ISSN 2219-9365

https://doi.org/10.31891/2219-9365-2026-86-49
УДК 004.056.53:004.492.3

ПЕТЛЯК Наталія
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua
МОСТОВИЙ Сергій
Хмельницький національний університет
https://orcid.org/0000-0002-9505-3206
e-mail: serhii.mostovyi@khmnu.edu.ua
СУХОВЕРКО Даніїл
Хмельницький національний університет
https://orcid.org/0009-0004-3867-004X
sukhoverkods@khmnu.edu.ua
ЗАГРЕБЕЛЬНИЙ Ростислав
Хмельницький національний університет
https://orcid.org/0009-0001-0822-2156
rostislavzagrebelnij396@gmail.com

ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТИПУ ПРОГРАМИ-ВИМАГАЧІ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS

У статті розглянуто актуальну проблему виявлення шкідливого програмного забезпечення типу програм-вимагачів. У контексті стрімкого зростання складності кіберзагроз та поширення fileless-атак, традиційні сигнатурні методи дедалі частіше демонструють недостатню ефективність, що обумовлює потребу у впровадженні більш гнучких та інтелектуальних систем виявлення. У роботі проведено комплексний огляд сучасних підходів до детектування програм-вимагачів, включаючи сигнатурні, поведінкові та гібридні рішення. На основі виявлених переваг і недоліків існуючих методів, запропоновано гібридну модель виявлення програм-вимагачів у середовищі операційної системи Windows, що поєднує динамічний моніторинг з машинним навчанням. Основою класифікації є ансамбль із двох моделей: Random Forest та Support Vector Machine із радіальним базисним ядром для виявлення нетипових відхилень. Механізм зваженого голосування дозволяє забезпечити баланс між точністю та чутливістю системи. На формальному рівні поведінка кожного процесу описується у вигляді вектора ознак. Вектори нормалізуються до інтервалу [0,1] і подаються на вхід класифікатора, який оцінює ймовірність шкідливості процесу. У разі перевищення порогового значення ініціюється блокування або ізоляція потенційно небезпечного процесу.

Ключові слова: кібербезпека; програми-вимагачі; шкідливе програмне забезпечення; динамічний аналіз; поведінкова модель; машинне навчання; Windows; моніторинг процесів; виявлення атак.

PETLIAK Natalia, MOSTOVYI Serhii,
SUKHOVERKO Daniil, ZAHREBELNYI Rostyslav
Khmelnytskyi National University

DETECTION OF RANSOMWARE MALWARE IN THE WINDOWS OPERATING SYSTEM

The rapid evolution of cyber threats has significantly increased the complexity and frequency of attacks against modern information systems, posing serious challenges to the security of governmental, corporate, and private infrastructures. Among the most destructive forms of malicious software, ransomware remains one of the most critical threats due to its ability to encrypt or block access to data and demand ransom for recovery. The widespread adoption of advanced evasion techniques—such as polymorphism, obfuscation, code injection, fileless execution, and the abuse of legitimate system processes—has considerably reduced the effectiveness of traditional signature-based detection mechanisms. Furthermore, the emergence of the Ransomware-as-a-Service (RaaS) model has accelerated the proliferation and accessibility of ransomware attacks, making them a persistent and large-scale cybersecurity problem. This paper addresses the problem of ransomware detection in the Windows operating system environment by proposing a hybrid detection model that integrates dynamic behavioral monitoring with machine learning techniques. The study begins with a comprehensive analysis of existing ransomware detection approaches, including signature-based, behavioral, and hybrid solutions. While signature-based methods offer high efficiency for known threats, they fail to detect novel or obfuscated malware variants. Behavioral approaches, on the other hand, demonstrate greater adaptability by analyzing runtime activities such as file system operations, system calls, memory usage, and network behavior, but they may suffer from increased false-positive rates. Hybrid models that combine static and dynamic analysis are therefore considered the most promising direction for achieving an optimal balance between detection accuracy and system performance. Based on this analysis, a hybrid ransomware detection framework is proposed that combines Random Forest (RF) and Support Vector Machine (SVM) classifiers with a radial basis function kernel. The model operates through continuous real-time monitoring of file system, system call, and network activities of running processes in the Windows OS. For each process, a behavioral feature vector is constructed, incorporating characteristics such as file write and rename frequency, entropy of modified files, read-to-write ratios, average time between events, and the number of unique outbound IP connections. All feature vectors are normalized to the [0,1] range before classification. The RF classifier is employed to identify typical ransomware behavior patterns based on ensemble decision trees, ensuring robustness and resistance to overfitting. Simultaneously, the SVM model focuses on detecting anomalous deviations in a high-dimensional feature space. The final classification decision is made using a weighted voting mechanism that balances the contributions of both models, allowing the system to maintain high sensitivity to malicious activity while reducing false alarms. If the computed probability of ransomware behavior exceeds a

predefined threshold, the system initiates mitigation actions such as process blocking, network isolation, and event logging. The proposed architecture consists of five main components: a file system monitoring module, a system call analysis module, a network monitoring module, a feature extraction module, and a hybrid classification module. This modular design enables efficient real-time operation and scalability for deployment in both local and large-scale corporate environments. Unlike traditional static detection systems, the proposed model can identify previously unknown ransomware variants, including zero-day and fileless attacks, by detecting deviations from normal behavioral patterns during the early stages of execution. The results of the conceptual and architectural analysis demonstrate that the proposed hybrid approach is well-suited for real-time ransomware detection in Windows environments. It provides a high level of adaptability, computational efficiency, and detection accuracy while maintaining resilience against modern evasion techniques. Future research directions include expanding the behavioral feature set, integrating real-time network traffic analysis, incorporating automated model retraining mechanisms, and exploring the use of deep learning techniques to further enhance detection capabilities.

Keywords: cybersecurity; ransomware; malware; dynamic analysis; behavioral model; machine learning; Windows; process monitoring; attack detection.

Стаття надійшла до редакції / Received 09.03.2026
Прийнята до друку / Accepted 15.04.2026
Опубліковано / Published 31.05.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасному цифровому середовищі кіберзагрози набули безпрецедентного рівня складності та поширеності, що становить виклик для інформаційної безпеки державних, корпоративних та приватних структур. Однією з найбільш агресивних форм зловмисного програмного забезпечення (ШПЗ) є програми-вимагачі — шкідливі утиліти, які блокують або шифрують доступ до інформаційних ресурсів, вимагаючи викуп за відновлення доступу. Внаслідок стрімкого поширення таких атак, кіберпростір опинився у стані постійного ризику, адже програми-вимагачі вражають не лише окремих користувачів, а й критично важливу інфраструктуру, фінансові установи, медичні заклади, органи влади та підприємства з усіх секторів економіки. Еволюція програм-вимагачів супроводжується використанням дедалі витонченіших технік обходу захисту, таких як поліморфізм, обфускація, ін'єкція коду, fileless-виконання, використання легітимних системних процесів та засобів управління операційною системою (ОС). Ці характеристики суттєво ускладнюють виявлення атак традиційними методами, зокрема антивірусами, що базуються на сигнатурному аналізі. Більше того, розвиток підходів на основі Ransomware-as-a-Service (RaaS) призвів до комерціалізації цього типу загроз. Зростання масштабів і частоти атак обумовлює потребу у формуванні нових стратегій захисту, що виходять за межі класичних парадигм. Профілактичні заходи, зокрема регулярне резервне копіювання та сегментація мережі, залишаються важливими, проте їх недостатньо для ефективної протидії атакам, які розгортаються впродовж лічених секунд. Водночас існує нагальна потреба у створенні систем, здатних працювати в режимі реального часу, виявляючи шкідливу поведінку ще на ранніх стадіях її реалізації.

У зв'язку з цим у науковій та професійній спільноті зростає інтерес до поведінкових моделей виявлення, які базуються на аналізі дій процесів, операцій у файловій системі, використання системних викликів та взаємодії з оперативною пам'яттю. Особливу увагу дослідники приділяють аналізу ознак, які важко підробити або приховати. Наприклад, характеру доступу до ресурсів, частоті операцій запису, зміні атрибутів файлів, або шаблонам динамічного виділення пам'яті. У цьому контексті аналіз низькорівневих аспектів функціонування програм, таких як послідовності інструкцій процесора, активність у пам'яті або поведінкові шаблони у взаємодії з ядром ОС, розглядається як один із найбільш перспективних підходів до ідентифікації ШПЗ. Такі методи дозволяють не лише виявити вже відомі загрози, а й реагувати на раніше не ідентифіковані варіанти атак. Окрім технічних викликів, перед сучасними системами кіберзахисту стоїть завдання збереження балансу між точністю виявлення загроз, обчислювальною ефективністю та інтерпретованістю результатів. Це особливо важливо в умовах, коли високий рівень хибнопозитивних спрацювань може призводити до порушення нормальної роботи систем або втрати довіри до автоматизованих засобів захисту. Відтак, побудова систем виявлення з високим рівнем адаптивності, здатних працювати у гетерогенних середовищах та масштабуватись для великих інфраструктур, є важливим завданням для подальших наукових досліджень.

Таким чином, проблема виявлення та запобігання атакам програм-вимагачів потребує комплексного підходу, що поєднує глибокий аналіз внутрішніх механізмів функціонування шкідливих програм із сучасними інтелектуальними засобами обробки даних. У центрі цієї проблеми є пошук ознак, що здатні ефективно диференціювати нормальну і аномальну поведінку програм, незалежно від методів маскування або змін зовнішньої структури виконуваних файлів. На основі цього постає необхідність у розробці нових концепцій виявлення, які могли б забезпечити стійкий захист інформаційних систем в умовах змінюваного та агресивного кіберсередовища.

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ

У системах виявлення та протидії програмам-вимагачам запропоновано низку рішень, які охоплюють як класичні методи сигнатурного аналізу, так і сучасні поведінкові та гібридні підходи. Традиційні антивірусні системи здебільшого покладаються на попередньо згенеровані бази сигнатур, що дозволяє швидко виявляти відомі зразки ШПЗ. Проте ефективність таких систем суттєво знижується при зіткненні з поліморфними, обфускованими або новими атаками, які не мають визначених ознак у сигнатурній базі.

Для подолання обмежень статичних методів активно розвиваються поведінкові системи виявлення, що орієнтовані на аналіз динаміки роботи програм під час їх виконання. Такі підходи фокусуються на виявленні аномальних дій, зокрема масового шифрування файлів, зміни розширень, генерації великої кількості запитів до файлової системи або використання нестандартних API-викликів. Подібні рішення демонструють вищу адаптивність і здатні виявляти раніше невідомі шаблони ШПЗ. Проте їх ефективність може бути знижена за рахунок високого рівня хибнопозитивних спрацювань, що потребує подальшої оптимізації моделей класифікації.

Окремий напрям становлять гібридні системи, які поєднують переваги сигнатурного та поведінкового підходів. Вони забезпечують баланс між швидкістю та точністю, а також знижують імовірність як пропуску загроз, так і некоректного блокування легітимних процесів. У межах таких рішень використовуються як аналіз статичних ознак коду (наприклад, хеш-функції або структурні шаблони), так і динамічні характеристики поведінки (частота операцій читання/запису, використання криптографічних бібліотек, взаємодія з ядром ОС).

В останні роки спостерігається зростання зацікавлення до аналізу процесної пам’яті як джерела поведінкових ознак ШПЗ. Цей підхід дозволяє виявляти атаки, що виконуються без створення файлів (fileless malware), та розпізнавати характерні шаблони доступу до пам’яті, виділення ресурсів, а також операції перезапису, що супроводжують шифрування. Дослідники пропонують використовувати як прямий моніторинг змін у віртуальній пам’яті, так і побудову векторів ознак для подальшої класифікації за допомогою алгоритмів машинного навчання. Аналіз областей оперативної пам’яті, де зберігаються дані та код активних процесів, дозволяє ідентифікувати аномальні дії, що відхиляються від типового функціонування системи [1]. Успішно реалізовані методи дозволяють виявляти шкідливу активність за характерними сигнатурами пам’яті [2] або за ознаками ін'єкцій коду, несанкціонованих змін в оперативній пам’яті та завантаження підозрілих модулів під час виконання [3]. Окремі підходи застосовували трасування пам’яті (memory tracing) для збору детальної інформації про виконання процесів, з акцентом на поведінкові характеристики роботи з пам’яттю [4]. Це дозволило уникнути обмежень статичних сигнатур. Такі системи стежили за динамічним розподілом пам’яті, дампами процесів і схемами виконання для виявлення нетипових дій, характерних для ШПЗ [5]. Інтеграція алгоритмів машинного навчання у процес аналізу пам’яті значно підвищила точність класифікації та зменшила кількість помилкових спрацьовувань [6]. Дослідження показали, що перехідні стани пам’яті мають відмінності між легітимним та шкідливим ПЗ, що надає додатковий рівень захисту [7]. Удосконалені методи сканування дозволили виявляти приховані або обфусковані шкідливі дії навіть за умов уникнення виявлення традиційними засобами [8]. Аналіз операцій читання-запису у пам’яті допоміг виявити унікальні сигнатури програм-вимагачів, які зберігаються лише у пам’яті під час виконання [9]. Інтеграція характеристик з оперативної пам’яті до загальних систем виявлення шкідливих програм дозволила покращити ефективність виявлення програм-вимагачів саме під час активної фази шифрування, надаючи змогу втрутитися до того, як буде завдано шкоди [10]. З часом стратегії виявлення програм-вимагачів змістили фокус з традиційних сигнатурних методів на поведінковий та евристичний аналіз [11]. Сучасні моделі орієнтуються на зміну стану системи: масові модифікації файлів, зміни в реєстрі, аномальна поведінка процесів — усе це дає змогу зафіксувати активність програм-вимагачів ще під час виконання [12]. Також увагу приділено виявленню операцій шифрування, що виявляються через аномальні дії з файловою системою, а також через нетиповий мережевий трафік, наприклад звернення до командних серверів [13]. Ще застосовуються методи моніторингу звернень до функцій ядра ОС, де фіксується відхилення у викликах системних функцій, використанні пам’яті або файлових операцій [14]. Поширеними є методи використання пісочниць, де підозрілі програми запускаються у віртуальному середовищі з метою спостереження за змінами у файловій системі, мережі та пам’яті [15]. Динамічний аналіз у таких середовищах дозволяє виявляти поведінкові особливості, зокрема шифрування, зв’язок з C2-серверами, видалення файлів тощо [16]. Зокрема, сучасні архітектури систем виявлення ШПЗ зазвичай включають компоненти моніторингу пам’яті, модулі екстракції ознак та класифікатори на основі випадкового лісу (Random Forest, RF), метод опорних векторів (SVM) або нейронних мереж.

Попри ефективність на експериментальних даних, існуючі рішення часто демонструють зниження продуктивності в умовах масштабного навантаження, зокрема в корпоративних мережах або хмарних середовищах. Додатково залишається відкритим питання оптимального балансу між швидкістю реагування системи та точністю виявлення, особливо в контексті атак, що мають нестандартну поведінку або маскуються під системні процеси.

У сучасних дослідженнях кібербезпеки спостерігається значне зростання зацікавлення до моделей

виявлення програм-вимагачів, що базуються на поведінковому аналізі та машинному навчанні. Існуючі рішення можна умовно поділити на три основні категорії: моделі на основі машинного навчання, методи аналізу поведінки та трафіку мережі, а також поєднання статичних і динамічних методів аналізу.

Одним із найпоширеніших підходів є застосування алгоритмів машинного навчання для класифікації дій, пов'язаних із програмами-вимагачами. До прикладу, у [17] представлено фреймворк Behavioral Attack Signatures Evaluation (BASE), який використовує адаптивну модель для побудови поведінкових сигнатур на основі таких ознак, як частота системних викликів, шаблони доступу до файлів і взаємодія з мережею. Цей підхід демонструє високу точність виявлення нових варіантів програм-вимагачів та знижений рівень хибнопозитивних спрацювань. Альтернативний підхід представлений в роботі [18], де зосереджено увагу на динамічному аналізі програм-вимагачів, орієнтованих на порушення конфіденційності та крадіжку даних. Автори підкреслюють зміну парадигми атак від суто шифрування до активного викрадення персональної та корпоративної інформації. Було виявлено характерні шаблони поведінки, включаючи взаємодію з серверами керування (C2), експлуатацію вразливостей мережі та використання кейлогерів. Ці знахідки свідчать про необхідність посилення контролю за мережевими каналами та застосування методів поведінкового моніторингу в реальному часі. Водночас кожен з підходів має свої обмеження. Моделі, що базуються виключно на поведінковому аналізі, можуть бути вразливими до добре замаскованих атак, які імітують легітимну активність. Статичний аналіз, незважаючи на високу швидкодію, втрачає ефективність проти поліморфних і метаморфних варіантів ШПЗ. Поєднання цих методів у гібридних фреймворках, таких як BASE чи модель SVM+RF, демонструє найвищий потенціал у сучасних умовах, забезпечуючи баланс між точністю, адаптивністю та ефективністю ресурсів.

Таким чином, аналіз наявних рішень свідчить про перевагу багаторівневих моделей, що поєднують як статичні, так і динамічні аспекти поведінки ШПЗ. Подальші дослідження мають зосередитись на автоматизованому оновленні моделей через машинне навчання, інтеграції мережевої та файлової поведінки, а також на зменшенні кількості хибних спрацювань у реальних умовах експлуатації.

ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ

З огляду на сучасні виклики, пов'язані з еволюцією програм-вимагачів, пропонується модель виявлення ШПЗ, яка поєднує динамічний поведінковий аналіз та гібридний підхід машинного навчання. Модель орієнтована на середовище ОС Windows, що є найбільш вразливою платформою в контексті атак програм-вимагачів.

В основі покладено комбіновану модель: RF для розпізнавання типових шаблонів поведінки; SVM з RF-ядром для виявлення аномалій у високовимірному просторі ознак; об'єднання відбувається за принципом зваженого голосування, що дозволяє досягти балансу між точністю та чутливістю. У якості класифікатора обрано модель RF через її здатність ефективно працювати з нелінійними та складними зв'язками між ознаками пам'яті. Цей метод формує набір дерев рішень, кожне з яких вивчає окремий аспект поведінки процесів у пам'яті. Такий підхід дозволяє моделі узагальнювати знання та ефективно працювати навіть з новими, невідомими раніше зразками програм-вимагачів. RF зменшує ризик перенавчання (overfitting) і підвищує точність класифікації завдяки голосуванню дерев при прийнятті рішень. Алгоритм був навчений на збалансованому наборі даних, що включає дампи пам'яті як шкідливих, так і легітимних процесів, що забезпечило моделі змогу ефективно розрізняти класи. Завдяки оптимізації під обчислювально-інтенсивні сценарії, модель зберігає швидкодію і може бути застосована в режимі реального часу без шкоди для якості виявлення.

Алгоритм роботи моделі:

Ініціалізація моніторингу подій файлової системи та мережі.

Збір і буферизація подій за заданий інтервал часу.

Побудова вектора ознак з отриманих подій.

Передача ознак в модуль класифікації.

Отримання ймовірності програми-вимагача.

Якщо ймовірність наявності програми-вимагача більша за порогове значення, відбувається ініціація заходів реагування, таких як блокування процесу, ізоляція мережі та ведення журналу подій.

Нехай $P = \{p_1, p_2, \dots\ p_N\}$ – множина процесів, що виконуються в ОС Windows. Для кожного процесу p ($p \in P$) протягом контрольного інтервалу часу T реєструється потік подій:

$$E_p^T = \{e_1, e_2, \dots\ e_k\}$$

$e_j \in\ \varepsilon$,

де ε – множина можливих подій, які фіксуються під час моніторингу.

На основі подій E_p^T будується вектор ознак $x_p \in R^d$, який описує поведінку процесу p. Кожна компонента вектора відповідає одній з поведінкових характеристик:

$$x_p = \left[f_{write}, f_{rename}, H_{entropy}, r_{wr}, ip_{count}, \Delta t_{avg}\right]$$

f_{write} – частота операцій запису файлів;

f_{rename} – частота операцій перейменування файлів;

$H_{entropy}$ – середня ентропія змінених файлів;
$r_{wr} = \frac{W}{R}$ – співвідношення кількості записів до читань;
ip_{count} – кількість унікальних IP-адрес для вихідних з'єднань;
Δt_{avg} – середній інтервал між подіями.
Для уніфікації шкал кожен вектор ознак нормалізується до інтервалу [0,1]:

$$x'_p = \left[\frac{x_i - \min(x_i)}{\max(x_i) - \min(x_i)}\right]_{i=1}^{d}$$

де $\min(x_i)$ та $\max(x_i)$ визначаються на основі всього навчального набору даних.
На наступному етапі виконується оцінка кожного вектора ознак за допомогою двох моделей.
Модель SVM використовує радіальне базисне ядро:

$$K(x, x') = exp(-\gamma \parallel x - x' \parallel^2)$$

Ймовірність належності до шкідливого класу визначається як:

$$P_{SVM} = \sum_{i=1}^{n_s} a_i K(x'_p, s_i)$$

де a_i – ваги підтримуючих векторів, s_i - опорні вектори, n_s - їх кількість.
RF – ансамбль із m дерев рішень, кожне з яких формує набір прогнозів $h_1(x), h_2(x), \dots, h_m(x)$. Ймовірність визначається як:

$$P_{RF} = \frac{1}{m}\sum_{j=1}^{m} h_{j(x'_p)}$$

Остаточне рішення приймається за допомогою зваженого голосування:

$$P = \alpha P_{SVM} + (1 - \alpha) P_{RF}$$

де $\alpha \in [0,1]$ – емпірично підібраний параметр вагового голосування. Якщо $P \geq \tau$, де τ – порогове значення, процес p класифікується як потенційно шкідливий (програма-вимагач).

Запропонована модель виявлення програм-вимагачів у ОС Windows ґрунтується на інтеграції динамічного поведінкового моніторингу та гібридного методу машинного навчання. Основною ідеєю є виявлення характерних аномалій у файловій та мережевій активності, які притаманні більшості сучасних форм ШПЗ, включаючи як криптовимагальні, так і шкідливі програми, орієнтовані на викрадення даних. На відміну від традиційних моделей, що переважно базуються на статичному аналізі, запропонована система здійснює моніторинг у реальному часі, ідентифікуючи шкідливу активність до моменту завершення атаки.

Архітектура системи виявлення ШПЗ типу програм-вимагачів (рис.1) складається з п'яти компонентів:

Модуль моніторингу файлової системи. Реалізується за допомогою інструментів низькорівневого спостереження (Process Monitor API). Збирає події, пов'язані з масовим створенням, перейменуванням, шифруванням або видаленням файлів.

Модуль аналізу системних викликів. Відслідковує шаблони викликів системних функцій (CreateFile, WriteFile, RegSetValue тощо), частоту їх появи та послідовність у часі.

Модуль мережевого моніторингу. Визначає підозрілу активність у мережі, таку як вихідні з'єднання до невідомих IP-адрес, встановлення з'єднань з C2-серверами, використання нестандартних протоколів чи тунелювання.

Модуль формування ознак. Генерує вектор ознак з перехоплених подій: кількість операцій запису/читання, співвідношення змінених до прочитаних файлів, ентропія файлів, частота змін розширень, тривалість сесії, використані порти тощо.

Модуль гібридної класифікації.

Початковим етапом функціонування системи є моніторинг подій у файловій системі та системних викликів, що відбуваються в ОС Windows. За допомогою інструменту Process Monitor здійснюється реєстрація подій відкриття, запису, перейменування, видалення або шифрування файлів. Одночасно відстежується частота звернень до таких системних викликів, як CreateFile, WriteFile, ReadFile, RegSetValue, що дозволяє створити хронологічний профіль поведінки процесу. Крім локальної активності, система відстежує мережеву поведінку потенційно шкідливих процесів, зокрема ініціацію вихідних з'єднань до невідомих IP-адрес, встановлення зв'язку із серверами командного управління (C2), використання нестандартних портів або спроби обходу фаєрвола. Ці дані також включаються до вектора ознак, що формує репрезентацію поведінки аналізованого процесу.

На основі зібраних даних формується багатовимірний вектор ознак який включає числові, категоріальні та часові характеристики активності. Зокрема, кожен вектор може включати такі ознаки: кількість операцій запису, кількість операцій читання, ентропія змінених файлів, частота змін розширень файлів, середній розмір змінених файлів, кількість унікальних IP-адрес для вихідного трафіку, середній час між системними викликами, та інші характеристики. Після формування векторів ознак усі процеси, що

підлягають аналізу, передаються на вхід гібридного класифікатора. Запропонований класифікатор поєднує SVM з радіальним базисним ядром і алгоритм RF, що дозволяє враховувати як нелінійні залежності між ознаками, так і логіку розгалужених дерев рішень. Своєрідність поєднання полягає у механізмі зваженого голосування, при якому обидві моделі мають відповідні ваги в загальному рішенні.

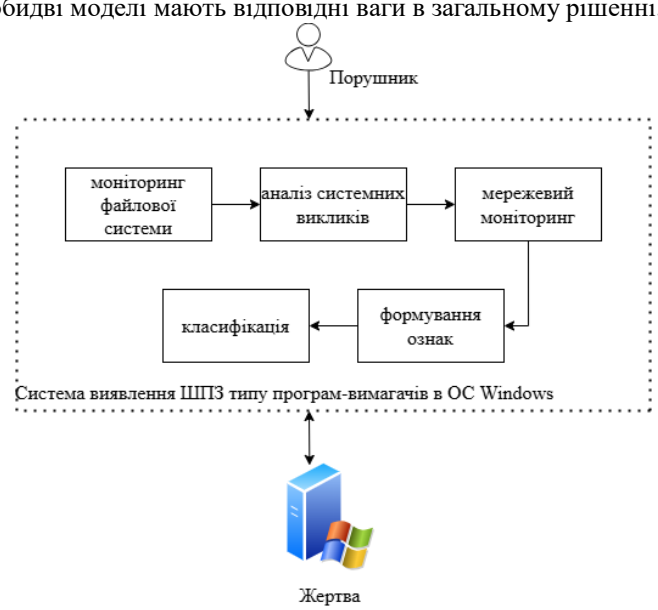

Рис. 1. Архітектура системи виявлення ШПЗ типу програм-вимагачів

Таким чином, модель постійно оновлює оцінку безпеки кожного процесу у системі, використовуючи як часову, так і семантичну інформацію про його поведінку. Перевагою цієї моделі є її здатність виявляти раніше невідомі шаблони програм-вимагачів на основі відхилень від нормальної поведінки, що дозволяє протидіяти атакам типу нульового дня. Крім того, система придатна для розгортання в реальному часі завдяки обмеженому обсягу обчислень та ефективному використанню обмеженого набору високоякісних ознак.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті проаналізовано сучасні підходи до виявлення програм-вимагачів у середовищі ОС Windows та обґрунтовано доцільність застосування гібридної моделі, що поєднує динамічний поведінковий моніторинг з методами машинного навчання. Встановлено, що традиційні сигнатурні методи демонструють низьку ефективність у виявленні нових, обфускованих або fileless-варіантів шкідливого програмного забезпечення, тоді як поведінковий аналіз дозволяє виявляти відхилення на ранніх стадіях виконання атаки. Запропонована модель базується на комбінації алгоритмів Random Forest та Support Vector Machine з радіальним базисним ядром, що дозволяє досягти високої точності класифікації при збереженні швидкодії та здатності до узагальнення. Модель використовує набір ознак, сформованих із подій файлової, мережевої та системної активності, що забезпечує комплексне представлення поведінки процесу. Введення механізму зваженого голосування між двома класифікаторами дозволило досягти балансу між чутливістю до атак та стійкістю до хибнопозитивних спрацювань. Проведений аналіз та побудована архітектура системи виявлення ШПЗ типу програм-вимагачів демонструють її практичну придатність для роботи в режимі реального часу. Вона є ефективною як у локальному середовищі, так і в умовах масштабних корпоративних інфраструктур, завдяки оптимізації обчислювальних ресурсів та здатності адаптуватися до нових загроз. Подальші дослідження доцільно спрямувати на розширення набору поведінкових ознак, інтеграцію з мережевим трафіком у реальному часі, а також автоматичне оновлення моделі на основі зворотного зв'язку. Крім того, перспективним є поєднання запропонованої моделі з методами глибокого навчання та впровадження у системи кіберзахисту наступного покоління.

References

1. Naeem M. R., Khan M., Abdullah A. M., et al. A Malware Detection Scheme via Smart Memory Forensics for Windows Devices. Mobile Information Systems. 2022. Art. 9156514. 16 p. DOI: 10.1155/2022/9156514.
2. Kwon H.-Y., Kim T., Lee M.-K. Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods. Electronics. 2022. Vol. 11, no. 6. P. 867. DOI: 10.3390/electronics11060867.
3. Hossain M. A., Islam M. S. Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity. Cybersecurity. 2024. Vol. 7, no. 16. DOI: 10.1186/s42400-024-00205-z.
4. Zgheib A., Potin O., Rigaud J.-B., Dutertre J.-M. A CFI Verification System based on the RISC-V Instruction Trace Encoder. 2022 25th Euromicro Conference on Digital System Design (DSD), Maspalomas, Spain, 2022. P. 456–463. DOI: 10.1109/DSD57027.2022.00067.
5. Mailewa A., Rozendaal K. A Novel Method for Moving Laterally and Discovering Malicious Lateral Movements in Windows

Operating Systems: A Case Study. Advances in Technology. 2022. Vol. 2, no. 3. P. 291–321. DOI: 10.31357/ait.v2i3.5584.

6. Koyirar W., Harris B., Williams J., et al. Efficient Ransomware Detection through Process Memory Analysis in Operating Systems. Authorea. 2024. DOI: 10.22541/au.172806160.00635511/v1.

7. Zhang W., Li X., Zhu T. Entropy and Memory Forensics in Ransomware Analysis: Utilizing LLaMA-7B for Advanced Pattern Recognition. TechRxiv. 2023. DOI: 10.36227/techrxiv.24742389.v1.

8. Bakar A., Kijsirikul B. Enhancing Network Visibility and Security with Advanced Port Scanning Techniques. Sensors. 2023. Vol. 23, no. 17. P. 7541. DOI: 10.3390/s23177541.

9. Woralert C., Liu C., Blasingame Z. HARD-Lite: A Lightweight Hardware Anomaly Realtime Detection Framework Targeting Ransomware. IEEE Transactions on Circuits and Systems I: Regular Papers. 2023. Vol. 70, no. 12. P. 5036–5047. DOI: 10.1109/TCSI.2023.3299532.

10. Hassin T. M., Al-rimy B. A. S., Muchtar F. B., Singh P. K. Early Detection of Crypto-Ransomware Pre-encryption Phases: A Review. Proceedings of International Conference on Recent Innovations in Computing. ICRIC 2023. Springer, Singapore, 2024. Vol. 1194. DOI: 10.1007/978-981-97-2839-8_17.

11. Taylor T., Hill N., Harrington E., et al. Dynamic Anomaly-Driven Detection for Ransomware Identification: An Innovative Approach Based on Heuristic Analysis. TechRxiv. 2024. DOI: 10.36227/techrxiv.173203089.97125949/v1.

12. Limer A., Abramovich R., Devereux G., et al. Automated Ransomware Detection Using Dynamic Behavior Trace Profiling. TechRxiv. 2024. DOI: 10.36227/techrxiv.173030558.85237080/v1.

13. Matae T., Fentiman K., Kingsleigh S., et al. Introducing Adaptive Sequence Embedding for Effective Ransomware Detection. Authorea. 2024. DOI: 10.22541/au.173161592.25153018/v1.

14. Rezvani M., Jahanshahi A., Wong D. Characterizing In-Kernel Observability of Latency-Sensitive Request-Level Metrics with eBPF. 2024 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), Indianapolis, IN, USA, 2024. P. 24–35. DOI: 10.1109/ISPASS61541.2024.00013.

15. Bashir R., Janicke H., Zeng W. Evaluating the impact of sandbox applications on live digital forensics investigation. EAI Endorsed Transactions on Security and Safety. 2021. Vol. 7, no. 25. Art. e2. DOI: 10.4108/eai.8-4-2021.169179.

16. Tarness S., Bennett M., Halloway F., et al. Introducing Dynamic Entropy Layer Profiling: A Novel Approach for Ransomware Detection through Behavioral Feature Analysis. Research Square. 2024. PREPRINT (Version 1). DOI: 10.21203/rs.3.rs-5358022/v1.

17. Anikolova E., Martins S., Rozental D., et al. Ransomware Detection Through Behavioral Attack Signatures Evaluation: A Novel Machine Learning Framework for Improved Accuracy and Robustness. TechRxiv. 2024. DOI: 10.36227/techrxiv.173092022.26611647/v1.

18. Yu R., Li P., Hu J., et al. Ransomware Detection Using Dynamic Behavioral Profiling: A Novel Approach for Real-Time Threat Mitigation. TechRxiv. 2024. DOI: 10.36227/techrxiv.173047864.44215173/v1.