УДК 004.85:004.056 **DOI:** 10.31673/2412-9070.2025.047306
Н. В. ГАЛАГАН, канд. техн. наук, доцент;
ORCID: 0000-0001-8582-3126
Н. С. ХАБ'ЮК, ст. викладач;
ORCID: 0009-0005-7917-5528
К. В. ДУНАЄВСЬКИЙ, аспірант;
ORCID: 0009-0004-2078-4348
О. О. САЗОНОВ, аспірант,
ORCID: 0009-0008-1110-9120
Державний університет інформаційно-комунікаційних технологій, Київ

МАШИННЕ НАВЧАННЯ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ СУЧАСНИХ СИСТЕМ МОНІТОРИНГУ

Стаття присвячена можливостям використання машинного навчання (ML) як інноваційного інструменту в управлінні організацією або навчальним закладом. Розглянуто питання впровадження ML у системи моніторингу для підвищення ефективності управлінських процесів та прийняття рішень на основі даних. У межах дослідження проаналізовано основні типи машинного навчання, їх практичне застосування у задачах інтелектуального аналізу даних, виявлення закономірностей, прогнозування поведінки систем і суб'єктів управління. Особливий акцент зроблено на питаннях збору, очистки та обробки даних, а також важливості правильного вибору релевантних ознак, що суттєво впливають на якість моделей та достовірність результатів. Окрема увага приділяється вибору алгоритмів машинного навчання, їх адаптації до специфіки управлінських завдань та інтеграції у цифрові системи.

Ключові слова: машинне навчання; модель машинного навчання; прогнозування даних; моніторинг; навчання.

Вступ

З урахуванням стрімкого поширення технологій штучного інтелекту та машинного навчання у різних галузях суспільного та економічного життя, особливої актуальності набувають питання етичності процесів збору, зберігання та обробки даних, що слугують основою для навчання моделей. Зокрема, необхідним є проведення подальших міждисциплінарних досліджень, спрямованих на вивчення можливостей і викликів інтеграції інтелектуальних систем у діяльність малих і середніх підприємств, де ресурси для цифрової трансформації є обмеженими, а ризики впровадження особливо значущими. Такий підхід дозволяє забезпечити як технічну ефективність моделей, так і відповідність їхнього застосування етичним та правовим нормам.

Щоб зрозуміти сучасні підходи до машинного навчання, доцільно розглянуто кілька показових публікацій українських авторів. У роботі *«Моделі та методи машинного навчання для розпізнавання фейкового контенту»* (журнал «Технічна інженерія», 2023) [1], Володимир Праздніков та Інна Сугоняк аналізують алгоритми ML для виявлення фейків у медіа, наголошуючи на важливості якісних даних та комбінованих методів обробки тексту й зображень.

У публікації *«Дослідження застосування автоматизованого машинного навчання для порівняльного аналізу методів прогнозування курсу криптовалют»* (журнал «Технічна інженерія», 2024) [2], Дмитро Плечистий та Максим Сітайло розглядають потенціал AutoML-платформ для обробки фінансових даних. У центрі дослідження - нейронні мережі, які перевершують традиційні методи за точністю прогнозування. Також розглянуто переваги автоматизації моделювання, що дозволяє суттєво зменшити тривалість експериментів.

У дослідженні Олександра Бабіча, Дмитра Духа та Анни Глухової, опублікованому у «Збірнику наукових праць Військового інституту КНУ ім. Тараса Шевченка» (2019) під наз-

вою «Особливості методів машинного навчання щодо їх використання в процесі аналізу англомовних джерел» [3], автори вивчають застосування різних алгоритмів для визначення емоційного тону англомовних матеріалів. У дослідженні порівнюються наївний Байєсівський класифікатор, логістична регресія та нейронні мережі, з акцентом на здатності останніх виявляти складні текстові залежності. Робота має прикладне значення для медіааналізу в умовах інформаційної війни.

Українські дослідники активно застосовують машинне навчання у прикладних сферах, що відкриває нові можливості для інновацій та інтеграції у глобальні технологічні тренди.

Основна частина

У дослідженні здійснено поглиблений аналіз потенціалу машинного навчання як ключового компонента сучасних систем моніторингу, розглянуто принципи його застосування, сфери використання у різних галузях, а також перспективи впровадження інтелектуальних моніторингових рішень у контексті цифрової трансформації України. Дослідження охоплює весь цикл ML-моделей - від збору даних до впровадження, підкреслюючи їх роль у створенні гнучких систем управління й моніторингу.

Для розуміння концепції машинного навчання доцільно визначити ключові поняття. Data Science є міждисциплінарною галуззю, що охоплює методи аналізу й обробки даних. Машинне навчання (Machine Learning), як її складова, спрямоване на побудову моделей, здатних до самонавчання, з подальшим застосуванням у прогнозуванні поведінки користувачів, рекомендаційних системах та розпізнаванні образів [4].

В Україні раніше терміни Data Science і Machine Learning часто використовувалися взаємозамінно, але зараз відбувається їх розмежування. Однак на практиці назви посад можуть не завжди відповідати фактичним обов'язкам: посади, що вимагають компетенцій у машинному навчанні, можуть називатися Data Scientist і навпаки.

Отже, для ефективної роботи з даними необхідні знання як у галузі Data Science, так і у машинному навчанні.

Сучасні системи моніторингу представляють собою технологічно складні комплекси, що забезпечують автоматизований збір, обробку та аналіз даних у режимі реального часу. Вони знаходять застосування у різноманітних галузях і активно використовують штучний інтелект, зокрема машинне навчання, з метою підвищення точності, оперативності реагування та можливостей прогнозування.

У таблиці представлено основні сфери застосування машинного навчання у системах моніторингу. Вони класифікуються на декілька ключових типів, залежно від галузі використання. В інформаційних технологіях широко розповсюджені системи моніторингу мереж і серверів, які здійснюють контроль за продуктивністю, навантаженням і безпекою. У промисловості застосовуються системи моніторингу виробничих процесів для управління обладнанням і запобігання аварійним ситуаціям. В екології впроваджуються системи спостереження за станом повітря, води та ґрунтів для аналізу змін у навколишньому середовищі. У медицині важливими є системи моніторингу стану пацієнтів у реальному часі, що сприяють швидкій реакції на зміни показників здоров’я.

Сфери застосування машинного навчання у системах моніторингу

Галузь	Тип системи	Приклади систем	Застосування машинного навчання
IT/ Телекомунікації	Моніторинг інфраструктури	Zabbix, Prometheus, Datadog	Виявлення аномалій, передбачення навантажень, самоналаштування
Екологія	Моніторинг довкілля	AirVisual, Copernicus, IoT-датчики	Прогнозування забруднення, моделювання клімату

Промисловість	SCADA-системи, цифрові платформи	Siemens MindSphere, GE Predix	Предиктивне обслуговування, оптимізація виробництва
Охорона здоров'я	Медичні моніторингові системи	Philips IntelliVue, Apple HealthKit	Виявлення критичних станів, персоналізовані рекомендації
Безпека/ відеонагляд	Відеоаналітика	Hikvision, SenseTime, Face++	Розпізнавання облич, виявлення загроз, поведінковий аналіз
Транспорт/ логістика	Системи моніторингу транспорту	Waze, Here, Fleet Complete	Прогнозування трафіку, оптимізація маршрутів, аналіз поведінки водіїв

Таким чином, сучасні системи моніторингу є невід'ємним компонентом інфраструктури критично важливих сфер, забезпечуючи швидкий збір, обробку та аналіз інформації у режимі реального часу. Їх застосування дає можливість не тільки виявляти відхилення та потенційні ризики на ранніх стадіях, а й оптимізувати управлінські процеси, покращувати надійність роботи систем та приймати рішення на основі достовірних даних.

Протягом останніх років машинне навчання, зокрема глибоке навчання, активно використовується у сучасних системах моніторингу як один із провідних методів виявлення та дослідження зловмисного коду.

Malware Detection Systems (MDS) або системи виявлення шкідливого ПЗ слугують заключною межею у боротьбі з кіберзагрозами. Для таких систем критично важливим є забезпечення максимальної точності та ефективності виявлення. MDS часто застосовують класичні алгоритми машинного навчання, які потребують тривалого процесу вибору та вилучення ознак, що може зумовлювати похибки.

Ідентифікацію шкідливого ПЗ реалізують за допомогою моделей глибинного навчання для візуальних даних; раніше застосовували кластерні алгоритми за відсутності чітких класів. За допомогою алгоритмів кластеризації можна здійснювати поділ об'єктів у випадках, коли класи не задані наперед, а кластери повинні утворюватися на основі схожості елементів. Ці алгоритми знаходять застосування у задачах сегментації ринку, аналізі нових даних та компресії зображень. Кластерний аналіз (Data clustering) є проблемою розбиття заданого набору даних (об'єктів) таким чином, щоб кожен кластер складався з подібних об'єктів, тоді як об'єкти різних кластерів мали значні відмінності. Мета кластеризації полягає у прогнозуванні, використовуючи всю доступну інформацію, приналежності об'єктів вибірки до їхніх кластерів, формуючи таким чином ці кластери. Кластеризація застосовується для аналізу та ідентифікації характеристик, за якими можливо об'єднати об'єкти, для зменшення обсягу даних та виявлення новизни (елементів, що не входять до жодного кластера).

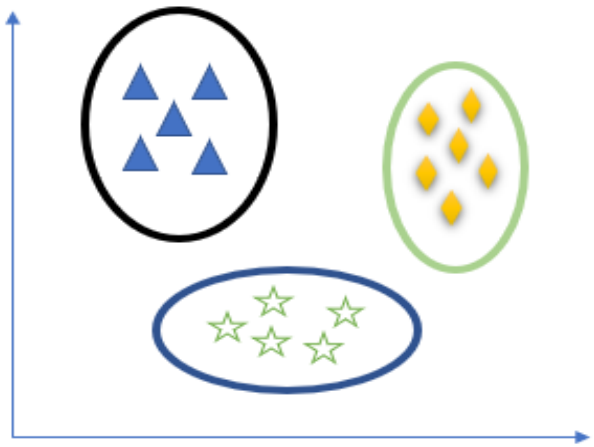

Рис. 1. Кластеризація

Кожен кластер складався із схожих об'єктів, а об'єкти різних кластерів значно відрізнялися одне від одного Шкідливе програмне забезпечення постійно еволюціонує, що значно ускладнює його виявлення та дозволяє зловмисникам ефективно обходити класичні методи кіберзахисту.

Процеси аналізу та ідентифікації внутрішньої логіки функціонування таких програм стають дедалі більш складними. Завдяки швидкому прогресу в галузі обробки даних і розвитку телекомунікацій, одна й та сама шкідлива програма здатна набувати різних структурних і семантичних варіацій, що ускладнює її розпізнавання. Враховуючи потенційну загрозу, яку несе шкідливе ПЗ для інформаційної безпеки, особливо у сфері критичної інфраструктури, досягнення максимальної точності в його виявленні, близької до абсолютної, набуває стратегічного значення. У 2011 році у праці «Malware Images: Visualization and Automatic Classification» дослідники [6] запропонували інноваційний підхід аналізу шкідливих програм, шляхом їхньої візуалізації у вигляді зображень у відтінках сірого. Метод, розроблений Натараджем з колегами, полягав у використанні виконуваних файлів, що містять шкідливий код. Необроблені бінарні дані таких файлів трансформувалися у послідовність байтів, яка далі конвертувалася у сірошкальні зображення, призначені для подальшої автоматичної класифікації (рис. 3). Візуалізація шкідливого ПЗ у вигляді зображень у градаціях сірого має низку обмежень, які пов’язані з процесом перетворення двійкових файлів у візуальний формат. Оскільки файли не мають природної двовимірної структури, їх відображення як зображень створює штучні просторові зв’язки, зокрема між пікселями у різних рядках, які не відповідають реальним потребам у коді. Уже на етапі формування зображення потрібно задати його ширину, що додає ще один параметр, який потребує оптимізації. Висота ж визначається автоматично відповідно до розміру бінарного файлу. До того ж, такий підхід створює штучні просторові кореляції між пікселями, особливо у різних рядках, які не відображають реальних зв'язків у вихідному коді. Використання шифрування або стиснення суттєво змінює внутрішню структуру виконуваного файлу, що значно ускладнює точну класифікацію. На рис. 2 показано приклади зображень, отриманих з двійкових файлів двох різних сімейств шкідливого ПЗ - Fakerean та Swizzor.gen!E. Як можна побачити, зразки одного й того ж сімейства мають схожий візуальний вигляд, тоді як програми з різних сімейств демонструють значні відмінності у своїх зображеннях. Це свідчить про те, що, попри певні недоліки методу візуалізації, такий підхід зберігає важливу інформацію, яка може бути корисною для розрізнення класів шкідливого ПЗ.

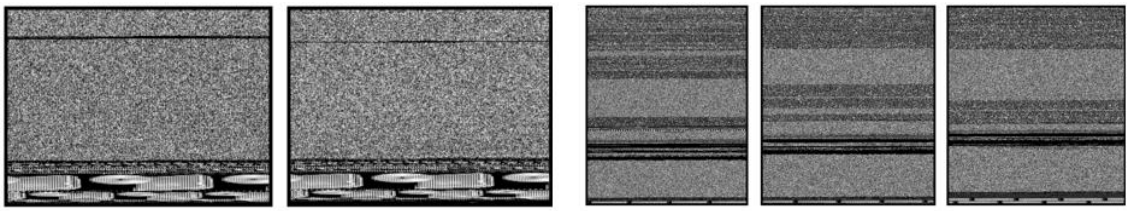

Рис. 2. Візуалізація шкідливого програмного забезпечення після конвертації з бінарних файлів:
а) сімейство шкідливих програм Fakerean;
б) сімейство шкідливих програм Swizzor.gen!E [7]

Бінарні файли шкідливого програмного забезпечення відображалися як зображення у градаціях сірого. Було встановлено, що для багатьох сімейств шкідливих програм (що належать до одного сімейства) зображення дуже схожі за оформленням та узгодженістю. Як згадувалося вище, більшість нових шкідливих програм є модифікаціями існуючих, тому їхні варіанти мають майже однаковий зміст.

Висновки

У результаті проведеного дослідження встановлено, що машинне навчання є фундаментальним компонентом сучасних систем моніторингу, здатним суттєво підвищити їхню ефективність, адаптивність і прогностичні можливості. Застосування алгоритмів машинного навчання забезпечує можливість обробки великих обсягів різнорідних даних у реальному часі, автоматичне виявлення аномалій, прогнозування критичних подій і динамічне налаштування параметрів моніторингу без втручання оператора. Це робить такі системи не лише інструментом

спостереження, а й активним засобом підтримки прийняття рішень у складних технічних, екологічних, медичних та інформаційних середовищах.

Однак, незважаючи на значні досягнення, використання машинного навчання у системах моніторингу потребує подальших міждисциплінарних досліджень, зокрема у напрямках підвищення прозорості моделей, розробки енергоефективних алгоритмів для периферійних пристроїв, забезпечення конфіденційності даних, а також інтеграції з технологіями Інтернету речей (IoT), хмарних обчислень і блокчейну.

Таким чином, машинне навчання відкриває широкі перспективи для розвитку інтелектуальних систем моніторингу нового покоління. Подальші дослідження мають бути зосереджені на поєднанні математичної строгості моделей, їхньої практичної ефективності та відповідності етичним стандартам цифрового суспільства.

В умовах зростаючої цифровізації та інтеграції до європейського науково-технологічного простору, Україна має потенціал для активного використання інтелектуальних технологій у ключових галузях - зокрема, в IT, енергетиці, медицині, агропромисловому комплексі, транспортній інфраструктурі та екологічному контролі.

Особливо актуальним є застосування машинного навчання у сфері безпеки як кібербезпеки, так і моніторингу критичних об'єктів інфраструктури, що набуває стратегічного значення в умовах військових викликів та ризиків. Крім того, українські IT-компанії демонструють високий рівень експертизи в галузі штучного інтелекту, що створює сприятливе середовище для розробки та впровадження локалізованих рішень на базі ML-алгоритмів.

Водночас необхідною передумовою успішної імплементації таких систем є підтримка з боку держави, інвестиції в інфраструктуру, стандартизація даних, а також підготовка кваліфікованих кадрів. Університети, наукові установи та бізнес мають об'єднати зусилля задля створення екосистеми інновацій, яка дозволить не лише впроваджувати готові рішення, а й формувати власні технології, конкурентоспроможні на глобальному ринку.

Список літератури

1. Празднiков В. О., Сугоняк І. І. «Моделі та методи машинного навчання для розпізнавання фейкового контенту». Журнал «Технічна інженерія» №2 (92) 2023, державний університет «Житомирська політехніка». С. 131.

2. Плечистий Д. Д., Сітайло, М. С. (2024). Дослідження застосування автоматизованого машинного навчання для порівняльного аналізу методів прогнозування курсу криптовалют. Технічна інженерія, №1(93), 218–224. https://doi.org/10.26642/ten-2024-1(93)-218-224.

3. Бабіч О., Дух Д., Глухова А. (2019). ОСОБЛИВОСТІ МЕТОДІВ МАШИННОГО НАВЧАННЯ ЩОДО ЇХ ВИКОРИСТАННЯ В ПРОЦЕСІ АНАЛІЗУ АНГЛОМОВНИХ ДЖЕРЕЛ. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, (61), 32–39. вилучено із https://miljournals.knu.ua/index.php/zbirnuk/article/view/331.

4. Харченко В. О. Основи машинного навчання. Навчальний посібник. Суми. Сумський державний університет, 2023. С. 263.

5. He K., Kim D.-S. (2019). Malware detection with malware images using deep learning techniques. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) (pp. 95-102). IEEE. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00022.

6. Nataraj. L., Karthikeyan, S., Jacob, G., & Manjunath, B.S. (2011). Malware images: Visualization and automatic classification. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (Article 4). ACM. https://doi.org/10.1145/2016904.2016908.

7. Mustafa Umut Demirezen. INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE M.U. Demirezen, Vol.10, No.2, pp.42-59.https://dergipark.org.tr/en/download/article-file/2160156.

N. Halahan, N. Khabiuk, K. Dunaievskyi, O. Sazonov

MACHINE LEARNING AS A KEY ELEMENT OF MODERN MONITORING SYSTEMS

The article is dedicated to exploring the possibilities of using machine learning (ML) as an innovative tool to enhance the efficiency of managing organizations and educational institutions. The focus is on the implementation of ML in modern monitoring systems, which enable the optimization of management processes and data-driven decision-making. The study thoroughly analyzes the main types of machine learning, including supervised, unsupervised, and reinforcement learning, as well as their practical applications in tasks such as intelligent data analysis, pattern detection, and predicting the behavior of systems and management entities. Special emphasis is placed on the issues of data collection, cleaning, and preprocessing, which are critically important for developing high-quality ML models. The importance of selecting relevant features that directly impact the accuracy and reliability of model results is highlighted. Additionally, the process of selecting and adapting machine learning algorithms to the specifics of management tasks, as well as their integration into digital systems to ensure automated monitoring and real-time data analysis, is examined.

The research covers a wide range of machine learning applications across various sectors, including information technology, industry, ecology, healthcare, security, and transportation. The article also addresses ethical and legal aspects of ML use, particularly issues of data privacy and the need for interdisciplinary research to ensure compliance with modern standards.

The analysis demonstrates that machine learning is a fundamental component of modern monitoring systems, contributing to their adaptability, forecasting accuracy, and process automation. In the context of Ukraine's digital transformation, the article emphasizes the prospects for developing intelligent monitoring systems applicable in IT, energy, healthcare, agriculture, and cybersecurity. Special attention is given to the strategic importance of ML in protecting critical infrastructure amid contemporary challenges, as well as the need for government support, data standardization, and training of qualified personnel to ensure the successful implementation of such technologies.

Keywords*:* machine learning; monitoring systems; data forecasting; data analysis; clustering; anomaly detection; malware; data visualization; digital transformation; cybersecurity.