УДК 004.056.54

С. М. ЛИСЕНКО,
О. І. ШЕВЧУК
Хмельницький національний університет

МЕТОД ТА ПРОГРАМНІ ЗАСОБИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТИПУ BACKDOOR НА ОСНОВІ ВИКОРИСТАННЯ АЛГОРИТМУ КЛОНАЛЬНОГО ВІДБОРУ

В роботі представлено метод виявлення шкідливого програмного забезпечення типу backdoor на основі алгоритму клонального відбору. Експериментальні результати показують, що запропонований метод здатний здійснювати виявлення шкідливого програмного забезпечення типу backdoor з високою ефективністю, яка складає понад 95%. Запропонований метод може бути основою для побудови програмного забезпечення для антивірусного діагностування.

Ключові слова: шкідливе програмне забезпечення, backdoor, штучні імунні системи, алгоритм клонального відбору.

S. LYSENKO,
O. SHEVCHUK
Khmelnytsky National University

TECHNIQUE FOR BACKDOORS' DETECTION BASED ON THE USAGE OF THE CLONAL SELECTION ALGORITHM

The paper presents a technique for backdoors' detection based on the usage of the clonal selection algorithm. Experimental results show that the proposed method is able to detect the backdoor malware with high efficiency up to 95%. The proposed method is able to become the basis for the anti-virus software development. The results of experimental studies suggest that the attraction of the clonal selection algorithm demonstrates high rates of detection of backdoor type SUs. So the overall detection efficiency was more than 95%, but the rate of false alarms is also quite high now (6%), which necessitates the improvement of the method and the search for the optimal parameters of the algorithm. Thus, the proposed method demonstrated the possibility of implementing a software classification on utility and a backdoor with high reliability. In this article, a method for detecting malicious software based on the algorithm of artificial immune systems - the clonal selection algorithm. Experimental results show that the proposed method is capable of detecting malicious software of the backdoor type with high efficiency, which is more than 95%. The proposed method can be the basis for constructing software for anti-virus diagnostics.

Keywords: malware, backdoor, artificial immune system, clonal selection algorithm.

ВСТУП. В даний час, комп'ютерні системи відіграють вадливу роль в усіх аспектах людського життя. Тому проблема захисту наших даних і інформації вкрай актуальною. Однією із загроз щодо порушення цілісності та конфіденційності інформації є несанкціонований доступ з третьої сторони [1], зокрема зловмисників, що використовують шкідливе програмне забезпечення (ШПЗ) для такого несанкціонованого доступу – ШПЗ типу backdoor [1].

Основною особливістю із засобів активного здійснення порушення конфіденційності в КС є залучення шкідливого програмного забезпечення типу backdoor, яке здійснює встановлення файлів або шкідливого програмного забезпечення (ШПЗ), модифікації коду або виявлення файлів та отримання доступу до системи або даних.

Сучасне антивірусне програмне забезпечення здатне виявляти та видаляти відоме шкідливе програмне забезпечення, оскільки застосовують сигнатурний аналіз [2]. Однак не в повній мірі адаптовані до розпізнавання нового ШПЗ.

З огляду на вказані вище проблеми актуальним є розроблення методів виявлення шкідливого програмного забезпечення типу backdoor.

ПОВ'ЯЗАНІ РОБОТИ. Традиційно аналіз шкідливого програмного забезпечення є складною задачею, і більшість не сигнатурних методів аналізу характеризуються високою обчислювальною складність та недостатньою ефективністю. Саме тому увага науковців прикута до розроблення нових методів виявлення ШПЗ типу backdoor, які б нівелювали вказані недоліки.

В роботі [3] представлено метод до вилучення ознак для ШПЗ визначення шаблонів (поведінок) троянських програм, призначених для шпіонажу даних та створення ШПЗ типу backdoor. Для виявлення таких ознак прийнято статичну методологію аналізу матеріалів. Метод включає в себе п'ять кроків: виявлення, ідентифікація, обфускація коду, вилучення ознак ШПЗ та оновлення шкідливих функцій. Ці встановлені закономірності, а також множина побудованих шаблонів ШПЗ типу backdoor потім використовуються для його виявлення. Недоліком даного методу є обмеженість поведінкового набору, і, як наслідок, недостатня масштабованість такого підходу.

У праці [4] наведено метод для ефективного моніторингу мережного трафіку. Метод враховує особливості функціонування ШПЗ типу backdoor у мережі, зокрема вплив на трафік, що проходить через маршрутизатори, а також особливості побудови апаратних backdoor-систем. Підхід базується на безпечній, надмірній та адаптивній схемі розподілу трафіку, що дозволяє належним чином виявляти шкідливий трафік на мережному обладнанні. Метод базується на аналізі спроб пере направлення трафіку, його дзеркалювання, скидання, вставки або заміни пакетів.

Зокрема, в [5] досліджено можливості застосування формальних методів до рішення задачі виявлення ШПЗ типу backdoor. Було встановлено, що застосування cnf, ragon, krom, monotone і positive-unit логік висловлювань дозволяють здійснити розпізнавання ШПЗ, але є складним для класифікації.

У [6] докладно розглядаються загрози з боку ШПЗ типу backdoor в бездротових мережах і пропонуються нові рішення, які дозволять не тільки виявити атаку на мережу даним ШПЗ, але й приймати контрзаходи для збереження цілісності бездротових мереж на апаратному рівні.

Метод, що представлений у [7] із залученням апарату нечіткої логіки, дозволяє здійснити виявлення вторгнень шкідливим програмним забезпеченням типу backdoor шляхом використання нечіткої системи для оцінки шкідливої активності в комп'ютерних мережах. Підхід будується на основі агентів, які використовуються для моніторингу в мережі. Висновок щодо присутності ШПЗ типу backdoor здійснюється системою нечіткого логічного на основі аналізу отриманих даних з агентів, що функціонують в мережі.

Загальним недоліком вище вказаних методів є недостатня ефективність, зумовлена високою обчислювальною складністю, недостатнім рівнем виявлення, та високим рівнем хибних спрацювань. З огляду на це виникає задача розробки нового методу виявлення шкідливого ПЗ типу backdoor, який би усунув вищевказані недоліки.

ШТУЧНІ ІМУННІ СИСТЕМИ ЯК ЗАСІБ КЛАСИФІКАЦІЇ ОБ'ЄКТІВ. На сьогодні одним з актуальних напрямків розроблення ефективних евристичних методів виявлення ШПЗ є залучення апарату штучного інтелекту. Система базується на інтеграції двох методів штучного інтелекту: методу штучних нейронних мереж і методу штучних імунних систем. Штучні імунні системи базуються на основних принципах біологічного імунітету, який успішно захищає організм від хвороботворних бактерій і вірусів. Штучні імунні системи (ШІС) мають основні властивості штучного інтелекту: пам'ять, здатність до навчання і прийняття рішень [8].

Зокрема, засоби ШІС успішно застосовуються для вирішення завдань оптимізації і класифікації, крім цього, штучні імунні системи застосовуються для стиснення інформації, кластеризації, пошуку аномалій, машинного навчання, обробки неструктурованих даних і вилучення інформації, комп'ютерної безпеки і адаптивного контролю. У порівнянні з популярними нині генетичними алгоритмами, які зазвичай мають тенденцію до зміни всієї популяції, імунні алгоритми використовують тільки найкращі знайдені рішення, що може ефективно використовуватися в задачах мультимодальній оптимізації.

Також, використання штучної імунної системи (ШІС) зробило великий внесок у розроблення нових систем гарантування безпеки. Одним з ефективним засобів класифікації об'єктів в апараті ШІС є алгоритм клонального відбору, який характеризується високою точністю результатів виявлення шкідливого програмного забезпечення (ШПЗ).

Імунні системи. Імунні системи, як системи захисту живих організмів проти патогенів, стали основою для побудови штучних імунних систем (ШІС). Інтерес дослідників викликаний особливостями імунних систем таких як: розпізнавання антигенна (Ag), можливість запам'ятовування, самоорганізовуюча пам`ять , адаптивність, здатність до навчання, паралельна обробка даних, багатошарова структура і можливість узагальнення [9]. Один з базових алгоритмів ШІС – алгоритм клонального відбору, який володіє властивостями нелінійної класифікації та є засобом адаптивного розпізнавання образів [10].

Біологічна основа імунних систем. Основна функцією імунної системи є здатність розпізнавати «чужі» клітини які називають антигенами (Ag) і «свої» клітини [11].

Природній імунітет забезпечує безпосередній захист тіла і знищує антигени, використовуючи макрофаги і природні клітини-вбивці. Його імунна відповідь не має імунологічної пам'яті, з тих пір, поки відповідь не отримає повторний вплив від специфічних антигенів Ag's. З іншого боку, імунітет має імунологічну пам'ять для специфічних антигенів Ag's. Імунна відповідь складається з специфічних для антигенна відповідей від лімфоцитів (Т та В клітин), які діють як проміжний і гуморальний імунітети вхідних клітин. Кожна В клітина може виробляти одну специфічну форму антигенів – антитіла (Ab's), які здатні боротися з антигенами Ag's [12].

Принцип клонального відбору. Алгоритм клонального відбору демонструє спосіб, у який імунна система реагує на антигени, та її здатність усувати антигени [13]. Коли антиген атакує організм, імунні клітини (В лімфоцити) виробляють специфічні антитіла (Ab's) проти нападаючих антигенів (Ag's). Антитіла Ab's – молекули, прикріплені до поверхні клітин В, чия мета – розпізнати і реагувати на антигени Ag's. Процес швидкого розмноження клітин, які розпізнають нападаючі антигени Ag's, призводить до породження клітин двох нових типів: нападаючих і клітини пам'яті. Нападаючі клітини виділяють багато ефективних антитіл Ab's, для

знешкодження нападаючих антигенів Ag's. Клітини пам'яті мають довготривалий період існування і у випадку майбутніх атак антигенів Ag's з схожими властивостями, вони можуть реагувати швидше і ефективніше [14].

Беручи до уваги властивості алгоритму клонального відбору щодо розпізнавання образів, він може бути основою процесу класифікації, зокрема процесу виявлення ШПЗ типу backdoor.

ПОСТАНОВКА ЗАДАЧІ. Таким чином, актуальною науково-практичною задачею є розроблення нового методу виявлення шкідливого програмного забезпечення типу backdoor на основі використання алгоритму клонального відбору. Виявлення наявності шкідливого програмного забезпечення на комп'ютері здійснюється шляхом аналізу поведінки програмного забезпечення в комп'ютерній системі.

МЕТОД ТА ПРОГРАМНІ ЗАСОБИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТИПУ BACKDOOR НА ОСНОВІ ВИКОРИСТАННЯ АЛГОРИТМУ КЛОНАЛЬНОГО ВІДБОРУ. В статті пропонується метод виявлення шкідливого програмного забезпечення типу backdoor на основі використання алгоритму клонального відбору. Метод дозволяє забезпечити виявлення ШПЗ типу backdoor на основі ознак характерних життєвому циклу функціонування даного типу ШПЗ. Робота методу полягає в здійсненні відслідковування системних подій в КС, формуванні множини ознак, що вказують на присутність ШПЗ типу backdoor, а також здійсненні висновку на основі залучення апарату штучних імунних систем.

Метод складається з етапів: навчання систем та безпосереднього виявлення ШПЗ типу backdoor.

Етап навчання включає наступні кроки:

1. побудова бази поведінок ШПЗ типу backdoor на основі знань про особливості їх функціонування в КС;

2. представлення поведінок ШПЗ типу backdoor у вигляді множини антигенів шляхом застосування алгоритму клонального відбору (побудова навчальної вибірки).

Етап виявлення ШПЗ типу backdoor:

1) здійснення відслідковування системних подій (API calls) в КС та їх журналювання;

2) динамічна побудова поведінки ШПЗ типу backdoor;

3) динамічне порівняння поведінок серед множини антигенів з поведінкою досліджуваного ПЗ та класифікація ПЗ.

4) блокування ПЗ, класифікованого як шкідливе.

Укрупнена схема функціонування методу виявлення ШПЗ типу backdoor на основі алгоритму клонального відбору подана на рис. 1.

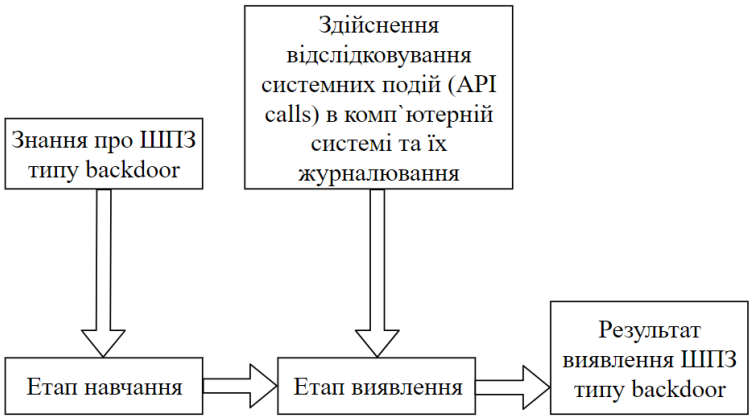

Рис. 1. Укрупнена схема функціонування методу виявлення ШПЗ типу backdoor на основі алгоритму клонального відбору

Загальна схема функціонування метода виявлення ШПЗ типу backdoor на основі алгоритму клонального відбору на рис. 2.

Розглянемо більш детально перший етап методу виявлення ШПЗ типу backdoor на основі алгоритму клонального відбору.

Представлення поведінок ШПЗ типу backdoor у вигляді множини антигенів шляхом застосування алгоритму клонального відбору (побудова навчальної вибірки). Подамо поведінку ШПЗ типу backdoor як множину шкідливих дій у вигляді двійкової послідовності довжини кількості усіх ознак ШПЗ, *X*. Приймемо $(a_{i1}, a_{i2}, ..., a_{iX})$, $i = 1,2,...,n$ як антиген/антитіло (поведінка ПЗ), де $a_{ij} = 0, j = 1,2,...,X$ визначає наявність відповідної ознаки ШПЗ, а $a_{ij} = 1, j = 1,2,...X$ – її наявність; a_i – API-виклик, множина яких формує шкідливий функціонал backdoor додатку Кожен антиген/антитіло представляє підмножину ознак, що описує певну поведінку конкретного ШПЗ типу backdoor. Множина побудованих антигенів формує

навчальну вибірку системи виявлення ШПЗ типу backdoor.

Навчання системи виявлення ШПЗ типу backdoor на основі алгоритму клонального відбору. Процес здійснення навчання системи виявлення ШПЗ типу backdoor базується на залучені навчальної вибірки і включає наступні кроки [15]:

Ініціалізація. Включає формування пулу антитіл розміром N, який ділиться на дві множини: антитіла пам'яті *m* і решта з пулу антитіл *r*, що залишився.

Здійснення дій в циклі. Алгоритм клонального відбору ітераційно повторює необхідні операції щодо кожного антигену в системі. Кожна ітерація в алгоритмі клонального відбору є поколінням. Кількість поколінь *G,* що виконує система може бути визначено користувачем; проте, система може також використовувати критерій «зупинки».

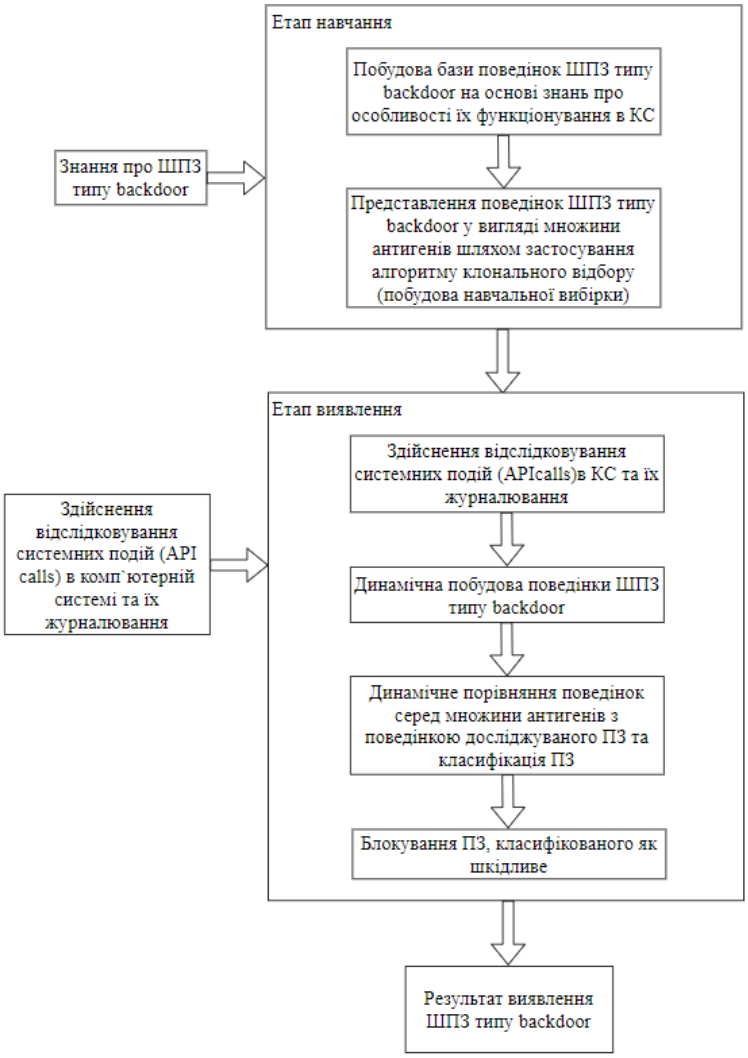

Рис. 2. Загальна схема функціонування методу виявлення ШПЗ типу backdoor на основі алгоритму клонального відбору

a. Відбір антигенна. Один антиген обирається випадковим чином без процедури перестановки (для поточного покоління) із пулу антигенів.

b. Вплив. Система піддається впливу щодо вибраного антигену. Для всіх антитіл створених для протидії антигену обчислюється значення міри схожості – афінності. В даному дослідженні було застосовано відстань Хеммінга, яка була обчислення за допомогою формули:

$$D(Ag, Ab) = \sum_{k=1}^{L} [Ag_k \neq Ab_k], \quad (1)$$

де D – відстань Хеммінга, Ag – антиген, Ab – антитіло, L – довжина двійкової послідовності.

c. Відбір. Множина з *n* антитіл вибираються з множини пулу антитіл, що має найвищу афінність з антигеном.

d. Клонування. На основі отриманих значень афінності, множина відібраних антитіл піддається процедурі клонування, де кількість клонів *C* обчислюється за формулою:

$$C = \left\lceil \frac{\beta \cdot N}{i} + 0.5 \right\rceil, \tag{2}$$

β – коефіцієнт клонування, N – розмір пулу антитіл, i – ранг поточного антитіла, де $i \in [1, n]$.

Загальна кількість клонів, готових для впливу на кожен антиген систем, визначається так:

$$N_C = \sum_{i=1} \left\lceil \frac{\beta \cdot N}{i} + 0.5 \right\rceil \tag{3}$$

e. Мутація. Виконання процедури афінної мутації здійснюється для отримати кращої відповідності між клоном і антигеном. Рівень дозрівання обернено пропорційний до афінності: чим вище афінність, тим нижче рівень мутації.

f. Впливи на клони. Клон піддається впливу антигеном, і здійснюється обчислення афінності дозріваючих клонів відносно антигену.

g. Відбір кандидатури. Кандидатом до множини антитіл пам'яті m є антитіла з найвищою афінністю. Якщо афінність кандидата вища, ніж афінність антигенна з множини *m,* то вона замінюється попереднім антигеном.

h. Перестановки. Індивіди *d* із множини антигенів *r* з найнижчою афінністю замінюються новими випадковими антитілами.

3. Зупинка роботи алгоритму. Після завершення процедури навчання, множина антигенів пам'яті *m* з пулу антигенів є рішенням алгоритму. Критерієм зупинки є ситуація, коли середня афінність антитіл Ab's перевищує певне порогове значення. У цій ситуації навчання даного антигену припиняється. Якщо критерій не виконується, здійснюється повтор виконання кроків починаючи з етапу відбору антигену.

КЛАСИФІКАЦІЯ ШПЗ ТИПУ BACKDOOR ЗА ДОПОМОГОЮ АЛГОРИТМУ КЛОНАЛЬНОГО ВІДБОРУ. Після завершення етапу навчання, набір пам'яті антигенів *m* доступний для класифікації. Кожна клітина пам'яті представлена певним елементом даних. Процес класифікації передбачає обчислення афінності між клітиною пам'яті та отриманим ШПЗ типу backdoor. Класифіковане ШПЗ типу backdoor відноситься до шуканого класу, якщо має максимальну афінність.

На даному етапі методу необхідно здійснювати відслідковування системних подій в операційній системі КС. Відносно кожного програмного об'єкту повинен вестися журнал виконання його дій. На основі даних журналів динамічно формується поведінка того чи іншого програмного забезпечення.

Використовуючи побудований набір антигенів (базу поведінок ШПЗ), динамічно здійснюється порівняння поведінки досліджуваного ПЗ з поведінками в базі. У випадку виявлення ШПЗ його виконання блокується.

ЕКСПЕРИМЕНТИ. Для оцінки ефективності пропонованого методу було проведено ряд експериментів. З цією метою було згенеровано 500 поведінок функціонування шкідливого програмного забезпечення типу backdoor чотирьох типів, які здійснюють DoS (Denial of Service) атаки, R2L атаки (несанкціонований доступ до комп'ютерної системи), 2Su атаки (надання привілейованих прав шкідливим додаткам), Probing-атаки (несанкціоноване стеження за діями користувача. Для виявлення хибних спрацювань також було згенеровані для експериментів поведінок корисного ПЗ.

Для класифікації було використано WEKA Plug-in [16]. Реалізація алгоритму клональної селекції дозволило здійснити налаштування наступних параметрів алгоритму класифікації CLONALG:

- розмір пулу антитіл (*N*) – загальна кількість антитіл в системі (в подальшому розподіляється на пул пам'яті та пул залишку антитіл);
- коефіцієнт клонування (β) – коефіцієнт, що використовується для масштабування кількості клонів, створених для кожного обраного антитіла;
- кількість поколінь (*G*) – загальне число поколінь, де одне покоління складається з ітерації для всіх антигенів;
- пул залишку антитіл – кількість усіх антитіл (*r*) для розміщення в пулі залишку антитіл, які використовуються для вставки нових антитіл;
- початкове значення для генератора випадкових чисел, *s*;
- розмір секцій в пулі (*n*) – загальна кількість антитіл, що вибирається з усього пулу антитіл для представлення кожного антигену;
- загальна кількість перестановок (*p*) – загальна кількість нових випадкових антитіл для вставки в пул залишку антитіл для представлення кожного антигену.

Значення параметрів алгоритму класифікації представлено в таблиці 1.

Результати експериментів виявлення шкідливого програмного забезпечення із залученням алгоритму клонального відбору представлено в таблиці 2.

Результати експериментальних досліджень дозволяють зробити висновок, що залучення алгоритму клонального відбору демонструє високі показники виявлення ШПЗ типу backdoor. Так загальна ефективність виявлення склала понад 95%, але при цьому показник хибних спрацювань наразі також достатньо високий (6%), що зумовлює необхідність удосконалення методу та пошуку оптимальних параметрів алгоритму.

Таблиця 1

Параметри алгоритму клонального відбору

Параметр алгоритму	Значення параметра алгоритму
*розмір пулу антитіл (*N*)*	500
*коефіцієнт клонування (*β*)*	1.0
*кількість поколінь (*G*)*	1000
*пул залишку антитіл (*r*)*	10
*початкове значення для генератора випадкових чисел (*s*)*	1
*розмір секцій в пулі (*n*)*	20
*загальна кількість перестановок (*p*)*	5

Таблиця 2

Результати виявлення ШПЗ типу backdoor

Параметр алгоритму	Вірно класифікованих об'єктів (true positives)	Невірно класифікованих об'єктів (false positives)
ШПЗ типу backdoor	477	23
Ефективність виявлення	95,4	4,6

Таким чином, запропонований метод продемонстрував можливість здійснення класифікації програмного забезпечення на корисне та ШПЗ типу backdoor з високою достовірністю.

ВИСНОВКИ. У цій статті розроблено метод виявлення шкідливого програмного забезпечення на основі алгоритму штучних імунних систем – алгоритму клонального відбору. Експериментальні результати показують, що запропонований метод здатний здійснювати виявлення шкідливого програмного забезпечення типу backdoor з високою ефективністю, яка складає понад 95%. Запропонований метод може бути основою для побудови програмного забезпечення для антивірусного діагностування.

Література

1. The cyber threats [Електронний ресурс] // Інформаційний портал Інтерполу. – Режим доступу : https://www.interpol.int/Crime-areas/Cybercrime / The-threats/Malware (дата звернення 23.03.2018).

2. Scott J. Signature Based Malware Detection is Dead / J. Scott, Sr. Fellow // ICITC , vol 1, 2017. – P. 5–12.

3. Javed A. Patterns in Malware Designed for Data Espionage and Backdoor Creation / A. Javed, M. Akhlaq // 12th International Confrence on Applied Sciences and Technology(IBCAST), 2015, pp. 338–342.

4. Thimmaraju K. Software-Defined Adversarial Trajectory Sampling / K. Thimmaraju, L. Schiff, S. Schmid // Arhiv: 1705.0037, vol 1, 2017, pp. 8–12.

5. Fichte J. K. Strong Backdoors for Default Logic / J.K. Fichte, A. Meier, I. Schindler // Arhiv: 1602.06052, vol 1, 2016, pp. 6–10.

6. Diksha N. Backdoor Intrusion in Wireless Networks-problems an solutions / N.Diksha, A. Shubham // Indian Institute of Information Technology-Allahabad, Deoghat- Jhalwa, Allahabad- 211011, 2006, pp. 1–4.

7. Dickerson J.E. Fuzzy Intrusion Detection / J.E. Dickerson, J. Juslin, O. Koukousoula, J.A. Dickerso // Electrical and Computer Engineering Department, 0-7803-7078-3/0l/$10~00 (C)2001 IEEE, pp. 1506–1510.

8. Dasgupta Dipankar Artificial Immune Systems and Their Applications / Dasgupta Dipankar // Springer: ISBN 978-3-642-59901-9, 1999. – 306 p.

9. Youssef A. A review of the clonal selection algorithm as an optimization method / A. Youssef, M. Galal and Mohamed M. ALADL // Leonardo Journal of Sciences. 2015. – vol. 1, p. 10.

10. Dudek G. An artificial immune system for classification with local feature selection / G. Dudek // IEEE Transactions on Evolutionary Computation, 2012, 16(6), p. 847–60.

11. Farmer J. D. The immune system adaptation and machine learning / J. D. Farmer, N. H. Packard, A.S. Perelson // Physica D: Nonlinear Phenomena, 1986, 22(1), p. 187–204.

12. Wu J.Y. Artificial immune system for solving constrained global optimization problems / J.Y. Wu // IEEE Symposium on Artificial Life, 2007, pp. 92–99.

13. Aickelin U. Artificial immune systems / U. Aickelin D. Dasgupta, F. Gu, // InSearch Methodologies, 2014, pp. 187–211.

14. De Castro L. N. An artificial immune network for multimodal function optimization / L. N. De Castro, J. Timmis // Evolutionary Computation, 2002. CEC'02. Proceedings of the 2002 Congress, 2002, 1, p. 699–704.

15. Brownlee J. Clonal Selection Theory & Clonalg The Clonal Selection Classification Algorithm (Csca) / J. Brownlee // Technical Report No. 2-02 Swinburne University of Technology (SUT) January 2005.

16. WEKA Classification Algorithms [Електронний ресурс] // The WEKA project. – Режим доступу : http://wekaclassalgos.sourceforge.net/. – (дата звернення 23.03.2018).

References

1. The cyber threats [Elektronnyi resurs] // Informatsiinyi portal Interpolu. – Rezhym dostupu : https://www.interpol.int/Crime-areas/Cybercrime / The-threats/Malware (data zvernennia 23.03.2018).

2. Scott J. Signature Based Malware Detection is Dead / J. Scott, Sr. Fellow // ICITC , vol 1, 2017. – R. 5–12.

3. Javed A. Patterns in Malware Designed for Data Espionage and Backdoor Creation / A. Javed, M. Akhlaq // 12th International Confrence on Applied Sciences and Technology(IBCAST), 2015, pp. 338–342.

4. Thimmaraju K. Software-Defined Adversarial Trajectory Sampling / K. Thimmaraju, L. Schiff, S. Schmid // Arhiv: 1705.0037, vol 1, 2017, pp. 8–12.

5. Fichte J. K. Strong Backdoors for Default Logic / J.K. Fichte, A. Meier, I. Schindler // Arhiv: 1602.06052, vol 1, 2016, pp. 6–10.

6. Diksha N. Backdoor Intrusion in Wireless Networks-problems an solutions / N.Diksha, A. Shubham // Indian Institute of Information Technology-Allahabad, Deoghat- Jhalwa, Allahabad- 211011, 2006, pp. 1–4.

7. Dickerson J.E. Fuzzy Intrusion Detection / J.E. Dickerson, J. Juslin, O. Koukousoula, J.A. Dickerso // Electrical and Computer Engineering Department, 0-7803-7078-3/0l/$10~00 (C)2001 IEEE, pp. 1506–1510.

8. Dasgupta Dipankar Artificial Immune Systems and Their Applications / Dasgupta Dipankar // Springer: ISBN 978-3-642-59901-9, 1999. – 306 p.

9. Youssef A. A review of the clonal selection algorithm as an optimization method / A. Youssef, M. Galal and Mohamed M. ALADL // Leonardo Journal of Sciences. 2015. – vol. 1, p. 10.

10. Dudek G. An artificial immune system for classification with local feature selection / G. Dudek // IEEE Transactions on Evolutionary Computation, 2012, 16(6), p. 847–60.

11. Farmer J. D. The immune system adaptation and machine learning / J. D. Farmer, N. H. Packard, A.S. Perelson // Physica D: Nonlinear Phenomena, 1986, 22(1), p. 187–204.

12. Wu J.Y. Artificial immune system for solving constrained global optimization problems / J.Y. Wu // IEEE Symposium on Artificial Life, 2007, pp. 92–99.

13. Aickelin U. Artificial immune systems / U. Aickelin D. Dasgupta, F. Gu, // InSearch Methodologies, 2014, pp. 187–211.

14. De Castro L. N. An artificial immune network for multimodal function optimization / L. N. De Castro, J. Timmis // Evolutionary Computation, 2002. CEC02. Proceedings of the 2002 Congress, 2002, 1, p. 699–704.

15. Brownlee J. Clonal Selection Theory & Clonalg The Clonal Selection Classification Algorithm (Csca) / J. Brownlee // Technical Report No. 2-02 Swinburne University of Technology (SUT) January 2005.

16. WEKA Classification Algorithms [Elektronnyi resurs] // The WEKA project. – Rezhym dostupu : http://wekaclassalgos.sourceforge.net/. – (data zvernennia 23.03.2018).