DOI: 10.58254/viti.6.2024.19.232

УДК 004.056.57

д-р філософії Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Кисиленко Д. Ю. ORCID: 0000-0001-5491-6231 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ВИЗНАЧЕННЯ ІНВАРІАНТНОЇ КОМПОНЕНТИ В ПОВЕДІНЦІ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ІНТЕГРАЦІЇ НЕЧІТКОЇ ЛОГІКИ ТА ГЕНЕТИЧНИХ АЛГОРИТМІВ

Виявлення поліморфного та метаморфного шкідливого програмного забезпечення є надзвичайно важливим завданням забезпечення кібербезпеки через їх здатність уникати виявлення існуючими системами кіберзахисту шляхом автоматичної модифікації власного коду та/або структури. У даному контексті запропоновано підхід до виявлення поліморфного та метаморфного шкідливого програмного забезпечення, який базується на визначенні інваріантної компоненти для кожного відомого типу шкідливого програмного забезпечення під час аналізу його поведінки. Суть даного підходу полягає у визначенні такої області поведінки, яка залишається незмінною для конкретного типу шкідливого програмного забезпечення, незалежно від проведених модифікацій. Для пошуку зазначеної інваріантної компоненти в поведінці шкідливого програмного забезпечення для кожного його типу, множина значень вихідного простору ознак описується нечіткими лінгвістичними термами з метою отримання множини нечітких продукційних правил для кожного типу шкідливого програмного забезпечення. Наступним кроком є визначення нечіткої інваріантної компоненти для кожного відомого типу шкідливого програмного забезпечення у вигляді нечіткої підмножини ознак з отриманої на попередньому кроці множини нечітких продукційних правил засобами генетичних алгоритмів. Запропонована модель дає змогу значно підвищити точність виявлення поліморфного та метаморфного програмного забезпечення на основі поведінкових характеристик, властивих вже класифікованим зразкам, що, у свою чергу, сприяє підвищенню загальної ефективності системи кібербезпеки.

Ключові слова: *поліморфне та метаморфне шкідливе програмне забезпечення, поведінковий аналіз, кібербезпека, нечітка логіка, машинне навчання, зменшення розмірності, генетичні алгоритми.*

V. Fesokha, D. Kysylenko. A model for determining the invariant component in the behavior of malware software based on the integration of fuzzy logic and genetic algorithms

The detection of polymorphic and metamorphic malware is a critical cybersecurity challenge due to its ability to evade detection by existing cyber defense systems by automatically modifying its own code and/or structure. In this context, an approach to the detection of polymorphic and metamorphic malware is proposed, which is based on the determination of an invariant component for each known type of malware during the analysis of its behavior. The essence of this approach is to define such an area of behavior that remains unchanged for a specific type of malicious software, regardless of the modifications made. To find the specified invariant component in the behavior of malware for each of its types, a set of values of the original feature space is described by fuzzy linguistic terms in order to obtain a set of fuzzy production rules for each type of malware. The next step is to determine the fuzzy invariant component for each known type of malicious software in the form of a fuzzy subset of features from the set of fuzzy production rules obtained in the previous step by means of genetic algorithms. The proposed model makes it possible to significantly increase the accuracy of detection of polymorphic and metamorphic software based on behavioral characteristics characteristic of already classified samples, which, in turn, contributes to increasing the overall effectiveness of the cyber security system.

Keywords: *polymorphic and metamorphic malware, behavioral analysis, cyber security, fuzzy logic, machine learning, dimensionality reduction, genetic algorithms.*

Актуальність та постановка завдання в загальному вигляді. Поліморфне та метаморфне шкідливе програмне забезпечення (ШПЗ) представляє собою одну з найбільш складних та еволюційних загроз для кіберстійкості існуючих інформаційних систем (ІС). Його здатність до модифікації власного коду та/або структури значно ускладнює процес виявлення та нейтралізації існуючими системами кіберзахисту, які здебільшого базуються на поєднанні сигнатурного аналізу та методів машинного навчання для виявлення ШПЗ за відомими ознаками.

За останні роки спостерігається значна еволюція методів створення ШПЗ, які використовують передові системи та технології штучного інтелекту (ШІ) [1, 2]. Існуючі підходи до створення ШПЗ стають все більш автоматизованими та доступними для зловмисників будь-якого рівня кваліфікації. Це дає змогу їм досить швидко генерувати складні

варіації коду та адаптуватися до алгоритмів і моделей існуючих систем кіберзахисту, дозволяючи ШПЗ здійснювати приховану деструктивну діяльність протягом тривалого часу.

Враховуючи зростання кількості та складності поліморфного, олігоморфного та метаморфного ШПЗ, а також недостатню ефективність існуючих систем кіберзахисту в процесі їх виявлення [1] виникає нагальна потреба у вдосконаленні існуючих підходів до виявлення спроб реалізації такого класу загроз.

Аналіз попередніх досліджень. Враховуючи високий рівень адаптації поліморфного та метаморфного ШПЗ, а також використання новітніх технологій для їх модифікації, більшість традиційних методів виявлення мають певні обмеження щодо їх ідентифікації та нейтралізації.

Аналіз нижчевикладених наукових досліджень [3–6] демонструє найбільш ефективні існуючі методи виявлення поліморфного та метаморфного ШПЗ.

У роботах [3–4] пропонується використання *декларативного підходу* до виявлення шкідливих програм, що ґрунтується на аналізі поведінки модулів об’єкта кіберзахисту. Основна ідея дослідження полягає в порівнянні поведінки потенційно шкідливих програм, зокрема на збіжність та повторювання шаблонів у трасах системних викликів, які є характерними для шкідливих програм. Основна відмінність декларативного підходу від інших полягає в тому, що він спрямований на опис бажаного результату або стану системи, а не на використання конкретних методів досягнення цього результату. Так, фахівці з кібербезпеки описують правила і політики для виявлення аномальної поведінки або підозрілих дій у системі, які адаптуються до нових типів загроз, оскільки зміни в політиках та правилах можна вносити без необхідності змінювати основний код або архітектуру системи. Поряд з цим, даний підхід має певні недоліки: декларативним правилам властива недостатня гнучкість, тому виявляти нову деструктивну діяльність, яка не відповідає заздалегідь визначеним шаблонам, їх засобами досить складно; складність у створенні декларативних правил (потребує глибокого розуміння поведінки ШПЗ та контексту, в якому воно діє); залежність від суб’єктивного експертного судження в процесі побудови декларативних правил.

У дослідженні [5] розглядається підхід до виявлення кіберзагроз на основі *еволюційних алгоритмів*. Основна ідея даного підходу полягає у визначенні підмножини найбільш інформативних ознак з вихідної множини ознак для подальшого формування чітких правил виявлення деструктивної діяльності. Визначення підмножини найбільш інформативних ознак здійснюється засобами генетичних алгоритмів (ГА), які дозволяють отримати оптимальні комбінації ознак кіберзагроз. Проте, даний підхід має певні обмеження щодо виявлення поліморфних і метаморфних кіберзагроз. Так, толерантність до неточностей певної невизначеності, забезпечується використанням як дискретних значень ознак, так і діапазонів їх значень, що значно ускладнює роботу ГА щодо визначення оптимальної підмножини ознак кіберзагроз. До того ж, підмножина правил для кожного відомого класу кіберзагроз визначається окремо, що може призвести до випадків класифікації кіберзагрози одного класу як екземпляра іншого класу.

У роботі [6] запропоновано модель виявлення кібератак нульового дня на основі визначення підмножини найбільш значущих ознак для кожного відомого класу кібератак експертним шляхом. Так, в першу чергу вихідна множина значень для всіх відомих класів кібератак описується нечіткими правилами. Далі експертом визначається підмножина ознак з подальшим перетином вихідної та результуючої підмножин, з метою отримання таких нечітких правил, які достатньо повно описують незмінну структуру в ознаках кібератак для кожного відомого їх класу. Побудована модель за рахунок використання нечіткого опису незмінної структури в ознаках кібератак для кожного відомого їх класу є адаптивною, оскільки дозволяє виявляти поліморфні та метаморфні кібератаки, побудовані на основі раніше відомих

кібератак. Основним недоліком даного підходу є його залежність від суб'єктивного експертного судження при визначенні найбільш значущих ознак кібератак.

Підводячи підсумок розглянутих підходів щодо виявлення поліморфного та метаморфного ШПЗ, можна зробити висновок, що кожен з них має певну множину обмежень, які знижують їх ефективність. Жоден з розглянутих методів не використовує весь потенціал ключової особливості поліморфних та метаморфних кіберзагроз – інваріантної компоненти в їх поведінці під час динамічного аналізу. Використання інваріантної компоненти в поведінці ШПЗ для виявлення поліморфного та метаморфного ШПЗ на основі поєднання переваг нечіткої логіки та ГА може суттєво підвищити ефективність його виявлення та забезпечити ефективний кіберзахист ІС, у тому числі від нових зразків ШПЗ.

Метою статті є розробка моделі визначення інваріантної компоненти в поведінці ШПЗ на основі інтеграції нечіткої логіки та генетичних алгоритмів.

Модель визначення інваріантної компоненти в поведінці ШПЗ. Оскільки переважна більшість зразків існуючого поліморфного та метаморфного ШПЗ є модифікаціями вже існуючих (класифікованих) шкідливих програм, то за умови збереження їх інформаційно-деструктивного вектору впливу залишається незмінною певна підмножина поведінкових ознак для кожного відомого типу ШПЗ [1, 6, 7]. Ця підмножина описує інваріанту компоненту для кожного типу ШПЗ, тоді як решта ознак відображають поліморфну та/або метаморфну компоненту ШПЗ. Виходячи з цього, поведінка кожного окремого екземпляра певного типу ШПЗ є поліморфною та/або метаморфною по відношенню до решти зразків.

Враховуючи викладене, для вирішення завдання усунення виявлених недоліків існуючих підходів до протидії поліморфному та метаморфному ШПЗ [3–6] доцільно використати підхід, запропонований в роботі [7]. Суть даного підходу полягає у визначенні підмножини таких ознак з усього вихідного простору ознак поведінки ШПЗ, значення яких є інваріантними або близькими до інваріантних для кожного окремого типу ШПЗ.

Так, визначення підмножини шуканих ознак (інваріантної компоненти) доцільно здійснювати на основі підходу зменшення розмірності простору вихідних ознак, що описують поведінку ШПЗ засобами ГА. Вибір ГА для реалізації даного завдання обумовлено їх перевагами над іншими методами зниження розмірності, зокрема властивостями стійкості до шуму в даних та потенційною здатністю визначати глобальний оптимум [7]. Оскільки значення більшості ознак, які описують поведінку ШПЗ одночасно для всіх відомих його типів є варіативними (представлені діапазонами значень), тому доцільно описати навчальну вибірку нечіткими лінгвістичними термами. Даний підхід дає змогу:

значно зменшити обчислювальну складність ГА в процесі визначення інваріантної компоненти в поведінці ШПЗ на основі підходу зменшення розмірності простору ознак;

врахувати варіативність поведінкових ознак, які характерні для поліморфного та метаморфного ШПЗ;

глибоко розуміти приховані структури в поведінці ШПЗ внаслідок їх інтерпретації нечіткими правилами;

забезпечити гнучкість та адаптивність підходу в процесі виявлення поліморфного та метаморфного ШПЗ.

Для аналітичного обґрунтування зазначеного, представимо покроковий формальний опис математичної моделі визначення інваріантної компоненти в поведінці поліморфного та метаморфного ШПЗ. На рисунку 1 зображено узагальнену схему визначення інваріантної компоненти в поведінці ШПЗ шляхом зниження розмірності простору досліджуваних ознак на основі інтеграції нечіткої логіки та ГА, де x_i – ознака [7].

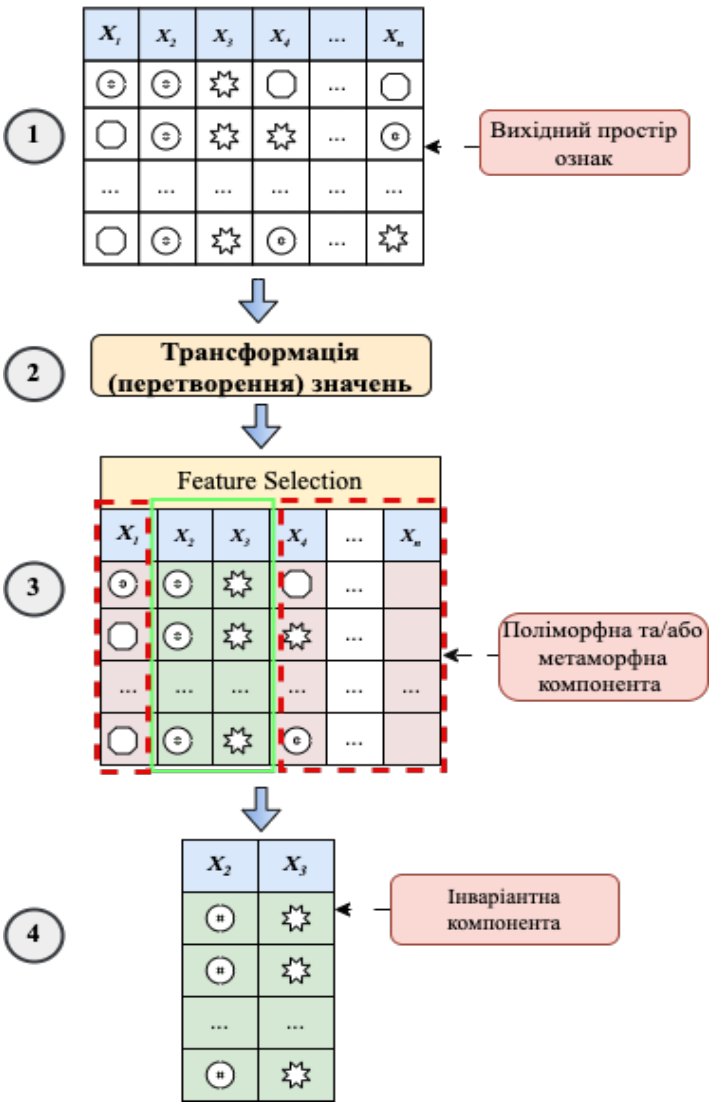

Рис. 1. Узагальнена схема визначення інваріантної компоненти в поведінці ШПЗ на основі інтеграції нечіткої логіки та ГА

1. *Ініціалізація вихідного простору ознак* $x_1 - x_n$ з навчальної вибірки опису поведінки ШПЗ, де окрема ознака x_i відповідає певному аспекту деструктивної діяльності відомих типів $T_1 - T_m$ (класів) ШПЗ, таких як [8, 13]:

worms (мережеві хробаки) – самостійно поширюються мережами створюючи власні копії;

trojans (троянське програмне забезпечення) – маскує шкідливу активність під легальне програмне забезпечення (ПЗ);

комп'ютерні віруси – прикріплюються до файлів чи програм з метою подальшої активації під час їх запуску;

rootkits (руткіти) – надають зловмисникам контроль над об'єктом атаки;

packers (пакувальники) – використовуються для стиснення або обфускації ШПЗ з метою уникнення виявлення захисними системами;

ransomware (програми вимагачі) – шифрують файли та вимагають викуп за їх розшифрування;

fileless malware (безфайлові програми) – функціонують в оперативній пам'яті, не створюючи жодних файлів на жорсткому диску;

spyware (шпигунське програмне забезпечення) – автоматично збирає конфіденційну інформацію без відома користувача;

adware (рекламне програмне забезпечення) – показує небажану рекламу;

keyloggers (логери клавіш) – відслідковують та записують кожне натискання клавіш;

bots – дистанційно керують інфікованими пристроями;

wiper malware – знищує або видаляє дані на жорсткому диску.

2. *Трансформація (перетворення) діапазонів значень ознак* навчальної вибірки засобами нечітких лінгвістичних термів з метою формування підмножин нечітких правил для кожного відомого типу ШПЗ. Для реалізації зазначеного, вхідні лінгвістичні змінні визначаються як початковий простір ознак $X_i = \left[x_i, \underline{x_i}\right]$ навчальної вибірки та вихідною лінгвістичною змінною $y \in Y = \left[y, \underline{y}\right]$ – висновком щодо належності фіксованого вектору ознак поведінки певному типу ШПЗ. Так, відповідність вектора фіксованих значень поведінки ШПЗ конкретному типу ШПЗ представлено наступним аналітичним виразом (1):

$$X = (x_1, \dots, x_n) \to y = d_j\left(a_j^1, \dots, a_i^{j_i}, \dots, w_1, w_n\right) \in D = (d_1, \dots, d_m), \quad (1)$$

де $i = \overline{1, \dots, m}$; y – лінгвістичний опис висновку $d \in D$ для вектора значень $\{x_1, \dots, x_n\}$; d – лінгвістичний терм; $a_i^{l_i}$ – номери комбінацій значень ознак; w_n – вага нечіткого правила; m – кількість можливих значень змінної y.

Відповідно до [6, 9] залежність між досліджуваним простором ознак та відповідним прийнятим рішенням може бути представлено у вигляді композиційної таблиці 1.

Таблиця 1

Композиційна таблиця множини отриманих нечітких правил

Номер вхідної комбінації	Вхідна підмножина поведінкових ознак				Ваговий коефіцієнт	Вхідна змінна y
	x_1	x_2	… x_i …	x_n		
11	a_1^{11}	a_2^{11}	… a_i^{11} …	a_n^{11}	w_{11}	d_1
12	a_1^{12}	a_2^{11}	… a_i^{12} …	a_n^{12}	w_{12}	
…	…	…	…			
$1k_1$	$a_1^{1k_1}$	$a_2^{1k_1}$	… $a_i^{1k_1}$ …	$a_n^{1k_1}$	w_{1k_1}	
…	…	…	…	…	…	…
$j1$	a_1^{j1}	a_2^{j1}	… a_i^{j1} …	a_n^{j1}	w_{j1}	d_j
$j2$	a_1^{j2}	a_2^{j2}	… a_i^{j2} …	a_n^{j2}	w_{j2}	
…	…	…	…	…	…	
jk_j	$a_1^{jk_j}$	$a_2^{jk_j}$	… $a_i^{jk_j}$ …	$a_n^{jk_j}$	w_{jk_j}	
…	…	…	…	…	…	…
$m1$	a_1^{m1}	a_2^{m1}	… a_i^{m1} …	a_n^{m1}	w_{m1}	d_m
$m2$	a_1^{m2}	a_2^{m2}	… a_i^{m2} …	a_n^{m2}	w_{m2}	
…	…	…	…	…	…	
mk_m	$a_1^{mk_m}$	$a_2^{mk_m}$	… $a_i^{mk_m}$ …	$a_n^{mk_m}$	w_{mk_m}	

де x_i – поведінкова ознака; w_n – вага нечіткого правила; $a_i^{j_k}$ – номери комбінацій значень ознак; *d* – лінгвістичний терм змінної y; *m* – кількість можливих значень змінної y.

Функція належності – гаусова. Спосіб визначення оптимальної кількості термів для кожної ознаки – показник силуету. Алгоритм нечіткого логічного виводу – Мамдані. Після трансформації значень необхідно здійснити видалення дублікатів правил.

3. *Зниження розмірності досліджуваного простору ознак* засобами ГА полягає у визначенні інваріантної компоненти в поведінці ШПЗ шляхом відбору таких ознак, які закономірно (системно) в сукупності повторюються для більшості екземплярів кожного класу ШПЗ [10, 11].

На основі викладеного виникає завдання пошуку оптимальної підмножини ознак для кожного типу ШПЗ, засобами якої точність класифікації екземплярів ШПЗ буде максимальною для коректного типу і водночас мінімальною для решти типів. Доцільність реалізації такого підходу обумовлюється виключенням можливості отримання ідентичних інваріантних компонент для різних типів ШПЗ на спільному просторі ознак та забезпечення її специфічності для кожного типу [7].

Вхідними даними на даному етапі є композиційна таблиця нечітких правил, отримана на попередньому етапі. Ген ГА – ознака $x_i \in X$. Кожне рішення (хромосома) у ГА представляє підмножину ознак X_{sub} з простору ознак *X*, яка може бути ефективною для класифікації ШПЗ за типами. Представлення підмножин у популяції здійснюється засобами двійкового кодування (вектором двійкових значень довжиною *m <= n, де m – потужність підмножини* X_{sub}*; n – потужність підмножини X*); де кожен біт відповідає певній ознаці *i*. Наявність одиниці в бітовому рядку [1, 0, 1, 0, 1] відповідає відбору *i-ї* ознаки до підмножини X_{sub}.

Цільова функція ГА (Target Function): пошук оптимальної підмножини ознак поведінки ШПЗ для подальшої класифікації за типами (2).

$$TF(X_{sub}) = \arg\max\left(Accuracy\left(X_{sub,\ target}\right) - \sum_{i \neq target} Accuracy(X_{sub,\ i}) \right), \tag{2}$$

де X_{sub} – підмножина ознак, яку генерує ГА;

$Accuracy\left(X_{sub,\ target}\right)$ – точність класифікації для коректного типу ШПЗ (цільовий тип);

$\sum_{i \neq target} Accuracy\left(X_{sub,\ i}\right)$ – сума значень точностей класифікації для всіх інших типів ШПЗ;

arg max – аргумент (підмножина ознак), при якому функція досягає максимального значення.

Функція пристосованості ГА (Fitness Function): оцінка кожної отриманої підмножини X_{sub} щодо її ефективності максимізувати точність класифікації для цільового типу ШПЗ і мінімізувати для решти типів. Математична модель даної функції пристосованості може бути представлена аналітичним виразом (3).

$$FF(X_{sub}) = Accuracy\left(X_{sub,\ target}\right) - \sum_{i \neq target} Accuracy\left(X_{sub,\ i}\right). \tag{3}$$

Система класифікації: нечіткий логічний вивід Мамдані [12].

Критерії зупинки ГА: алгоритм може бути зупинено за умов отримання максимального значення ефективності класифікації ШПЗ за показником точності.

Результат роботи ГА: отримання підмножини ознак X_{sub}, яка є інваріантною для цільового типу ШПЗ.

Виконання ГА [13]:

1. *Формування початкової популяції:* алгоритм розпочинає роботу з випадково згенерованих початкових підмножин ознак (популяції), що являє собою певне рішення задачі в першому наближенні.

2. *Обчислення значень функції пристосованості:* на кожній ітерації ГА підмножини популяції оцінюються за допомогою функції пристосованості.

3. *Перевірка умови зупинки алгоритму:* якщо результат задовольняє умову завершення алгоритму – кінець алгоритму, у противному випадку – далі.

4. *Селекція пар батьківських хромосом:* вибір батьківських підмножин для операції схрещування полягає у виборі (на основі розрахованих на 2-му етапі значень функції пристосованості) тих підмножин X_{sub}, які будуть брати участь в створенні нащадків для наступного покоління. Дана операція здійснюється відповідно до принципу природного відбору, за яким найбільші шанси на участь в створенні нових нащадків мають підмножини з найбільшими значеннями функції пристосованості. Найбільш популярним вважається метод рулетки, який отримав свою назву за аналогією з відомою азартною грою. Кожній підмножині виділено сектор колеса рулетки, величина якого пропорційна значенню її функції пристосованості. Чим більше значення функції, тим більший сектор на колесі рулетки.

5. *Застосування генетичних операторів (схрещування, мутація)*: оператор схрещування (P_c), сприяє обміну генетичною інформацією між батьківськими підмножинами з метою створення нових нащадків. Цей процес полягає у випадковому об'єднанні підмножин батьківської популяції у пари, де в точках схрещування (L_k) відбувається обмін генетичною інформацією. Це сприяє розширенню простору пошуку та збереженню важливих ознак в нащадках. Результатом схрещування пари батьківських підмножин є створення пари нащадків. Оператор мутації P_m зазвичай використовується на батьківській популяції перед схрещуванням, або на новій популяції, що утворена в результаті схрещування. Мутація полягає у випадковій заміні ознак у підмножині з метою уникнення локальних мінімумів. Далі формується нова популяція, яка стає поточною для наступної ітерації. Процес виконується до виконання умов зупинки.

6. *Отримання результату:* якщо аналітичний опис поведінки деякого екземпляра конкретного типу ШПЗ можна представити у вигляді (4) [6]:

$$X = \{x_1, x_2, \dots, x_i, \dots, x_n\}, \text{де } i = \overline{1,n}, \tag{4}$$

то поведінку поліморфного (метаморфного) йому екземпляра того ж типу ШПЗ представимо як (5):

$$X_{plmf} = \{f_1(x_1), f_2(x_2) \ \dots, x_i, \dots, f_m(x_m)\}, i \in I_{inv}, f_i(x_i) \in F_{plmf}, \tag{5}$$

де x_i – поведінкова ознака; $f_i(x_i)$ – функція модифікації ознак; I_{inv} – підмножина індексів інваріантних ознак; F_{plmf} – підмножина функцій $f_i(x_i)$, які змінюють ознаки x_i.

Звідси, інваріантна компонента описується наступним чином (6):

$$X_{inv} = \{x_i \in X \mid x_i = static\}, i \in \tag{6}$$

Так, для типів ШПЗ [14] Ransomware, Fileless Malware, Spyware, Adware, Trojans, Worms, Rootkits, Keyloggers, Bots, Wiper Malware (7):

$$X_{ransom} = \{x_1^1, x_2^1, \dots, x_n^1\} \rightarrow X_{ransom}^{inv}\{x_1^1, x_2^1, \dots, x_m^1\}, \tag{7}$$

$$X_{fileless} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{fileless}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{spy} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{spy}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{ad} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{ad}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{trojans} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{trojans}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{worms} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{worms}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{rootkits} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{rootkits}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{keyloggers} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{keyloggers}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{bots} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{bots}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{wiper} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{wiper}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$

де m – кількість поведінкових ознак інваріантної компоненти ШПЗ.

Після виконання певної кількості ітерацій алгоритм сходиться до найкращої підмножини X_{sub}, яка буде являти собою оптимальне або субоптимальне рішення. Таким чином, на основі отриманих нечітких підмножин поведінкових ознак для кожного відомого типу ШПЗ, які описують їх інваріантну активність у процесі реалізації кібервпливу, здійснюємо виявлення поліморфного або метаморфного ШПЗ засобами нечіткого логічного виводу (8).

$$\mu^{d_j}(x_1, x_2, \dots, x_{n(mp)}) = \max_{p=\overline{1,k_j}}\{w_{jp}\min_{i=\overline{1,n}}[\mu^{jp}(x_i)]\}, \mathrm{j} = \overline{1,m}. \quad (8)$$

В якості прийнятого рішення про наявність/відсутність деструктивної активності ШПЗ визначається результат з максимальним значенням, отриманим в результаті згортки функцій належності термів нечітких правил опису їх інваріантних компонент для кожного типу ШПЗ $T_1 - T_m$.

Оцінка ефективності. Для визначення точності виявлення ШПЗ на основі запропонованої моделі було використано офіційний набір даних про кіберзагроз ML-Based NIDS Datasets, зокрема NF-UQ-NIDS-v2 [15], який містить опис різноманітних типів ШПЗ. Обрані зразки ШПЗ у NF-UQ-NIDS-v2 [15]:

analysis – різноманітні загрози, націлені на вебдодатки через порти, електронну пошту та скрипти (2190 зразків);

generic – ШПЗ, здатне до несанкціонованого саморозмноження локальними ресурсами комп'ютера (12098 зразків);

ransomware – ШПЗ для шифрування файлів з метою вимагання компенсації в обмін на метод/ключ розшифрування (3420 зразків);

shellcode – ШПЗ для віддаленого контролю об'єкта впливу (1426 зразків);

theft – ШПЗ для отримання конфіденційної інформації, наприклад, крадіжка даних або клавіатурне шпигунство (2410 зразків);

worms – ШПЗ для самокопіювання та поширення на інші вузли мережі (163 зразки).

В таблиці 2 наведено результати визначення нечітких інваріантних компонент ШПЗ, описаних зазначеними підмножинами ознак для кожного типу ШПЗ з усього представленого простору ознак, а також ефективність виявлення ШПЗ за показником точності на їх основі.

Таблиця 2

Визначені інваріантні компоненти поведінки
ШПЗ і точність виявлення ШПЗ

ШПЗ / **Ознака**	Analysis	Generic	Ransomware	Shellcode	Theft	Worms
L4_SRC_PORT						
L4_DST_PORT	■					
PROTOCOL			■	■	■	■
L7_PROTO						
IN_BYTES				■		
IN_PKTS	■	■		■		■
OUT_BYTES	■	■	■	■		■
OUT_PKTS	■	■		■		
TCP_FLAGS						
CLIENT_TCP_FLAGS						
SERVER_TCP_FLAGS						
FLOW_DURATION_MILLISECONDS						
DURATION_IN	■	■	■	■		■
DURATION_OUT		■				
MIN_TTL				■		
MAX_TTL						
LONGEST_FLOW_PKT	■	■	■	■		■
SHORTEST_FLOW_PKT			■		■	
MIN_IP_PKT_LEN						
MAX_IP_PKT_LEN	■	■	■	■		■
SRC_TO_DST_SECOND_BYTES	■	■	■	■		■
DST_TO_SRC_SECOND_BYTES	■	■		■	■	■
RETRANSMITTED_IN_BYTES	■	■	■	■	■	
RETRANSMITTED_IN_PKTS		■				
RETRANSMITTED_OUT_BYTES	■	■		■	■	
RETRANSMITTED_OUT_PKTS	■	■		■	■	
SRC_TO_DST_AVG_THROUGHPUT	■	■		■		
DST_TO_SRC_AVG_THROUGHPUT	■	■		■		
NUM_PKTS_UP_TO_128_BYTES	■	■	■	■		■
NUM_PKTS_128_TO_256_BYTES	■	■		■		■
NUM_PKTS_256_TO_512_BYTES				■	■	■
NUM_PKTS_512_TO_1024_BYTES						
NUM_PKTS_1024_TO_1514_BYTES	■	■		■		
TCP_WIN_MAX_IN						
TCP_WIN_MAX_OUT						
ICMP_TYPE						
ICMP_IPV4_TYPE						
DNS_QUERY_ID	■		■	■	■	■
DNS_QUERY_TYPE	■		■	■	■	■
FTP_COMMAND_RET_CODE	■		■		■	■
Точність (%)	100	99,6	98,6	100	98	98,8

Висновки. У статті вирішується актуальне наукове завдання визначення інваріантної компоненти в поведінці ШПЗ. Запропоновано модель визначення інваріантної компоненти в поведінці ШПЗ на основі поєднання переваг нечіткої логіки та ГА. Суть даної моделі, що відрізняє її від існуючих, полягає в автоматизованому визначенні засобами ГА підмножини таких поведінкових ознак ШПЗ, описаних нечіткими лінгвістичними термами, які представляють унікальну інваріантну компоненту для кожного відомого типу ШПЗ. Оцінка ефективності розробленої моделі демонструє високу точність виявлення ШПЗ на основі попередньо визначених нечітких інваріантних компонент ШПЗ. Застосування даної моделі дає змогу описувати поведінку ШПЗ за умов певної нечіткості значень досліджуваних ознак без залучення експертів, а також підвищити ефективність виявлення поліморфного та метаморфного ШПЗ.

Перспективним напрямком подальших наукових досліджень є розробка методу самонавчання підсистеми кіберзахисту на основі використання запропонованої моделі в процесі протидії ШПЗ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Фесьоха В. В., Кисиленко Д. Ю., Нестеров О. М. Аналіз спроможності існуючих систем антивірусного захисту та покладених у їхню основу методів до виявлення нового шкідливого програмного забезпечення у військових інформаційних системах. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2023. Т. 3. С. 143–151.

2. Фесьоха В. Особливості протистояння оборонного та наступального штучного інтелектів у кіберпросторі. *International Science Journal of Engineering & Agriculture*. 2024. Т. 3, № 4. С. 105–114. URL: https://doi.org/10.46299/j.isjea.20240304.11.

3. Bernardi M. L., Cimitile M., Mercaldo F. Process mining meets malware evolution: a study of the behavior of malicious code. *International symposium on computing and networking – across practical development and theoretical research*. 2016. URL: https://www.semanticscholar.org/paper/Process-Mining-Meets-Malware-Evolution:-A-Study-of-Bernardi-Cimitile/7838664913ba2ab34d78f6120188293bd77a7fb3.

4. Ardimento P., Bernardi M. L., Cimitile M. Malware phylogeny analysis using data-aware declarative process mining. *IEEE conference on evolving and adaptive intelligent systems (EAIS)*. 2020. URL: https://www.semanticscholar.org/paper/Malware-Phylogeny-Analysis-using-Data-Aware-Process-Ardimento-Bernardi/859dd8a091b4af71426a189225ee09a3a2e78a69.

5. Метод виявлення кіберзагроз на основі еволюційних алгоритмів / С. М. Лисенко, Д. І. Стопчак, В. В. Самотес // Вісник Хмельницького національного університету. Технічні науки. 2017. № 6. С. 81–88. URL: http://nbuv.gov.ua/UJRN/Vchnu_tekh_2017_6_15.

6. Zero-day polymorphic cyberattacks detection using fuzzy inference system / V. V. Fesokha et al. *Austrian Journal of Technical and Natural Sciences*. 2020. P. 8–13. URL: https://doi.org/10.29013/ajt-20-5.6-8-13.

7. Фесьоха В. В., Кисиленко Д. Ю., Фесьоха Н. О. Обґрунтування вибору підходу до визначення інваріантної компоненти у поведінці поліморфного (метаморфного) шкідливого програмного забезпечення на основі зниження розмірності простору ознак. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2024. Т. 5. С. 181–192.

8. Енциклопедія Інтернет-загроз – ESET. *ESET*. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/.

9. Subach I., Fesokha V. Model of detecting cybernetic attacks on information-telecommunication systems based on description of anomalies in their work by weighed fuzzy rules. *Collection "Information technology and security"*. 2017. Vol.5, no. 2. P. 145–152. URL: https://doi.org/10.20535/2411-1031.2017.5.2.136984.

10. Feature dimensionality reduction: a review – Complex & Intelligent Systems. *SpringerLink*. URL: https://link.springer.com/article/10.1007/s40747-021-00637-x#:~:text=The%20basic%20principle%20of%20feature,5,6,7].

11. Sanjyal A. Dimensionality reduction VS feature selection. *Medium*. URL: https://medium.com/@asanjyal81/dimensionality-reduction-vs-feature-selection-e68f91aa8724.

12. Зінов‘єва О. Г., Лубко Д. В. Алгоритм Мамдані в системах нечіткого виведення. *ElarTSATU: Home*. URL: http://elar.tsatu.edu.ua/handle/123456789/16952.

13. Kanade V. Genetic algorithms – meaning, working, and applications – spiceworks. *Spiceworks*. URL: https://www.spiceworks.com/tech/artificial-intelligence/articles/what-are-genetic-algorithms/.

14. 12 Types of Malware + Examples That You Should Know | CrowdStrike. *CrowdStrike: We Stop Breaches with AI-native Cybersecurity*. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/.

15. ML-Based NIDS Datasets. *School of Information Technology and Electrical Engineering*. URL: https://staff.itee.uq.edu.au/marius/NIDS_datasets/#RA6.