УДК 004.421.3
DOI https://doi.org/10.32689/maup.it.2025.4.14

Наталія КІЦЕЛЬ
науковий співробітник відділу організації наукової діяльності,
Кременчуцький льотний коледж Харківського національного університету внутрішніх справ, kitselnata@gmail.com
ORCID: *0000-0003-4414-7226*
Scopus Author ID: *57406611300*

Євген ВОЛКАНІН
кандидат технічних наук, завідувач кафедри електронних комунікацій, радіотехніки та авіоніки, Кременчуцький льотний коледж Харківського національного університету внутрішніх справ, volkanin@ukr.net
ORCID: *0000-0003-3507-1987*
Scopus Author ID: *59296447700*

Оксана БОРИСЕНКО
завідувач відділення практичного навчання,
Кременчуцький льотний коледж Харківського національного університету внутрішніх справ, o.borisenko.klk@gmail.com
ORCID: *0000-0002-7858-1349*

Валерій МАТВЄЄВ
викладач кафедри електронних комунікацій, радіотехніки та авіоніки,
Кременчуцький льотний коледж Харківського національного університету внутрішніх справ, valerii.matvieiev@gmail.com
ORCID: *0009-0007-8430-2418*

Володимир МАЛЬОВАНИЙ
кандидат технічних наук, професор кафедри електронних комунікацій, радіотехніки та авіоніки, Кременчуцький льотний коледж Харківського національного університету внутрішніх справ, aireo.nv.klk@ukr.net
ORCID: *0009-0003-4900-4272*

КОМПЛЕКСНИЙ АНАЛІЗ ШКІДЛИВИХ ПРОГРАМ: ПІДХОДИ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Анотація. Метою *даного дослідження є систематизація та аналіз сучасних методів дослідження шкідливого програмного забезпечення (malware) у контексті забезпечення кібербезпеки. Робота спрямована на визначення ефективності різних підходів до аналізу шкідливого коду, виявлення їх переваг та обмежень, а також оцінку перспектив розвитку інструментів і методик для протидії еволюціонуючим кіберзагрозам. Особлива увага приділяється комплексному підходу, який передбачає поєднання традиційних і сучасних технологій, зокрема методів машинного навчання та автоматизації процесів аналізу.*

Методологія. *У роботі застосовується системний підхід до вивчення шкідливих програм, який включає статичний, динамічний та гібридний аналіз. Крім того, дослідження включає аналіз автоматизованих платформ і методів машинного навчання для класифікації та прогнозування поведінки шкідливих зразків. Практична частина базується на аналізі кейсів відомих загроз, таких як WannaCry, TrickBot та Emotet, що демонструє застосування комбінованих методів для отримання достовірних результатів.*

Наукова новизна *роботи полягає у комплексному порівнянні існуючих методів аналізу шкідливого ПЗ, виділенні їх сильних та слабких сторін у контексті сучасних загроз, а також у визначенні перспектив інтеграції традиційних підходів з інтелектуальними системами аналізу на основі машинного навчання. Дослідження підкреслює значущість використання гібридного підходу та автоматизованих лабораторних середовищ для підвищення точності та безпеки аналізу.*

Висновки. *Результати дослідження демонструють, що ефективний аналіз шкідливого ПЗ потребує поєднання статичних, динамічних та гібридних методів, застосування сучасних інструментів автоматизації та інтеграції технологій штучного інтелекту. Практичне застосування комбінованих методів дозволяє формувати цілісну картину кіберзагроз, ідентифікувати приховані механізми атак та прогнозувати потенційні ризики. Комплексний підхід до аналізу шкідливого ПЗ є ключовим елементом у системі забезпечення інформаційної безпеки, забезпечує підвищення надійності захисних механізмів та створює основу для формування стратегій протидії сучасним кіберзагрозам. Робота підкреслює необхідність постійного вдосконалення методів аналізу, розвитку міжнародного*

співробітництва та інтеграції новітніх технологій для своєчасного реагування на еволюціонуючі загрози в цифровому середовищі.

Ключові слова: *шкідливе програмне забезпечення, статичний аналіз, динамічний аналіз, гібридний аналіз, автоматизація, машинне навчання, кібербезпека.*

Nataliia KITSEL, Yevhen VOLKANIN, Oksana BORYSENKO, Valerii MATVIEIEV, Volodymyr MALOVANYI.
COMPREHENSIVE ANALYSIS OF MALWARE: APPROACHES, CHALLENGES AND PROSPECTS

Abstract. The purpose *of this study is to systematize and analyze modern methods for examining malicious software (malware) in the context of cybersecurity. The paper focuses on determining the effectiveness of different approaches to malware analysis, identifying their strengths and limitations, and assessing prospects for the development of tools and methodologies aimed at countering evolving cyber threats. Particular attention is paid to an integrated approach that combines traditional and modern technologies, including machine learning methods and automation of analysis processes.*

Methodology. *The study applies a systematic approach to malware examination, which includes static, dynamic, and hybrid analysis. In addition, the research involves the analysis of automated platforms and machine learning techniques used for classifying and predicting the behavior of malicious samples. The practical part is based on the examination of well-known threat cases such as WannaCry, TrickBot, and Emotet, which demonstrate the use of combined methods to obtain reliable and verifiable results.*

The scientific novelty *of this work lies in the comprehensive comparison of existing malware analysis methods, identification of their advantages and limitations in the context of modern cyber threats, and the determination of prospects for integrating traditional approaches with intelligent analysis systems based on machine learning. The study emphasizes the importance of employing a hybrid approach and automated laboratory environments to improve the accuracy and safety of malware analysis.*

Conclusions. *The results of the study demonstrate that effective malware analysis requires a combination of static, dynamic, and hybrid methods, the application of modern automation tools, and the integration of artificial intelligence technologies. The practical implementation of combined methods allows for forming a holistic understanding of cyber threats, identifying hidden attack mechanisms, and predicting potential risks. A comprehensive approach to malware analysis is a key element in the information security system, ensuring the reliability of protective mechanisms and forming a foundation for strategies to counter modern cyber threats. The paper underlines the necessity of continuously improving analytical methods, expanding international cooperation, and integrating advanced technologies to ensure timely responses to evolving threats in the digital environment.*

Key words: *malware, static analysis, dynamic analysis, hybrid analysis, automation, machine learning, cybersecurity.*

Вступ. Проблема протидії шкідливому програмному забезпеченню потребує застосування системного й комплексного підходу. Аналіз malware включає в себе як дослідження його внутрішньої будови та архітектури, так і вивчення поведінки в різних обчислювальних середовищах. Наразі, метою даного дослідження є опис ключових методологічних підходів, які застосовуються в сучасній практиці аналізу шкідливих програм, а також розглянути інструмент та умови проведення дослідження [8].

Статичний аналіз являє собою вивчення структури шкідливого файлу без його виконання. Основна перевага даного підходу полягає у безпеці: дослідник отримує можливість проаналізувати об'єкт без ризику зараження робочого середовища. До базових задач статичного аналізу відносяться:

– вивчення формату використовуваного файлу (PE, ELF і др.);
– виявлення імпортованих бібліотек і функцій;
– виявлення підозрілих рядків (наприклад, адрес командних серверів або зашифрованих ключів);
– вилучення вбудованих ресурсів, скриптів або прихованих даних.

Для вирішення цих задач застосовуються такі інструменти, як дизасемблери (IDA Pro, Ghidra, Radare2), утиліти аналізу бінарних файлів (PEiD, Detect It Easy), а також засоби пошуку сигнатур. Однак, статичний аналіз має свої обмеження: сучасні шкідливі програми часто використовують поліморфізм, пакувальники, шифрування коду та складні методи маскування програмного коду, що значно ускладнює їх декомпеляцію та інтерпретацію [13].

Приклади застосування статичного аналізу. При дослідженні програм-вимагачів сімейства *Ryuk* спеціалісти застосовували дизасемблер IDA Pro для вилучення фрагментів коду, відповідальних за генерацію криптографічних ключів. Аналіз імпортуємих бібліотек дозволив виявити використання криптографічного алгоритму AES в поєднанні з RSA, що вказувало на гібридну модель шифрування. Подібні знахідки дозволяють оцінити складність процедури дешифровки даних і вірогідність успішного відновлення файлів без виплати викупу.

Динамічний аналіз передбачає виконання шкідливого коду в контролюючому середовищі («пісочниці») з наступним наглядом за його поведінкою. Основні параметри, які досліджуються включають:

– взаємодію з файловою системою (створення, видалення, модифікація файлів);
– зміни системного реєстру;
– мережеву активність (звернення до IP-адрес, доменів, командним серверам);
– намагання ескалації привілеїв;
– використання міжпроцесної взаємодії.

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

Для динамічного аналізу застосовуються спеціалізовані програмні комплекси, такі як Cuckoo Sandbox, Any.Run, Joe Sandbox. Додатково використовуються монітори системних викликів (Sysinternals Suite, Process Monitor), аналізатори мережевого трафіку (Wireshark, Fiddler) та віртуальні машини (VirtualBox, VMware, QEMU). Переваги даного методу полягають у можливості виявляти фактичні дії шкідливої програми й оцінити її дію на систему. Однак, динамічний аналіз потребує значних обчислювальних ресурсів та пов'язаний з ризиками виходу шкідливого коду за межі тестового середовища при недостатній ізоляції [5, 15].

Приклади застосування динамічного аналізу. В ході вивчення зразків шкідливої програми *Emotet* дослідники використовували пісочницю Cuckoo Sandbox для відстеження мережевої активності. Було зафіксовано, що програма ініціювала з'єднання з командними серверами, розташованими в декількох країнах, й загружала додаткові модулі. Аналіз поведінки дозволив підтвердити функціонал «дропера» – попереднього завантаження, що відкриває шлях для інших шкідливих компонентів. Це демонструє, що динамічний аналіз особливо ефективний при виявленні багатоступеневих атак.

Гібридний підхід поєднує у собі елементи статичного та динамічного аналізу, дозволяє отримати найбільш повне уявлення про об'єкт дослідження. На першому етапі зазвичай застосовується статичний аналіз для виявлення загальних характеристик шкідливого файлу та побудова гіпотез про його функціонал. На другому етапі ці гіпотези перевіряються за допомогою динамічного аналізу, що дозволяє підтверджувати або спростовувати припущення про поведінку програми. Такий метод дає можливість мінімізувати обмеження кожного із підходів окремо та підвищує ефективність дослідження.

Гібридний аналіз довів свою ефективність при дослідженні банківських троянів, таких как *Zeus* або *TrickBot*. Попередній статичний аналіз дозволяє виділяти зашифровані рядки і функції роботи з мережевими протоколами, тоді як динамічний етап уточнював механізми перехвату даних користувачів. Таким чином, комбінація методів забезпечує комплексне розуміння архітектури та поведінкою шкідливого ПЗ [12].

Сучасні тенденції демонструють активне впровадження методів штучного інтелекту в аналіз шкідливого ПЗ. Машинне навчання дозволяє автоматизувати процес класифікації зразків на основі набору ознак (наприклад, послідовностей системних викликів, мережевої активності, структури бінарного коду). Дослідження нейронних мереж сприяє прогнозуванню поведінки шкідливого ПЗ, виявленню раніше невідомих загроз та скороченню часу аналізу. Однак такі методи потребують значних масивів навчальних даних і створюють ризик хибнопозитивних результатів [1, 6, 10].

Для проведення аналізу необхідно створення спеціалізованої лабораторної інфраструктури, яка забезпечить повну ізоляцію досліджуваних зразків. В її склад входять:

– сегментована мережа з можливістю моніторингу трафіка;
– віртуалізована середа для безпечного запуску підозрілих файлів;
– набір інструментів для збирання та систематизації логів;
– бази даних для зберігання інформації про проаналізовані зразки.

Застосування такої середи дозволяє мінімізувати ризики ураження робочих систем, а також забезпечує відтворюваність і надійність отриманих результатів.

Особливе значення при аналізі шкідливих програм має грамотний вибір інструментів, оскільки від цього напряму залежить глибина дослідження і точності висновків.

Останніми роками отримували розповсюдження платформи для автоматизованого аналізу, що інтегрують різні інструменти в єдину екосистему. Наприклад, система *Malware Information Sharing Platform (MISP)* забезпечує сумісне використання індикаторів компрометації між дослідниками, а *YARA* дозволяє формувати набори правил для пошуку схожих зразків шкідливого коду. Застосування таких рішень значно пришвидшує процес ідентифікації загроз та забезпечує співробітництво між різними організаціями.

Проблеми та обмеження. Не дивлячись на прогрес, дослідники стикаються з рядом викликів. По-перше, багато сучасних шкідливих програм здатні визначати факт роботи у віртуальному середовищі та змінювати свою поведінку, що знижує ефективність динамічного аналізу. По-друге, широке використання пакувальників та багаторівневого приховування коду ускладнює процес статичного аналізування. По-третє, автоматизовані системи, засновані на алгоритмах машинного навчання, схильні до загроз «отруєння даних», коли зловмисники навмисно вбудовують помилкові ознаки у навчальні вибірки.

Таким чином, ефективне дослідження шкідливих програм потребує поєднання різних методів аналізу, гнучкого вибору інструментів та постійного удосконалення лабораторних середовищ. Тільки комплексний підхід дозволить отримати достовірні результати й забезпечити надійну основу для розробки засобів протидії сучасним кіберзагрозам [14].

Результати та обговорення. В ході проведеного дослідження вдалося систематизувати основні методи аналізу шкідливого програмного забезпечення та виділити їх ключові характеристики, переваги та обмеження. Порівняльна оцінка підходів показала, що ні один із методів окремо не забезпечує повного розуміння природи загроз, а максимальна ефективність досягається при їх комбінованому використанню.

Порівняльний аналіз методів. Статичний аналіз демонструє високу швидкість отриманої первинної інформації про шкідливий об'єкт. Він дозволяє виявити підозрілі елементи коду, які імпортують бібліотеки, вбудовані рядки і структури даних. Перевагою є можливість дослідження без фактичного запуску програми, що мінімізує ризик зараження середи. Проте метод виявляється малоефективним проти сучасного шкідливого ПЗ, яке застосовує пакування, шифрування та інші механізми варіативності коду [2, 7].

Динамічний аналіз забезпечує отримання достовірних даних про поведінку шкідливої програми в реальному часі. Він дозволяє спостерігати мережеву активність, взаємодію з системою та характерні зміни в оточенні. Такий підхід незамінний для вивчення багатоступеневих атак, завантажувачів та ботнетів. Основними обмеженнями є висока ресурємність і можливість ухилення шкідливого ПЗ від виявлення у віртуалізованому середовищі [5, 7, 11].

Гібридний аналіз підтвердив свою найбільшу результативність. Використання статичного етапу дозволить виділити ключові гіпотези про функціонал шкідливого об'єкта, а динамічна перевірка забезпечує їх верифікацію. Таким чином, вдається мінімізувати недоліки окремих методів та підвищити достовірність результатів [3, 4, 7].

В рамках аналізу кейсів, описаних у відкритих джерелах, можна виділити ряд прикладів. Так, дослідження програми-вимагача *WannaCry* показало, що статичний аналіз дозволив виявити вбудовані механізми розповсюдження через вразливість SMB-протоколу, а динамічний аналіз підтвердив агресивне саморозповсюдження в локальних мережах.

Інший приклад з вивченням банківського трояну *TrickBot*. Первинний статичний аналіз виявив використання зашифрованих рядків і мережевих бібліотек, що вказало на наявність комунікації з віддаленим сервером. Динамічна перевірка показала, що програма активно збирає облікові дані користувачів, інтегруються в процеси браузерів і пересилають викрадені дані в розподільчу інфраструктуру командних серверів.

Подібні випадки підтверджують, що застосування одного методу дає лише фрагментарне уявлення, як їх комбінація формує цілісну картину атаки.

Отримані результати також дозволяють виділити ряд актуальних викликів для спеціалістів з аналізу шкідливого ПЗ. По-перше, зростає кількість зразків, оснащених механізмами протидії відлагодженню, які змінюють свою поведінку під час спроби їхнього аналізу. По-друге, дедалі ширше застосовуються методи шифрування та маскування, що дає змогу ховати шкідливий код всередині звичайних файлів або мережевого трафіку. По-третє, сервісна модель розповсюдження шкідливого ПЗ (Malware-as-a-Service) значно спрощує доступ до складних інструментів атаки, що призводить до зростання кількості інцидентів.

Окремої уваги заслуговує роль штучного інтелекту. З одного боку, алгоритми машинного навчання активно використовують для автоматичної класифікації шкідливих зразків та виявлення аномалій поведінки. З іншого боку, кіберзлочинці також впроваджують технології ШІ для генерації поліморфного коду, обходу сігнатурних систем і створення більш переконливих сценаріїв соціальної інженерії [5, 9].

Порівняльний аналіз методів (Таблиця 1) показує, що подальший розвиток доречний у напрямку інтеграції традиційних підходів з інтелектуальними системами аналізу. Застосування гібридних

Таблиця 1

Порівняльний аналіз методів

Метод аналізу	Переваги	Обмеження	Приклади застосування
Статичний	Швидкий, безпечний, не потребує запуску ПЗ	Малоефективний до обфусцированого та зашифрованого коду	Ryuk, первинний аналіз файлів
Динамічний	Відслідковування реальної поведінки, вияв мережевої активності та змін у системі	Ресурсоємний, можливий обман захисними механізмами від відладки	Emotet, WannaCry
Гібридний	Комбінує переваги статичного та динамічного аналізу, мінімізує обмеження	Потребує інтеграції інструментів та кваліфікованого персоналу	TrickBot, банківські трояни
Машинне навчання	Автоматизація, класифікація, вияв аномалій	Необхідність у великих навчальних вибірках, ризик хибнопозитивних результатів	Автоматизована класифікація зразків

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

методик в поєднанні з машинним навчанням відкриває можливість автоматизованого виявлення раніше невідомих загроз, а також скорочує час реагування на інциденти. Важливим направленням також є розвиток міжнародного співробітництва і обміну даними між дослідниками, що дозволяє оперативно реагувати на нові хвилі атак.

Таким чином, результати досліджень підтверджують, що ефективний аналіз шкідливого ПЗ повинен спиратися на комбінацію методів, використовувати сучасні інструменти автоматизації та враховувати еволюцію загроз в кіберпросторі.

Висновки. Дослідження підтверджує, що ефективний аналіз шкідливого програмного забезпечення потребує інтеграції статичних, динамічних і гібридних методів із використанням засобів автоматизації та технологій штучного інтелекту. Поєднання цих підходів забезпечує комплексне розуміння кіберзагроз, підвищує точність виявлення та зміцнює захисні механізми в системі інформаційної безпеки. Комплексний підхід до аналізу залишається ключовим чинником у формуванні адаптивних і надійних стратегій кіберзахисту.

Перспективним напрямом подальших досліджень є вдосконалення методів гібридного аналізу шкідливого програмного забезпечення, розроблення інтелектуальних самонавчальних моделей для класифікації та прогнозування поведінки шкідливих зразків, а також оптимізація автоматизованих середовищ аналізу з метою підвищення точності, швидкості та безпеки дослідницьких процесів.

Список використаних джерел:

1. Belea A.-R. Methods for Detecting Malware Using Static, Dynamic and Hybrid Analysis. *International Conference on Cybersecurity and Cybercrime*. 2023. Vol. 10(2023). https://doi.org/10.19107/CYBERCON.2023.34
2. Jusoh R., Firdaus A., Anwar S., Osman M.-Z., Darmawan M.-F., Ab Razak M.-F. Malware detection using static analysis in Android: a review of FeCO (features, classification, and obfuscation). *PeerJ Comput*. 2021. Sci. 7:e522 http://doi.org/10.7717/peerjcs.522
3. Lee, Deepak Tomar A., Verma K., Chhillar A. Hybrid Static-Dynamic Malware Analysis Framework Using Interpretable Neural Network. *International Journal of Scientific Research in Engineering and Management*. 2025. Vol. 09, Issue 09. https://doi.org/10.55041/IJSREM52505
4. Leon R. S., Kiperberg M., Zabag A. L., Zaidenberg N. Hypervisor-assisted dynamic malware analysis. *Cybersecurity*, 2021. Vol. 4, Article 19(2021). https://doi.org/10.1186/s42400-021-00083-9
5. Nafiev A. E., Rodionov A. M. Malware dynamic analyses system based on virtual machine introspection and machine learning methods. *Problems in Programming*. 2023. № 2. P. 84–90. https://doi.org/10.15407/pp2023.02.084
6. Shevchenko A., Zastelo H., Shpachinskiy Y. Analysis of application a methods of machine learning based on artificial neural networks in the tasks of detecting cybersecurity threats. *Information Technology and Security*. 2019. Vol. 7. № 1 (12). Pp. 79–90. https://doi.org/10.20535/2411-1031.2019.7.1.184327
7. Sihwail R., Omar K., Zainol Ariffin K. A. A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis. *International Journal on Advanced Science, Engineering and Information Technology*. Vol. 8, No. 4-2, Pp. 1662–1671. http://doi.org/10.18517/ijaseit.8.4-2.6827
8. Vladov S., Jotsov V., Sachenko A., Prokudin O., Ostapiuk A., Vysotska V. Neural Network Method of Analysing Sensor Data to Prevent Illegal Cyberattacks. *Sensors*. 2025, 25(17), 5235; https://doi.org/10.3390/s25175235
9. Vladov S., Vysotska V., Lytvyn V., Komziuk A., Prokudin O., Ostapiuk A. Adaptive Neural Network System for Detecting Unauthorised Intrusions Based on Real-Time Traffic Analysis. *Computation Open source preview*, 2025, 13(9), 221. https://doi.org/10.3390/computation13090221
10. Vladov S., Vysotska V., Varlakhov V., Nazarkevych M., Bolvinov S., Piadyshev,V. Innovative Method for Detecting Malware by Analysing API Request Sequences Based on a Hybrid Recurrent Neural Network for Applied Forensic Auditing. *Applied System Innovation* (ASI). 2025, 8(5), 185. DOI: 10.3390/asi8050156
11. Voskoboinyk V., Savchenko Iu., Karpukov L., Parshyna O., Prokopovych-Tkachenko, D. Assessment of the state of information security using expert systems. *Systems and Technologies*, 2024, 67(1), 72–79. https://doi.org/10.32782/2521
12. Гапон А. О. Експериментальне дослідження, програмна реалізація та оцінка ефективності застосування методу захисту програмного забезпечення на основі гібридного аналізу. *Сучасний захист інформації*. № 3(63). С. 27–36. https://doi.org/10.31673/2409-7292.2025.030422
13. Єгоров С. В., Шкварницька Т. Ю. Розширений метод аналізу шкідливого програмного забезпечення з метою створення сигнатур. *Вісник Університету «Україна»*, № 1 (24), 2020. С. 161–170. https://doi.org/10.36994/2707-4110-2020-1-28-14
14. Жульковська І., Плужник А., Жульковський О. Сучасні методи виявлення шкідливих програм. *Математичне моделювання*. 2021. №1(44). С. 46–54. https://doi.org/10.31319/2519-8106.1(44)2021.235922
15. Сініцин І., Рогушина Ю., Бова Ю. Розробка семантичних засобів підтримки процесу авторизації безпеки інформаційних систем. *Вісник Кременчуцького національного університету імені Михайла Остроградського*. Випуск 4/2025(153). С. 249–264. https://doi.org/10.32782/1995-0519.2025.4.28

Дата надходження статті: 24.11.2025
Дата прийняття статті: 10.12.2025
Опубліковано: 30.12.2025