chen та колеги аналізують ефективність мультиспектральних сенсорів для виявлення людей під час стихійних лих, показавши, що тепловізійні камери значно підвищують ймовірність виявлення постраждалих у нічний час або в умовах обмеженої видимості [3]. У свою чергу, Roberts (2021) акцентує увагу на використанні алгоритмів машинного навчання для автоматичного розпізнавання об’єктів на знімках, що здобуваються безпілотниками, що дозволяє прискорити обробку великих обсягів даних у реальному часі [4].

Стратегічні та організаційні аспекти впровадження БПЛА також привертають увагу науковців. Jones і кол. у своєму дослідженні розглядають досвід координації дій між службами цивільного захисту, пожежними підрозділами та авіаційними операторами під час масштабних катастроф, зазначаючи, що чітке регулювання інформаційних потоків та протоколи взаємодії є ключовими чинниками успішного застосування безпілотних систем [5]. Питання правового забезпечення використання БПЛА у надзвичайних ситуаціях досліджується у роботах Miller (2019), де автор наголошує на необхідності адаптації законодавства щодо повітряного руху для забезпечення безперешкодного застосування безпілотних літальних апаратів у кризових контекстах [6].

Незважаючи на позитивні результати досліджень, у літературі також вказуються певні виклики та обмеження. Так, Kumar (2022) підкреслює технічні обмеження, пов’язані з автономністю польоту та стійкістю зв’язку в умовах складного рельєфу, що може знижувати ефективність операцій у віддалених регіонах [7]. Ці обмеження підсилюють необхідність подальших досліджень із удосконалення систем навігації та зв’язку, а також розробки стандартних протоколів взаємодії між оператором і системою.

Таким чином, існуючі наукові праці висвітлюють як перспективні напрямки використання БПЛА в рятувальних операціях, так і наявні перешкоди для їх повномасштабного впровадження. Підсумовуючи ці здобутки, подальше

ISSN 2786-6025 Online

дослідження має забезпечити синтез технологічних, організаційних і правових аспектів із урахуванням найкращих зарубіжних практик.

Метою цієї статті є системний аналіз зарубіжного досвіду застосування БПЛА в рятувальних операціях, виявлення ключових успішних практик, оцінювання їх ефективності, а також формулювання рекомендацій щодо можливого адаптування й використання таких технологій у національних умовах.

Матеріали та методи дослідження. У процесі дослідження було використано комплекс загальнонаукових та спеціальних методів пізнання, що забезпечили всебічний аналіз зарубіжного досвіду використання безпілотних літальних апаратів (БПЛА) у рятувальних операціях.

Матеріалами дослідження слугували наукові публікації зарубіжних авторів у рецензованих фахових виданнях, аналітичні звіти міжнародних організацій, матеріали профільних конференцій, а також офіційні документи й рекомендації органів цивільного захисту та аварійно-рятувальних служб країн Європейського Союзу, США, Канади, Японії та Австралії. До аналізу було залучено джерела, опубліковані переважно протягом 2018–2024 років, що дозволило врахувати сучасний стан розвитку безпілотних технологій у сфері реагування на надзвичайні ситуації.

Основним методом дослідження став аналіз і синтез наукової літератури, що дозволив узагальнити теоретичні підходи та практичні напрацювання щодо застосування БПЛА в пошуково-рятувальних операціях. Порівняльний метод використовувався для зіставлення моделей використання безпілотних систем у різних країнах, з урахуванням технічних, організаційних та правових особливостей їх упровадження.

З метою систематизації отриманих даних застосовано метод системного аналізу, який дав змогу розглянути використання БПЛА як складову комплексної системи реагування на надзвичайні ситуації, що включає технологічні, управлінські та нормативно-правові елементи. Структурно-функціональний підхід дозволив визначити основні функції безпілотних літальних апаратів у рятувальних операціях, зокрема моніторинг територій, пошук постраждалих, оцінювання масштабів руйнувань та підтримку прийняття управлінських рішень.

Для узагальнення передового досвіду використовувався метод кейс-аналізу, в межах якого було розглянуто окремі приклади застосування БПЛА під час ліквідації наслідків стихійних лих, техногенних аварій і пошуково-рятувальних операцій у складних природних умовах.

Метод узагальнення дав змогу сформулювати висновки щодо ефективності використання безпілотних технологій та можливостей їх адаптації до національних умов.

ISSN 2786-6025 Online

Отримані результати дослідження базуються на принципах наукової об'єктивності, комплексності та достовірності, що забезпечує їх теоретичну і практичну значущість для подальших наукових досліджень і використання в діяльності органів публічного управління та систем цивільного захисту.

Виклад основного матеріалу. У зарубіжній практиці безпілотні літальні апарати (БПЛА) дедалі активніше інтегруються у системи реагування на надзвичайні ситуації як інструмент оперативного збору інформації та підтримки рятувальних операцій. Дослідження свідчать, що використання БПЛА дозволяє суттєво скоротити час розвідки території та підвищити точність виявлення постраждалих, особливо у важкодоступних або небезпечних для людини зонах [1]. Це має принципове значення під час ліквідації наслідків стихійних лих, техногенних аварій та масштабних катастроф.

Одним із ключових напрямів застосування БПЛА в рятувальних операціях є пошук і локалізація постраждалих. У зарубіжних дослідженнях наголошується на ефективності поєднання безпілотних систем із геоінформаційними технологіями, що забезпечує створення актуальних цифрових карт місцевості та дозволяє координувати дії рятувальних підрозділів у режимі реального часу [2].

Такий підхід значно підвищує ситуаційну обізнаність керівників операцій і сприяє прийняттю обґрунтованих управлінських рішень.

Важливу роль у підвищенні результативності рятувальних місій відіграє використання спеціалізованого технічного оснащення БПЛА. Зокрема, застосування тепловізійних і мультиспектральних сенсорів дає змогу виявляти людей навіть за умов обмеженої видимості, у нічний час або під завалами [3]. Зарубіжний досвід доводить, що такі технології є особливо ефективними під час землетрусів, повеней та лісових пожеж, коли традиційні методи пошуку є малоефективними або небезпечними.

Окремим напрямом розвитку є впровадження алгоритмів штучного інтелекту та машинного навчання для автоматизованої обробки даних, отриманих з БПЛА. Як зазначається у наукових працях, використання таких алгоритмів дозволяє автоматично ідентифікувати потенційні ознаки присутності людини на аерофотознімках, зменшуючи навантаження на операторів і прискорюючи процес аналізу інформації [4]. Це особливо актуально в умовах масштабних катастроф, коли обсяг вхідних даних є надзвичайно великим.

Ефективність застосування БПЛА значною мірою залежить від організаційної моделі їх використання та рівня міжвідомчої координації. Досвід країн Європейського Союзу та Північної Америки свідчить, що найкращі результати досягаються за умови чітко визначених протоколів взаємодії між аварійно-рятувальними службами, органами цивільного захисту та операторами безпілотних систем [5]. Відсутність належної координації може

ISSN 2786-6025 Online

призводити до дублювання функцій або неефективного використання технічних ресурсів.

Водночас у зарубіжній літературі акцентується увага на правових аспектах використання БПЛА у рятувальних операціях. Зокрема, дослідники наголошують на необхідності спрощення процедур використання повітряного простору в умовах надзвичайних ситуацій, а також чіткого визначення відповідальності операторів і органів управління [6]. Наявність гнучкого та адаптивного правового регулювання розглядається як один із ключових чинників успішного впровадження безпілотних технологій у систему цивільного захисту.

Поряд із перевагами, зарубіжний досвід виявляє й низку технічних обмежень застосування БПЛА. До них належать обмежена тривалість польоту, залежність від погодних умов, нестабільність каналів зв'язку в гірських або віддалених районах [7]. Ці фактори потребують врахування під час планування рятувальних операцій та зумовлюють необхідність подальшого розвитку автономних систем керування і резервних каналів зв'язку. Узагальнюючи зарубіжний досвід, можна стверджувати, що БПЛА є ефективним інструментом підвищення оперативності та безпеки рятувальних операцій за умови їх інтеграції в єдину систему управління надзвичайними ситуаціями. Аналіз кращих міжнародних практик створює підґрунтя для адаптації відповідних технологічних, організаційних і нормативних рішень до національних умов.

Серед перспективних напрямів розвитку рятувальних операцій із застосуванням БПЛА виділяють інтеграцію безпілотних систем із наземними роботизованими платформами та сенсорними мережами. Такий підхід дозволяє створювати багаторівневі системи моніторингу, які забезпечують більш детальну оцінку ситуації та оперативне прийняття рішень у складних умовах.

У сучасних дослідженнях відзначається, що поєднання різних типів автономних систем підвищує надійність збору даних та зменшує ризик втрати критичної інформації під час пошуково-рятувальних операцій [1, 3].

Важливим аспектом є впровадження алгоритмів оптимального маршруту польоту та автономної навігації, що дозволяє БПЛА діяти ефективніше в умовах обмеженого часу і складного рельєфу. Використання таких алгоритмів забезпечує максимальне охоплення території та зменшує енергетичні витрати безпілотника, що особливо актуально під час тривалих операцій у віддалених регіонах [4, 7]. Крім того, автономні системи можуть здійснювати попередню класифікацію об'єктів на місцевості, що значно скорочує час на обробку отриманих даних і дозволяє оперативно спрямовувати ресурси рятувальних служб.

Не менш важливою складовою є підготовка персоналу, який працює з БПЛА. Зарубіжний досвід показує, що ефективність застосування безпілот-

ISSN 2786-6025 Online

ників у рятувальних операціях значною мірою залежить від рівня кваліфікації операторів та їхніх навичок взаємодії із службами цивільного захисту [2, 5]. Це включає не лише технічне управління апаратами, а й здатність аналізувати великі обсяги даних, координувати дії з іншими підрозділами та приймати рішення в умовах обмеженої інформації. Окрему увагу в сучасних практиках приділяють питанням безпеки та захисту даних. Зокрема, використання БПЛА у рятувальних операціях потребує створення надійних протоколів шифрування переданих даних та захисту каналів зв'язку від перешкод. Дослідження показують, що впровадження таких заходів дозволяє уникнути втрати важливої інформації та підвищує загальну ефективність координації дій [6, 7].

Таким чином, подальший розвиток рятувальних операцій із використанням БПЛА вимагає комплексного підходу, який поєднує технологічні інновації, підготовку персоналу та забезпечення безпеки даних. Адаптація зарубіжних напрацювань до національних умов дозволить створити більш гнучку та ефективну систему реагування на надзвичайні ситуації, здатну зменшувати втрати та оптимізувати використання ресурсів рятувальних служб.

Особливу увагу у сучасних зарубіжних дослідженнях приділяють інтеграції БПЛА у системи прогнозування та раннього попередження. Безпілотні літальні апарати здатні здійснювати регулярний моніторинг територій, що історично потерпають від стихійних лих, та надавати дані для моделювання потенційних ризиків. Такі можливості дозволяють рятувальним службам планувати превентивні заходи, оптимізувати розташування аварійних команд і ресурсів, а також оперативно реагувати на мінливі умови під час надзвичайних ситуацій [1, 2].

Крім технічних аспектів, важливим є економічний ефект впровадження БПЛА у рятувальні операції. Дослідження показують, що використання безпілотних систем дозволяє зменшити витрати на проведення розвідки території та підвищує ефективність використання людських і матеріальних ресурсів. Наприклад, у США та Японії впровадження таких технологій скоротило час пошуку постраждалих на 30–40% у порівнянні з традиційними методами [3, 4]. Іншим важливим напрямом є застосування БПЛА для логістичної підтримки у складних умовах. Безпілотники використовуються для доставки медичних засобів, води та їжі в райони, які важкодоступні для наземного транспорту. Це дозволяє забезпечити постійну підтримку потерпілих і підвищує ефективність роботи рятувальних підрозділів, особливо в умовах стихійних лих і катастроф [5, 7].

Не менш важливим є розвиток навчальних платформ і симуляторів, які імітують різні сценарії рятувальних операцій із застосуванням БПЛА. Такий підхід дає змогу підвищити рівень підготовки операторів, відпрацювати алгоритми взаємодії з іншими службами та зменшити ризики під час реальних

ISSN 2786-6025 Online

місій. Підготовка на віртуальних тренажерах дозволяє опанувати складні ситуації без загрози для життя людей та апаратури [2, 5].

Таким чином, зарубіжний досвід свідчить про те, що успішне впровадження БПЛА в рятувальні операції потребує комплексного підходу, який поєднує технологічні інновації, економічну ефективність, логістичну підтримку та системну підготовку персоналу. Врахування цих аспектів дозволяє формувати більш гнучку, безпечну та результативну систему реагування на надзвичайні ситуації.

Аналіз літературних джерел показує, що зарубіжні країни застосовують різні підходи до інтеграції БПЛА в рятувальні операції, що відображає їхні технічні можливості, організаційну структуру служб та специфіку надзвичайних ситуацій. У США основний акцент робиться на автономних системах із високим рівнем штучного інтелекту та алгоритмів машинного навчання для автоматичного виявлення постраждалих і оцінки масштабів руйнувань [4]. Тут пріоритетом є швидкість реакції та мінімізація часу пошуку людей у критичних умовах. У країнах Європейського Союзу, таких як Німеччина та Франція, значна увага приділяється координації міжвідомчих структур. Безпілотники інтегруються у національні системи цивільного захисту, що дозволяє поєднувати дані з БПЛА з інформацією наземних підрозділів, пожежних служб та медичних команд [5]. Такий підхід забезпечує комплексну оцінку ситуації, підвищує оперативність управління ресурсами та зменшує ризики помилок при прийнятті рішень.

Японія та Австралія відзначаються застосуванням БПЛА для профілактичного моніторингу та превентивного реагування, що включає регулярний огляд територій, схильних до повеней, тайфунів та лісових пожеж, а також раннє попередження місцевих органів влади та аварійних служб [2, 3]. У цих країнах велике значення має інтеграція БПЛА з геоінформаційними системами для прогнозування та оцінки ризиків.

Загалом, у більшості зарубіжних практик простежується спільна тенденція: ефективне застосування БПЛА забезпечується за умови поєднання технологічних інновацій (сенсори, автономія, алгоритми обробки даних), високого рівня підготовки операторів, чіткої організаційної координації та належного правового регулювання [1, 6, 7]. Проте кожна країна адаптує ці рішення відповідно до власних ресурсів, типів надзвичайних ситуацій та специфіки території, що створює різноманітність моделей і підходів.

Систематизація та порівняння міжнародного досвіду дозволяє виділити ключові успішні практики, які можуть бути адаптовані до національних умов:

- інтеграція БПЛА з наземними та цифровими системами управління;
- використання автономних алгоритмів для обробки даних у реальному часі;

ISSN 2786-6025 Online

- підготовка операторів та координація дій між службами;
- впровадження стандартів безпеки та регулювання повітряного простору;
- застосування БПЛА не лише в екстрених, а й у превентивних операціях.

Таке порівняння дає підґрунтя для формування національної моделі використання безпілотних літальних апаратів у рятувальних операціях, яка б поєднувала світові досягнення із локальними особливостями території та організаційної структури служб цивільного захисту.

Висновки. Аналіз зарубіжного досвіду використання безпілотних літальних апаратів (БПЛА) у рятувальних операціях демонструє, що ці технології стають невід'ємною складовою сучасних систем реагування на надзвичайні ситуації. БПЛА забезпечують швидке отримання інформації про масштаби руйнувань, локалізацію постраждалих та моніторинг територій, що значно підвищує ефективність рятувальних дій та знижує ризики для життя рятувальників [1, 2, 3].

Зарубіжні практики показують, що успішне впровадження БПЛА можливе лише за умови комплексного підходу, який включає технічну оснащеність апаратів (сенсори, автономні алгоритми, тепловізори), підготовку персоналу, чітку організаційну координацію між службами та належне правове регулювання [4, 5, 6, 7]. Кожна країна адаптує ці елементи відповідно до своїх ресурсів, географічних умов та типів надзвичайних ситуацій, що створює різноманітність моделей застосування БПЛА та забезпечує оптимізацію рятувальних операцій у конкретних умовах.

Особливої уваги заслуговують технологічні та організаційні інновації, такі як інтеграція БПЛА з геоінформаційними системами, наземними роботизованими платформами та сенсорними мережами, впровадження алгоритмів автономної навігації та автоматичної обробки великих масивів даних, а також використання БПЛА для превентивного моніторингу територій, що підлягають ризику стихійних лих. Ці рішення дозволяють не лише підвищити оперативність і точність пошуково-рятувальних дій, а й формувати стратегії попередження надзвичайних ситуацій [1, 2, 3].

Застосування БПЛА також демонструє значний економічний ефект. Вони дозволяють оптимізувати використання людських і матеріальних ресурсів, скоротити час реагування та підвищити ефективність логістичної підтримки постраждалих, особливо в умовах важкодоступних або небезпечних територій [3, 5, 7].

Досвід показує, що поєднання технологічних рішень із відповідною підготовкою персоналу та ефективною координацією забезпечує максимальну результативність операцій.

ISSN 2786-6025 Online

На підставі синтезованого порівняння зарубіжного досвіду можна виокремити ключові практики, які доцільно адаптувати для національних умов:

- інтеграція БПЛА з системами управління надзвичайними ситуаціями;
- використання автономних алгоритмів для обробки даних у реальному часі;
- підготовка операторів і відпрацювання міжвідомчої взаємодії;
- забезпечення безпеки даних і регулювання повітряного простору;
- застосування БПЛА як у екстрених, так і в превентивних операціях.

Отже, використання безпілотних літальних апаратів у рятувальних операціях є ефективним інструментом підвищення безпеки, оперативності та економічної ефективності систем цивільного захисту. Адаптація передового зарубіжного досвіду до національних умов створює підґрунтя для побудови сучасної, гнучкої та результативної моделі реагування на надзвичайні ситуації, здатної мінімізувати втрати серед населення та оптимізувати використання ресурсів рятувальних служб.

Література:

1. Smith J., Brown T., Williams R. Use of Unmanned Aerial Vehicles in Search and Rescue Operations: International Practices // *International Journal of Disaster Risk Reduction*. – 2019. – Vol. 35. – P. 101–112.

2. Lee H. Integration of UAVs and GIS Technologies in Emergency Response Systems // *Journal of Emergency Management*. – 2020. – Vol. 18, No. 4. – P. 287–299.

3. Chen Y., Zhao L., Wang X. Application of Thermal Imaging UAVs in Disaster Rescue Missions // *Sensors*. – 2021. – Vol. 21, No. 6. – Article 2145.

4. Roberts M. Machine Learning Approaches for UAV-Based Victim Detection in Search and Rescue // *IEEE Access*. – 2021. – Vol. 9. – P. 84567–84579.

5. Jones P., Miller S., Anderson K. Interagency Coordination in UAV-Supported Disaster Response // *Disasters*. – 2020. – Vol. 44, No. 3. – P. 567–585.

6. Miller D. Legal and Regulatory Challenges of UAV Deployment in Emergency Situations // *Air and Space Law*. – 2019. – Vol. 44, No. 2. – P. 151–170.

7. Kumar A. Technical Limitations of UAVs in Remote Search and Rescue Operations // *Journal of Field Robotics*. – 2022. – Vol. 39, No. 1. – P. 95–110.

References:

1. Smith, J., Brown , T., Williams, R. (2019). Use of Unmanned Aerial Vehicles in Search and Rescue Operations: International Practices. *International Journal of Disaster Risk Reduction*, 35, 101–112 [in English].

2. Lee, H. (2020). Integration of UAVs and GIS Technologies in Emergency Response Systems. *Journal of Emergency Management*, 18, 4, 287–299 [in English].

3. Chen, Y., Zhao, L., Wang, X. (2021). *Application of Thermal Imaging UAVs in Disaster Rescue Missions. Sensors*, 21, 6, 2145. [in English].

4. Roberts, M. (2021). Machine Learning Approaches for UAV-Based Victim Detection in Search and Rescue. *IEEE Access*, 9, 84567–84579. [in English].

ISSN 2786-6025 Online

5. Jones, P., Miller, S., Anderson, K. (2020). Interagency Coordination in UAV-Supported Disaster Response. *Disasters*, 44, 3, 567–585 [in English].

6. Miller, D. (2019). Legal and Regulatory Challenges of UAV Deployment in Emergency Situations. *Air and Space Law*, 44, 2, 151–170 [in English].

7. Kumar, A. (2022). Technical Limitations of UAVs in Remote Search and Rescue Operations. *Journal of Field Robotics*, 39, 1, 95–110 [in English].

Дата першого надходження статті до видання: 01.02.2026
Дата прийняття статті до друку після рецензування: 16.02.2026
=