УДК 004.491.42
DOI https://doi.org/10.32782/IT/2024-3-15

Олег САВЕНКО
доктор технічних наук, професор, декан факультету інформаційних технологій, Хмельницький національний університет, вул. Інститутська 11, м. Хмельницький, Україна, 29016
***ORCID:** 0000-0002-4104-745X*
***Scopus Author ID:** 54421023400*

Максим ЧАЙКОВСЬКИЙ
аспірант кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет, вул. Інститутська 11, м. Хмельницький, Україна, 29016
***ORCID:** 0000-0002-9596-6697*
***Scopus Author ID:** 57220050568*

Бібліографічний опис статті: Савенко, О, Чайковський, М. (2024). Метод нечіткої класифікації зловмисного програмного забезпечення з використанням інтелектуального агента. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 140–148, doi: https://doi.org/10.32782/IT/2024-3-15

МЕТОД НЕЧІТКОЇ КЛАСИФІКАЦІЇ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВИКОРИСТАННЯМ ІНТЕЛЕКТУАЛЬНОГО АГЕНТА

Мета дослідження: *розробка моделі інтелектуального агента в структурі мультиагентної системи для класифікації поліморфного зловмисного програмного забезпечення.* ***Методологія дослідження:*** *в зв'язку з тим, що чітко провести виявлення та класифікацію поліморфних вірусів є досить складною задачею і класифікація здійснюється в умовах невизначеності, тому вирішення даної задачі передбачає використання технологій штучного інтелекту, а саме нечіткої логіки (нечіткої класифікації).* ***Наукова новизна дослідження:*** *використання даного методу є другим етапом у запропонованому підході виявлення, аналізу та класифікації поліморфного зловмисного програмного забезпечення та передбачає використання нечіткого логічного висновку, який складається з наступних кроків: (1) визначення характеристик виявленого поліморфного зловмисного програмного забезпечення та формування дерева логічного висновку; (2) опис лінгвістичних змінних; (3) визначення функцій належності лінгвістичних термів; (4) формування бази знань системи нечіткого висновку; (5) отримання ймовірності належності досліджуваного файлу до поліморфного зловмисного програмного забезпечення різних рівнів складності; (6) нечітка класифікація поліморфних вірусів.* ***Висновки:*** *ефективність запропонованої методики, згідно проведеного експерименту, полягає в тому, що з усіх виявлених поліморфних вірусів у попередньому дослідженні (89) даний підхід дозволив здійснити їх класифікацію згідно рівнів складності (всі 89), а з 40 файлів, які не є поліморфним зловмисним програмним забезпеченням, було отримано 100 % вірних висновків. Тобто, даний підхід надав можливість із виявлених поліморфних вірусів здійснити їх класифікацію за рівнями складності із врахуванням належності до нечітких термів на рівні низький, нижче середнього, середній, вище середнього та високий, що є перевагою даного підходу. Виявлення належності поліморфного зловмисного програмного забезпечення до певного рівня складності дозволяє полегшити процес підбору необхідних методів для боротьби та їх знешкодження.*

Ключові слова: *інтелектуальний агент, мультиагентна система, поліморфне зловмисне програмне забезпечення, нечітка логіка, ймовірність, класифікація.*

Oleg SAVENKO
Doctor of Technical Sciences, Professor, Dean of the Faculty of Information Technologies, Khmelnytskyi National University, 11, Instytuts'ka Str., Khmelnytskyi, Ukraine, 29016, savenko_oleg_st@ukr.net
***ORCID:** 0000-0002-4104-745X*
***Scopus Author ID:** 54421023400*

Maksym CHAIKOVSKYI
Graduate Student at the Department of Computer Engineering and Information Systems, Khmelnytskyi National University, 11, Instytuts'ka Str., Khmelnytskyi, Ukraine, 29016, max.chaikovskyi@gmail.com
***ORCID:** 0000-0002-9596-6697*
***Scopus Author ID:** 57220050568*

To cite this article: Savenko, O, Chaikovskyi, M. (2024). Metod nechitkoi klasifikacii zlovmysnogo programnogo zabezpechennya z vykorystannyam intelektualnogo agenta [A method of fuzzy classification of malicious software using an intelligent agent]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 140–148, doi: https://doi.org/10.32782/IT/2024-3-15

A METHOD OF FUZZY CLASSIFICATION OF MALICIOUS SOFTWARE USING AN INTELLIGENT AGENT

Purpose: *development of an intelligent agent model in the structure of a multi-agent system for the classification of polymorphic malware. Research methodology: due to the fact that clearly identifying and classifying polymorphic viruses is a rather difficult task and classification is carried out under conditions of uncertainty, therefore, the solution of this problem involves the use of artificial intelligence technologies, namely fuzzy logic (fuzzy classification).* ***The scientific novelty of the study:*** *the use of this method is the second stage in the proposed approach to the detection, analysis and classification of polymorphic malware and involves the use of fuzzy logical inference, which consists of the following steps: (1) determining the characteristics of the detected polymorphic malware and forming a tree of logical inference ; (2) description of linguistic variables; (3) definition of functions belonging to linguistic terms; (4) formation of the knowledge base of the fuzzy inference system; (5) obtaining the probability of the investigated file belonging to polymorphic malware of different levels of complexity; (6) unclear classification of polymorphic viruses.* ***Conclusions:*** *the effectiveness of the proposed method, according to the conducted experiment, is that out of all detected polymorphic viruses in the previous study (89), this approach made it possible to classify them according to levels of complexity (all 89), and out of 40 files that are not polymorphic malicious software, 100% correct conclusions were obtained. That is, this approach made it possible to classify the detected polymorphic viruses by levels of complexity, taking into account belonging to vague terms at the level of low, below average, average, above average, and high, which is an advantage of this approach. Identifying the polymorphic malware belonging to a certain level of complexity makes it easier to select the necessary methods to combat and neutralize them.*

Key words: *intelligent agent, multiagent system, polymorphic malware, fuzzy logic, probability, classification.*

Актуальність проблеми. Для вирішення актуальної проблеми виявлення зловмисного програмного забезпечення (ЗПЗ) запропонована інтелектуальна мультиагентна система, відображена модель інтелектуального агента (ІА) для виявлення поліморфного ЗПЗ, а також визначення ймовірності його приналежності до різних рівнів складності поліморфних вірусів (тобто класифікація). В зв'язку з тим, що чітко провести виявлення та класифікацію поліморфних вірусів є досить складною задачею і класифікація здійснюється в умовах невизначеності, тому вирішення даної задачі передбачає використання технологій штучного інтелекту, а саме нечіткої логіки (нечіткої класифікації).

Аналіз останніх досліджень і публікацій. Поліморфний вірус відрізняється від звичайного вірусу способом маскування. Програмний код поліморфного ЗПЗ змінюється при кожному новому зараженні за допомогою шифрування. Скільки заражень – стільки й варіацій того самого вірусу. Але кожна модифікація, по суті, є новим екземпляром вірусу. У поліморфних вірусах для шифрування можна застосовувати складні криптографічні алгоритми. Тому, наприклад, антивірусний захист на основі сигнатурних баз безсилий проти просунутого поліморфного ЗПЗ. Для знешкодження поліморфних вірусів необхідне повне розшифрування їхнього «тіла» (Aboaoja et. al., 2022; Djenna et. al., 2023; Ganin et. al., 2020).

Поліморфні віруси прийнято класифікувати за рівнями поліморфізму (Nguyen, 2018). У найпростіших – олігоморфних вірусів – зустрічаються однакові ділянки коду, якими їх можна ідентифікувати за допомогою сигнатурних баз. Найскладніші з вірусів використовують пермутуючий код (permutation code): вони постійно змінюються лише на рівні підпрограм – інсталятора, шифрувальника, обробника переривань тощо. Тому досить актуальним є питання класифікації ЗПЗ (Abdullah et. al., 2023; Al-Andoli et. al., 2022; Atitallah et. al., 2022; Chaganti et. al., 2023; Goyal Manish, 2022; Qiao et. al., 2021; Vasan et. al., 2020; Xiao et. al., 2020).

Існують різні рівні складності поліморфного ЗПЗ **(**Nguyen, 2018). Рівень 1: для створення поліморфного вірусу вибирається схема з набору схем шифрування/дешифрування. Екземпляр вірусу матиме одну з цих схем у вигляді звичайного тексту. Відкритий ключ для цього шифрування можна надати багатьом користувачам для шифрування повідомлення. Це простий, так званий, «напівполіморфний» вірус. Рівень 2: процедура розшифровки вірусу містить одну або кілька постійних інструкцій, решта змінюється, алгоритм використовує змінні, наприклад, X_1 і X_2, але не змінну X_3, що дозволяє нескінченно змінювати X_3. Рівень 3: дешифрувальник вірусів містить невикористовувані функції або інструкції, такі як NOP, CLI та

STI тощо. Рівень 4: дешифратор вірусів використовує взаємозамінні інструкції та змінює їх порядок (змішування інструкцій). Рівень 5: на цьому рівні поліморфний вірус використовував усі перераховані вище методи. Крім того, алгоритм дешифрування може бути змінений. Рівень 6: перманентні віруси. Це найвищий рівень поліморфного вірусу, і його слід називати поліморфним вірусом тіла або метаморфічним вірусом. На цьому етапі весь основний код вірусу може бути змінений.

Значна кількість досліджень науковців присвячена різним методам, прийомам і підходам до аналізу та виявлення ЗПЗ (Akhtar & Feng, 2022; Chakraborty et. al., 2020; Choi et. al., 2020; Liu et. al., 2022; Lysenko et. al., 2015; Lysenko et. al., 2018; Savenko et. al., 2021).

Агент – обчислювальна система, поміщена у зовнішнє середовище, здатна взаємодіяти з нею, здійснюючи автономні раціональні дії для досягнення цілей (Ligo et. al., 2020; Taher et. al., 2023). Зазвичай для того, щоб вважатися «інтелектуальним» агент повинен мати наступні властивості: реактивність (reactivity) – агент повинен відчувати зовнішнє середовище та реагувати на зміни в ньому, здійснюючи дії, спрямовані на досягнення цілей; проактивність (pro-activeness) – агент повинен показувати керовану цілями поведінку, проявляючи ініціативу, здійснюючи дії спрямовані на досягнення цілей; соціальність (social ability) – агент повинен взаємодіяти з іншими сутностями зовнішнього середовища (іншими агентами, людьми тощо) для досягнення цілей.

Формальна модель ІА в багатоагентних системах, використовуючи дискретну математику, може бути описана як система окремих агентів, які взаємодіють один з одним. Кожен агент представлений як дискретна сутність із визначеним станом. Стан агента може змінюватися з часом відповідно до набору правил або функцій, які базуються на поточному стані агента та стані його середовища. Ці правила або функції можна виразити за допомогою різних дискретних математичних структур, таких як графіки, послідовності та набори. Наприклад, зв'язки між агентами можна представити у вигляді графа, де кожен вузол представляє агента, а кожне ребро представляє можливу взаємодію між двома агентами. Крім того, послідовність дій, які здійснює агент, можна представити як послідовність станів, де кожен стан відповідає дії. Набір усіх можливих дій для агента можна представити як набір, а стратегію агента можна визначити як функцію, яка відображає поточний стан агента на дію в цьому наборі.

Концепція багатоагентних систем (MAS) стала важливою темою інтересу в галузі штучного інтелекту (Dunets et. al., 2017; Pomorova et. al., 2013; Savenko et. al., 2020). Суть цих систем полягає в ІА, які є суб'єктами, здатними сприймати навколишнє оточення та виконувати дії самостійно або у співпраці з іншими для досягнення конкретних цілей. Формальна модель ІА, особливо коли вона побудована з використанням дискретної математики, пропонує надійну структуру для розуміння, проектування та вдосконалення цих складних систем.

Мультиагентна система, по суті, є сукупністю кількох взаємодіючих ІА. Кожен агент, у своїй найпростішій формі, є обчислювальною сутністю, яка відчуває своє оточення та реагує відповідно. Ці агенти здатні до автономної поведінки, можуть вчитися на своєму досвіді та мають здатність взаємодіяти з іншими агентами в системі.

У формальній моделі ІА зображується як окрема сутність із визначеним станом у системі. Ці стани динамічні та змінюються з часом відповідно до набору встановлених правил або функцій. Важливо, що ці правила або функції враховують поточний стан агента та конкретні умови в його середовищі.

Однією з головних переваг використання дискретної математики в цих моделях є можливість точного представлення та подальшого аналізу системи. Різноманітні структури в дискретній математиці, такі як графіки, послідовності та набори, можна ефективно використовувати для формулювання цих правил або функцій.

Наприклад, відносини між агентами всередині системи можна представити у вигляді графіка. На цьому графіку кожен вузол означає агента, а кожне ребро представляє потенційну взаємодію між двома агентами. Це візуальне представлення дозволяє чітко зрозуміти та проаналізувати взаємодію всередині системи.

Подібним чином серію дій, які виконує агент, можна представити як послідовність станів. Кожен стан у цій послідовності відповідає певній дії, яку виконує агент. Цей послідовний підхід забезпечує чітке, покрокове представлення дій агента, що дозволяє детально аналізувати та розуміти.

Крім того, повний діапазон можливих дій, доступних для агента в системі, може бути зображений як набір. Використовуючи цей підхід, ратегію агента можна визначити як функцію, яка відображає поточний стан агента на дію в цьому наборі. Цей метод забезпечує повний огляд усіх потенційних дій, сприяючи глибшому розумінню поведінки агента.

Мета дослідження. Метою дослідження є розробка моделі ІА в структурі мультиагентної системи для класифікації поліморфного ЗПЗ із використанням нечіткої логіки.

Виклад основного матеріалу дослідження. Нехай є множина файлів, які виконуються F_i, $i=\overline{1,K}$, які можуть містити зловмисні коди. Нехай є множина ІА A_j, $j=\overline{1,L}$, які мають розпізнати файли, які виконуються. Навколишнє середовище *NS* являє собою операційну систему комп'ютера, в якій взаємодіють як файли, які виконуються F_i з ІА A_j, так і ІА між собою. Передбачається, що для кожного файлу, що виконується F_i, $i=\overline{1,K}$ існує вектор ознак $S_i=\left[s_{i,1},s_{i,2},\ldots,s_{i,k}\right]$ з k елементів, який може містити зловмисні коди. У кожного ІА A_j, $j=\overline{1,L}$ також є вектор ознак $C_j=\left[c_{j,1},c_{j,2},\ldots,c_{j,l}\right]$ з l елементів, який визначає його самостійні цілі. При цьому вектори ознак і особливості програмних агентів, так і виконуваних файлів можуть відрізнятися один від одного.

Передбачається, що у ІА A_j є здатність ідентифікувати виконувані файли F_i в сенсорних областях за допомогою двовимірного масиву значень спорідненості (подібності).

$$SIM_{A_j,F_i}=\frac{1}{\left(1+P_{j,i}\right)};j=\overline{1,L};i=\overline{1,K}.,\qquad(1)$$

де $P_{j,i}=A_j-F_i$ – евклідова відстань.

Крім того, ІА також мають здатність повідомляти інформацію про виконувані файли іншим програмним агентам у комунікаційних областях. Проте, у даному дослідженні буде розглянуто окремий ІА в структурі мультиагентної системи.

Отже, задачею ІА є виявлення ЗПЗ (у даному дослідженні – поліморфного ЗПЗ), також досить важливим питанням є визначення рівня складності поліморфного ЗПЗ).

Тому необхідно розробити модель ІА для виявлення та аналізу поліморфного ЗПЗ з використанням нечіткої класифікації з метою встановлення ймовірності його належності до окремих рівнів складності поліморфних вірусів.

Розглянемо абстрактну модель ІА. У даному випадку агент будемо розглядати як набір:

$$A_j=(M_{NS},\ M_{SS},\ M_D,\ f_{ns},\ M_T,\ f_{new},\ f_{mng}),\qquad(2)$$

де M_{NS} – непуста скінчена множина станів зовнішнього навколишнього середовища;

M_{SS} – непуста скінчена множина самостійних цілей агента;

M_D – непуста скінчена множина дій агента;

$f_{ns}: M_{NS}\times M_D\rightarrow 2^{M_{NS}}$ – це функція поведінки зовнішнього навколишнього середовища, яка співставляє поточний стан зовнішнього навколишнього середовища та вибрану агентом дію непусту множину можливих наступних станів зовнішнього середовища;

M_T – непуста скінчена множина внутрішніх станів агента;

$f_{new}: M_T\times M_{NS}\rightarrow M_{NS}$ – це є функція оновлення стану, що зіставляє попереднього внутрішнього стану та нового стану зовнішнього середовища новий внутрішній стан агента;

$f_{mng}: M_T\rightarrow M_D$ є функція прийняття рішення, що зіставляє поточному внутрішньому стану агента певну дію.

У попередніх дослідженнях (Chaikovskyi et. al., 2024; Чайковський, 2024) був запропонований комплексний підхід до виявлення та аналізу поліморфного ЗПЗ. Дане дослідження є продовженням вказаних попередніх та передбачає здійснення нечіткої класифікації виявлених поліморфних вірусів згідно рівнів складності (рис. 1).

Належність поліморфного ЗПЗ до певного рівня складності описується наступною множиною: B = {Low, Low Medium, Medium, High Medium, High}.

Приймаючи елементи множини як назви нечітких змінних, їх формально можна представити наступним чином:

$$B=\{b_1,\ b_2,\ b_3,\ b_4,\ b_5\}\qquad(3)$$

Нечіткі змінні:

$$<b_i,\ X_B,\ M^i_E>;\ \text{де } M^i_E=\{x,\ \mu^i_E(x)\};$$
$$x\in X_B;\ X_B=[0;\ 100].\qquad(4)$$

На основі формули (4) введена лінгвістична змінна:

$$<\text{"Ймовірність\_належності\_ЗПЗ"},\ B,\ X_B>\qquad(5)$$

Набір функцій належності нечітких змінних (4) відображається у вигляді (рис. 2).

Таким чином, функції належності нечітких змінних мають такий узагальнений вигляд:

$$\mu^i(x)=\left\{\begin{array}{c}0,якщо\ x_i^d<x<x_i^a;\\ 1,якщо\ x_i^b\le x\le x_i^c;\\ \dfrac{x-x_i^a}{x_i^b-x_i^a},якщо\ x_i^a\le x<x_i^b;\\ \dfrac{x_i^d-x}{x_i^d-x_i^c},якщо\ x_i^c<x\le x_i^d\end{array}\right\}\qquad(6)$$

Для забезпечення високої ефективності роботи алгоритму класифікації найбільш важливим завданням є вибір області визначення функцій належності термів та способу завдання значень їхнього аргументу.

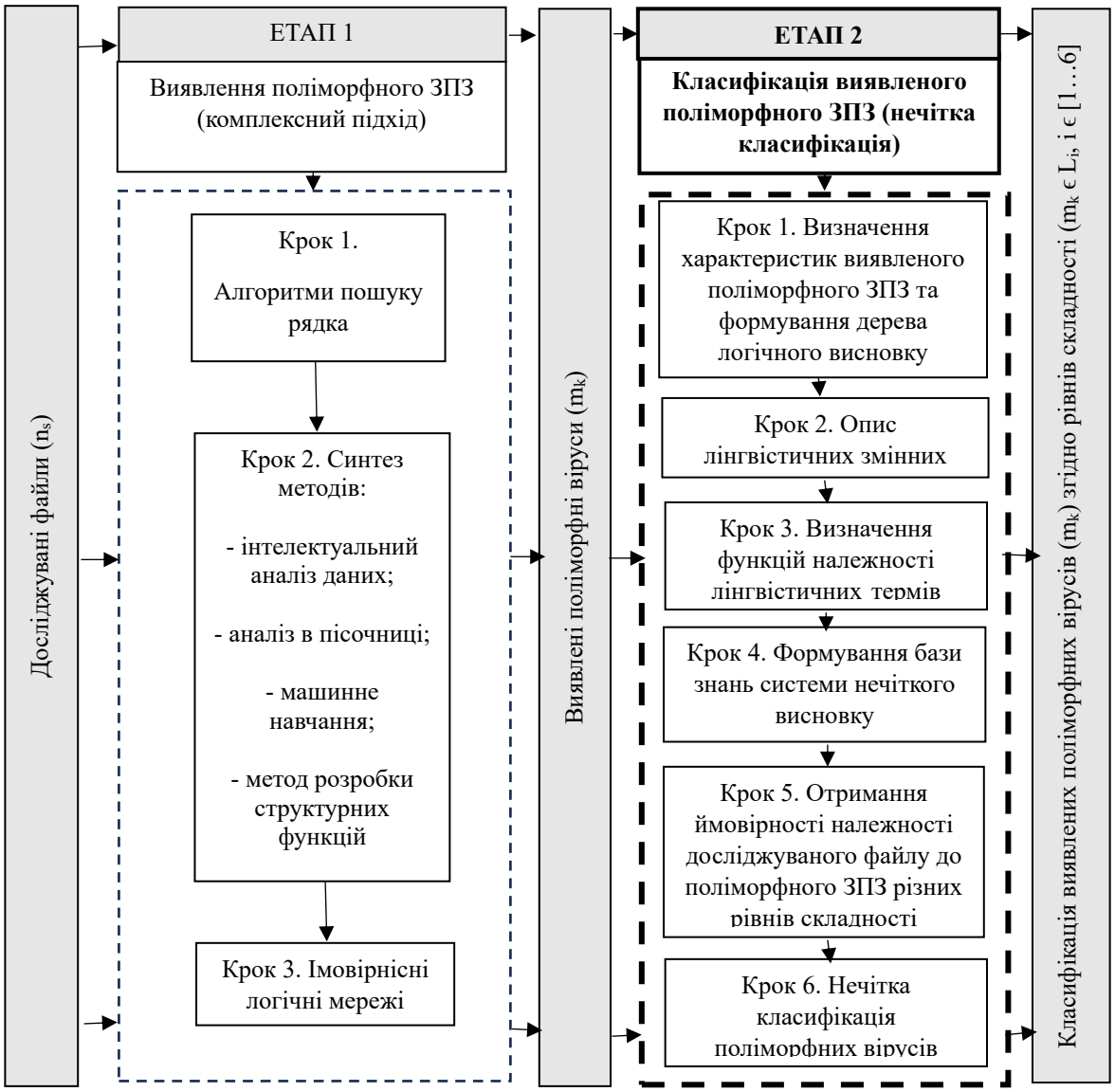

Рис. 1. Запропонований підхід для виявлення, аналізу та класифікації поліморфного ЗПЗ

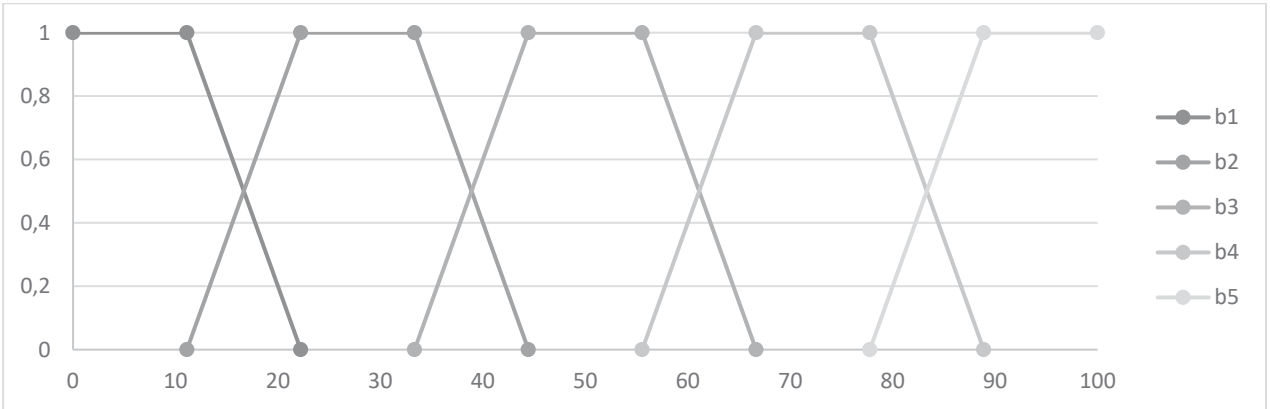

Рис. 2. Функції приналежності нечітких змінних лінгвістичної змінної ”Ймовірність_належності_ЗПЗ”

У даному дослідженні пропонується використовувати для класифікації спосіб оцінки лінгвістичної змінної, заснований на компонентах базових алгоритмів нечіткого висновку.

Також була згенерована база знань для кожного з рівнів складності поліморфного ЗПЗ, яка враховує інтерпретацію значень складових вектору ознак $S_i = \left[s_{i,1}, s_{i,2}, \ldots, s_{i,k} \right]$ у їх комплексному поєднанні для файлів, що виконуються.

В результаті використання нечіткого логічного висновку для кожного файлу, що виконується, було отримане числове значення (у %) ймовірності належності до кожного з рівнів складності поліморфного ЗПЗ.

Для визначення ефективності запропонованої методики була проведена серія експериментів. З усіх виявлених поліморфних вірусів (89) у попередньому дослідженні (Чайковський, 2024) даний підхід дозволив здійснити їх класифікацію згідно рівнів складності (всі 89). Також для перевірки надійності запропонованого підходу перевірялися файли, які не є поліморфним ЗПЗ. З 40 файлів, які не є поліморфним ЗПЗ, було отримано 100 % вірних висновків.

Нижче представлені точкові результати експерименту (таблиця 1-3).

Висновки і перспективи подальших досліджень. У дослідженні запропоновано модель ІА із використанням нечіткої класифікації для виявлення та аналізу поліморфного ЗПЗ. Ефективність запропонованої методики,

Таблиця 1

Результати експерименту для файлу, який не є поліморфним ЗПЗ

Рівень складності поліморфного зловмисного ПЗ	Розмірність універсуму (%)	Отримана ймовірність (%)	Значення функції належності для нечітких термів					Висновок
			Low	Low Medium	Medium	High Medium	High	
1	[0; 100]	0,00	0	0	0	0	0	Не є поліморфним зловмисним ПЗ
2		0,00	0	0	0	0	0	
3		0,00	0	0	0	0	0	
4		0,00	0	0	0	0	0	
5		0,00	0	0	0	0	0	
6		0,00	0	0	0	0	0	

Таблиця 2

Результати експерименту для згенерованого поліморфного ЗПЗ (варіант 1)

Рівень складності поліморфного зловмисного ПЗ	Розмірність універсуму (%)	Отримана ймовірність (%)	Значення функції належності для нечітких термів					Висновок
			Low	Low Medium	Medium	High Medium	High	
1	[0; 100]	0,00	0	0	0	0	0	Є поліморфним зловмисним ПЗ 2 рівня
2		75,00	0	0	0	1,00	0	
3		0,00	0	0	0	0	0	
4		0,00	0	0	0	0	0	
5		0,00	0	0	0	0	0	
6		0,00	0	0	0	0	0	

Таблиця 3

Результати експерименту для згенерованого поліморфного ЗПЗ (варіант 2)

Рівень складності поліморфного зловмисного ПЗ	Розмірність універсуму (%)	Отримана ймовірність (%)	Значення функції належності для нечітких термів					Висновок
			Low	Low Medium	Medium	High Medium	High	
1	[0; 100]	0,00	0	0	0	0	0	Є поліморфним зловмисним ПЗ 4 рівня
2		0,00	0	0	0	0	0	
3		0,00	0	0	0	0	0	
4		64,00	0	0	0,24	0,76	0	
5		0,00	0	0	0	0	0	
6		0,00	0	0	0	0	0	

згідно проведеного експерименту, полягає в тому, що з усіх виявлених поліморфних вірусів (89) даний підхід дозволив здійснити їх класифікацію згідно рівнів складності (всі 89), а з 40 файлів, які не є поліморфним ЗПЗ, було отримано 100 % вірних висновків. Тобто, даний підхід надав можливість виявити ті файли, які не є поліморфними вірусами, а із виявлених поліморфних вірусів здійснити їх класифікацію за рівнями складності із врахуванням належності до нечітких термів на рівні низький, нижче середнього, середній, вище середнього та високий, що є перевагою даного підходу. Виявлення належності поліморфного ЗПЗ до певного рівня складності дозволяє полегшити процес підбору необхідних методів для боротьби та їх знешкодження, у чому і полягає предмет наших подальших досліджень.

ЛІТЕРАТУРА:

1. Aboaoja F. A., Zainal A., Ghaleb F. A., Al-rimy B. A. S., Eisa T. A. E., Elnour A. A. H. Malware Detection Issues, Challenges, and Future Directions: A Survey. *Applied Sciences*. 2022. Vol. 12. № 17. P. 8482.

2. Djenna A., Bouridane A., Rubab S., Marou I.M. Artificial intelligence-based malware detection, analysis, and mitigation. *Symmetry*. 2023. Vol. 15. № 3. P. 677.

3. Ganin A., Quach P., Panwar M., Collier Z. A., Keisler J. M., Marchese D., Linkov I. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis.* 2017. Vol. 40. №. 1. P. 183–199.

4. Nguyen V.T. (2018). A study of polymorphic virus detection. URL: https://doi.org/10.13140/RG.2.2.19853.79842 (дата звернення: 15.08.2023).

5. Abdullah M. A., YuY., Adu K., Imrana Y., Wang X., Cai J. HCL-classifier: CNN and LSTM based hybrid malware classifier for internet of things (IoT). *Future Generation Computer Systems*. 2023. Vol. 142. P. 41–58.

6. Al-Andoli M. N., Tan S. C., Sim K. S., Lim C. P., Goh P. Y. Parallel deep learning with a hybrid BP-PSO framework for feature extraction and malware classification. *Applied Soft Computing*. 2022. P. 109756.

7. Atitallah S. B., Driss M., Almomani I. A novel detection and multi-classification approach for IoT-malware using random forest voting of finetuning convolutional neural networks. *Sensors*. 2022. Vol. 22. № 11. P. 4302.

8. Chaganti R., Ravi V., Pham T.D. A multi-view feature fusion approach for effective malware classification using deep learning. *Journal of Information Security and Applications*. 2023. Vol. 72. P. 103402.

9. Goyal Manish K. R. AVMCT: API Calls Visualization based Malware Classification using Transfer Learning. *Journal of Algebraic Statistics*. 2022. Vol. 13. № 1. P. 31–41.

10. Qiao Y., Zhang W., Du X., Guizani M. Malware classification based on multilayer perception and Word2Vec for IoT security. *ACM Transactions on Internet Technology (TOIT)*. 2021. Vol. 22. № 1. P. 1–22.

11. Vasan D., Alazab M., Wassan S., Naeem H., Safaei B., Zheng Q. IMCFN: Image-based malware classification using fine-tuned convolutional neural network architecture. *Computer Networks*. 2020. Vol. 171. P. 107138.

12. Xiao G., Li J., Chen Y., Li K. MalFCS: An effective malware classification framework with automated feature extraction based on deep convolutional neural networks. *Journal of Parallel and Distributed Computing*. 2020. Vol. 141. P. 49–58.

13. Akhtar M. S., Feng T. Malware Analysis and Detection Using Machine Learning Algorithms. *Symmetry (Basel)*. 2022. Vol. 14. № 11. P. 2304.

14. Chakraborty A., Kriti K., Yateendra, Bennet Praba M.S. Polymorphic Malware Detection by Image Conversion Technique. *International Journal of Engineering and Advanced Technology (IJEAT).* 2020. Vol. 9. № 3. P. 2898–2903.

15. Choi S., Bae J., Lee C., Kim Y., Kim J. Attention-based automated feature extraction for malware analysis. *Sensors (Switzerland).* 2020. Vol. 20. № 10. P. 1–17.

16. Liu S., Feng P., Wang S., Sun K., Cao J. Enhancing malware analysis sandboxes with emulated user behavior. Computers and Security. 2022. Vol. 115. P. 102613.

17. Lysenko S., Pomorova O., Savenko O., Kryshchuk A., Bobrovnikova K. (2015). DNS-based Anti-evasion Technique for Botnets Detection. *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Warsaw, Poland, 24–26 September 2015. 2015. P. 453–458.

18. Lysenko S., Savenko O., Bobrovnikova K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. *CEUR-WS*. 2018. Vol. 2104. P. 688–695.

19. Savenko B., Lysenko S., Bobrovnikova K., Savenko O., Markowsky G. Detection DNS Tunneling Botnets. *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Cracow, Poland, 22–25 September 2021. 2021.

20. Ligo A.K., Kott A., Linkov I. How to measure cyber-resilience of a system with autonomous agents: approaches and challenges. *IEEE Engineering Management Review*. 2021. Vol. 49. № 2. P. 89–97.

21. Taher F., AlFandi O., Al-kfairy M., Al Hamadi, H., Alrabaee S. DroidDetectMW: A Hybrid Intelligent Model for Android Malware Detection. *Applied Sciences.* 2023. Vol. 13. P. 7720.

22. Dunets O., Wolff C., Sachenko A., Hladiy G., Dobrotvor I. (2017). Multi-agent system of IT project plannin. *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Bucharest, 21–23 September 2017. 2017. P. 548–552.

23. Pomorova O., Savenko O., Lysenko S., Kryshchuk A. Multi-Agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic. *Communications in Computer and Information Science*. 2013. Vol. 370. P. 243–254.

24. Savenko O., Sachenko A., Lysenko S., Markowsky G., Vasylkiv N. Botnet Detection Approach based on the Distributed Systems. *International Journal of Computing*. 2020. Vol. 19. № 2. P. 190–198.

25. Chaikovskyi M., Chaikovska I., Sochor T., Martyniuk I., Lyhun O. Comprehensive approach to the detection and analysis of polymorphic malware. *CEUR-WS*. 2024. Vol. 3736. P. 312–323.

26. Чайковський М. Ю. Комплексний підхід до виявлення та аналізу поліморфного зловмисного програмного забезпечення. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2024. № 2. С. 42–50.

REFERENCES:

1. Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., Elnour, A. A. H. (2022). Malware Detection Issues, Challenges, and Future Directions: A Survey. Applied Sciences. 12(17). https://doi.org/10.3390/app12178482

2. Djenna, A., Bouridane, A., Rubab, S., Marou, I.M. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. Symmetry, 15(3), 677. https://doi.org/10.3390/sym15030677

3. Ganin, A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Analysis, 40(1), 183–199. https://doi.org/10.1111/risa.12891

4. Nguyen, V. T. (2018). A study of polymorphic virus detection. https://doi.org/10.13140/RG.2.2.19853.79842

5. Abdullah, M. A., Yu, Y., Adu, K., Imrana, Y., Wang, X., Cai, J. (2023). HCL-classifier: CNN and LSTM based hybrid malware classifier for internet of things (IoT). Future Generation Computer Systems, 142, 41–58. https://doi.org/10.1016/j.future.2022.12.034

6. Al-Andoli, M. N., Tan, S. C., Sim, K. S., Lim, C. P., Goh, P. Y. (2022). Parallel deep learning with a hybrid BP-PSO framework for feature extraction and malware classification. Applied Soft Computing, 131, 109756. https://doi.org/10.1016/j.asoc.2022.109756

7. Atitallah, S. B., Driss, M., Almomani, I. (2022). A novel detection and multi-classification approach for IoT-malware using random forest voting of finetuning convolutional neural networks. Sensors, 22(11), 4302. https://doi.org/10.3390/s22114302

8. Chaganti, R., Ravi, V., Pham, T. D. (2023). A multi-view feature fusion approach for effective malware classification using deep learning. Journal of Information Security and Applications, 72, 103402. https://doi.org/10.1016/j.jisa.2022.1034

9. Goyal Manish, K. R. (2022). AVMCT: API Calls Visualization based Malware Classification using Transfer Learning. Journal of Algebraic Statistics, 13(1), 31–41. https://doi.org/10.52783/jas.v13i1.59

10. Qiao, Y., Zhang, W., Du, X., Guizani, M. (2021). Malware classification based on multilayer perception and Word2Vec for IoT security. ACM Transactions on Internet Technology (TOIT), 22(1), 1–22. https://doi.org/10.1145/343675

11. Vasan, D., Alazab, M., Wassan, S., Naeem, H., Safaei, B., Zheng, Q. (2020). IMCFN: Image-based malware classification using fine-tuned convolutional neural network architecture. Computer Networks, 171, 107138. https://doi.org/10.1016/j.comnet.2020.107138

12. Xiao, G., Li, J., Chen, Y., Li, K. (2020). MalFCS: An effective malware classification framework with automated feature extraction based on deep convolutional neural networks. Journal of Parallel and Distributed Computing, 141, 49–58. https://doi.org/10.1016/j.jpdc.2020.03.012

13. Akhtar, M. S., Feng, T. (2022). Malware Analysis and Detection Using Machine Learning Algorithms. Symmetry (Basel), 14(11), 2304. https://doi.org/10.3390/sym14112304

14. Chakraborty, A., Kriti, K., Yateendra, Bennet Praba, M.S. (2020). Polymorphic Malware Detection by Image Conversion Technique. International Journal of Engineering and Advanced Technology (IJEAT), 9 (3), 2898–2903. https://doi.org/10.35940/ijeat.B4999.029320

15. Choi, S., Bae, J., Lee, C., Kim, Y., Kim, J. (2020). Attention-based automated feature extraction for malware analysis. Sensors (Switzerland), 20(10), 1–17. https://doi.org/10.3390/s20102893

16. Liu, S., Feng, P., Wang, S., Sun, K., Cao, J. (2022). Enhancing malware analysis sandboxes with emulated user behavior. Computers and Security, 115, 102613. https://doi.org/10.1016/j.cose.2022.102613

17. Lysenko, S., Pomorova, O., Savenko, O., Kryshchuk, A., Bobrovnikova, K. (2015). DNS-based Anti-evasion Technique for Botnets Detection. In Proc. of the 8-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Warsaw, Poland, 453–458.

18. Lysenko, S., Savenko, O., Bobrovnikova, K. (2018). DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. CEUR-WS, 2104, 688–695.

19. Savenko, B., Lysenko, S., Bobrovnikova, K., Savenko, O., Markowsky, G. (2021). Detection DNS Tunneling Botnets. In Proc. of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IDAACS'2021, Cracow, Poland.

20. Ligo, A.K., Kott, A., Linkov, I. (2021). How to measure cyber-resilience of a system with autonomous agents: approaches and challenges. IEEE Engineering Management Review, 49(2), 89–97. https://doi.org/10.1109/EMR.2021.3074288

21. Taher, F., AlFandi, O., Al-kfairy, M., Al Hamadi, H., Alrabaee, S. (2023). DroidDetectMW: A Hybrid Intelligent Model for Android Malware Detection. Applied Sciences, 13, 7720. https://doi.org/10.3390/app13137720

22. Dunets, O., Wolff, C., Sachenko, A., Hladiy, G., Dobrotvor, I. (2017). Multi-agent system of IT project plannin". In Proc. of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, Romania, 548–552. https://doi.org/10.1109/IDAACS.2017.8095141

23. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A. (2013). Multi-Agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic. Communications in Computer and Information Science, 370, 243–254. https://doi.org/10.1007/978-3-642-38865-1_16

24. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., Vasylkiv, N. (2020). Botnet Detection Approach based on the Distributed Systems. International Journal of Computing, 19(2), 190–198. https://doi.org/10.47839/ijc.19.2.1761

25. Chaikovskyi M., Chaikovska I., Sochor T., Martyniuk I., Lyhun O. (2024). Comprehensive approach to the detection and analysis of polymorphic malware. CEUR Workshop Proceedings, 3736, 312–323. Retrieved from: https://ceur-ws.org/Vol-3736/paper23.pdf

26. Chaikovskyi, M. (2024). Komplekcnui pidhid do vuyzvlennya ta analizu polimorfnogo zlovmysnogo programnogo zabezpechennya [Comprehensive approach to the detection and analysis of polymorphic malware]. Measuring and Computing Devices in Technological Processes, 2, 42–50 [in Ukrainian]. https://doi.org/10.31891/2219-9365-2024-78-5