DOI 10.31891/2307-5732-2025-347-74
УДК 004.491.42

ЧАЙКОВСЬКИЙ МАКСИМ
Хмельницький національний університет
https://orcid.org/0000-0002-9596-6697
e-mail: max.chaikovskyi@gmail.com

МОДЕЛЬ МУЛЬТИАГЕНТНОЇ СИСТЕМИ ДЛЯ ВИЯВЛЕННЯ ПОЛІМОРФНИХ ВІРУСІВ

У роботі встановлено, що мультиагентні системи (MAS) є потужним інструментом для виявлення поліморфних вірусів. Визначені основні переваги використання MAS для виявлення поліморфних вірусів: паралельна обробка та ефективність; розподілене виявлення загроз; інтелектуальна взаємодія між агентами; адаптивність до нових загроз; масштабованість; прогнозування та виявлення аномалій; динамічне реагування на загрози; розподілене навчання на основі досвіду; зниження навантаження на одну точку системи. Запропонована модель мультиагентної системи (MAS) виявлення поліморфних вірусів, яка включає: множину агентів; множину станів комп'ютерної системи; множину можливих дій агента; функцію переходу між станами; функцію винагороди, яка оцінює ефективність вибраних дій; функцію спостереження, яка визначає, яку інформацію отримує кожен агент; ймовірність переходу в новий стан після виконання дій агентами; стратегію агента, яка визначає, яку дію він обирає в кожному стані. Інтелектуальний агент даної MAS складається з наступних модулів: модуль аналізу, модуль класифікації поліморфних вірусів за рівнями складності, модуль прийняття рішення. Алгоритм роботи запропонованої MAS: збір інформації, виявлення поліморфних вірусів, класифікація поліморфних вірусів, прийняття рішення.

Ключові слова: поліморфний вірус, інтелектуальний агент, мультиагентна система.

CHAIKOVSKYI MAKSYM
Khmelnytskyi National University

MULTIAGENT SYSTEM MODEL FOR DETECTION OF POLYMORPHIC VIRUSES

The paper establishes that multi-agent systems (MAS) are a powerful tool for detecting polymorphic viruses. Such a system uses several intelligent agents (IAs), each of which has its own specific role in the process of detecting and trawling polymorphic viruses. he concept of multi-agent systems (MAS) has become an important topic of interest in the field of artificial intelligence. The main advantages of using MAS for detecting polymorphic viruses are identified: parallel processing and efficiency; distributed threat detection; intelligent interaction between agents; adaptability to new threats; scalability; prediction and detection of anomalies; dynamic response to threats; distributed learning based on experience; reducing the load on one point of the system. A model of a multi-agent system (MAS) for detecting polymorphic viruses is proposed, which includes: a set of agents; a set of computer system states; a set of possible agent actions; a transition function between states; a reward function that evaluates the effectiveness of selected actions; a monitoring function that determines what information each agent receives; the probability of transitioning to a new state after the agents perform actions; an agent strategy that determines what action it chooses in each state. The intelligent agent of this MAS consists of the following modules: an analysis module, a module for classifying polymorphic viruses by complexity levels, and a decision-making module. Agents operate in an environment and can cooperate or compete. They operate according to an algorithm. The algorithm of the proposed MAS: information collection, detection of polymorphic viruses, classification of polymorphic viruses, decision making.

Keywords: polymorphic virus, intelligent agent, multiagent system.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Мультиагентні системи (MAS) є потужним інструментом для виявлення вірусів, оскільки забезпечують високу ефективність, масштабованість, адаптивність та здатність до колективного аналізу загроз. Вони дозволяють створювати розподілені, інтегровані рішення для виявлення та нейтралізації вірусів, що є особливо важливим у боротьбі з сучасними складними та змінюваними загрозами. Оскільки така система використовує кілька агентів, кожен з яких має свою специфічну роль у процесі виявлення та нейтралізації вірусів, тому доцільним є її розробка для виявлення поліморфних вірусів.

Аналіз останніх досліджень і публікацій

Серед науковців, які досліджували різні аспекти виявлення зловмисного програмного забезпечення слід відзначити: Савенко О., Лисенко С., Нічепорук А., Кашталян А., Савенко Б., Крищук А. [8-13, 16] та ін.

Концепція багатоагентних систем (MAS) стала важливою темою інтересів у сфері штучного інтелекту [2, 6, 7]. В основі цих систем лежать IA, які є суб'єктами, здатними сприймати навколишнє середовище та виконувати дії самостійно або у співпраці з іншими для досягнення конкретних цілей.

До основних переваг використання MAS для виявлення поліморфних вірусів є:

1) паралельна обробка та ефективність: MAS складаються з кількох агентів, що працюють одночасно, виконуючи різні функції. Це дозволяє здійснювати паралельну обробку великої кількості даних (файлів, мережевого трафіку, системних журналів), що значно підвищує ефективність виявлення вірусів. Кожен агент може відповідати за окрему задачу (аналіз файлів, моніторинг процесів, сканування трафіку), що пришвидшує виявлення та нейтралізацію загроз;

2) розподілене виявлення загроз: у MAS агенти можуть бути розподілені по різних сегментах мережі або різних частинах комп'ютерної системи. Це дозволяє забезпечити глобальний моніторинг системи на всіх рівнях, що дає змогу виявляти загрози навіть у найвіддаленіших її частинах, які можуть бути не помічені традиційними методами;

3) інтелектуальна взаємодія між агентами: агентам у MAS доступна можливість взаємодії для обміну інформацією та прийняття рішень спільно. Якщо один агент виявляє потенційну загрозу, інші агенти можуть бути повідомлені, щоб проаналізувати її з різних аспектів (наприклад, один агент може перевірити мережевий трафік, інший — аналізувати поведінку програм). Це дозволяє швидко і точно виявляти нові види вірусів, які можуть маскуватися різними способами;

4) адаптивність до нових загроз: MAS можуть включати агентів, здатних самонавчатися, застосовуючи методи машинного навчання або еволюційні алгоритми. Це дозволяє агентам адаптуватися до нових типів загроз, виявляти невідомі віруси та реагувати на зміни у поведінці вірусів, що змінюють свою структуру або використовують нові техніки атак;

5) масштабованість: MAS дуже зручні для масштабованих середовищ. Якщо система стає більша або складніша (наприклад, з'являються нові сервери або пристрої), можна просто додавати нових агентів для розширення можливостей виявлення вірусів. Це робить такі системи зручними для великих організацій, хмарних платформ або великих мереж;

6) прогнозування та виявлення аномалій: в одному агенті можна реалізувати методи для прогнозування поведінки системи, а інший агент може виявляти аномалії в реальному часі. Це дозволяє виявити навіть загрози, які можуть не мати чіткої сигнатури або діяти дуже непомітно, на приклад, через використання нестандартних шляхів проникнення;

7) динамічне реагування на загрози: MAS дозволяють організувати динамічну реакцію на вірусні загрози. Кожен агент може мати свою стратегію реагування: ізоляція заражених файлів, блокування підозрілих процесів, повідомлення адміністратора або навіть автоматичне видалення шкідливих файлів. Це дає змогу швидко нейтралізувати загрози без ручного втручання;

8) розподілене навчання на основі досвіду: MAS можуть використовувати спільне навчання та обмін досвідом між агентами, що покращує виявлення нових загроз. Один агент може поділитися знаннями про новий тип вірусу, а інші агенти можуть швидко застосувати ці знання в інших частинах системи;

9) зниження навантаження на одну точку системи: замість того, щоб покладатися на один центральний процес, який перевіряє всі дані, мультиагентна система дозволяє розподіляти навантаження, що підвищує продуктивність та ефективність виявлення вірусів. Це особливо корисно в великих, складних або розподілених системах.

У роботі [15] Рохан Монга і Камалакар Карлапалем розробили структуру на основі багатоагентних систем (MASFMMS - Multi Agent Systems Framework for Malware Modeling and Simulation) для моделювання ефекту та поширення ЗПЗ в комп'ютерній мережі.

У роботі [3] Імен Брахмі, Садок Бен Яхія та ін. запропонували розподілену систему виявлення вторгнень (MAD-IDS), яка об'єднує бажані функції, надані багатоагентною методологією, з високою точністю методів інтелектуального аналізу даних.

Р. Абідар, К. Муммаді, Ф. Мутауаккіль, Х. Медромі у роботі [1] представили інтелектуальну та поширену платформу контролю безпеки інформаційної системи (ІС) на основі MAS, яка виявляє та класифікує події ЗПЗ, які виникають на програмних і апаратних компонентах, і надсилає сповіщення в режимі реального часу користувачам смартфонів.

У роботі [14] Рафаель Салема Маркес, Грегорі Епіфаніу та ін. запропонували нову архітектуру багатоагентного детектора ексфільтрації даних (MADEX), який натхненний механізмами та функціями імунної системи людини.

У роботі [17] Вівек Кумар Сінгх, Алтай Озен, Манімаран Говіндарасу представили підхід до розробки багатоагентної схеми RAS проти системних таємних кібератак.

Виділення невирішених раніше частин загальної проблеми, котрим присвячується стаття.

Зважаючи на значну кількість досліджень у даному напрямку, питання актуальної архітектури MAS для виявлення поліморфних вірусів вивчено недостатньо та вимагає подальших досліджень.

Формулювання цілей статті

Метою статті є розробка моделі MAS для виявлення поліморфних вірусів.

Виклад основного матеріалу

MAS є потужним підходом для забезпечення безпеки комп'ютерних мереж і систем. Така система використовує кілька інтелектуальних агентів (ІА), кожен з яких має свою специфічну роль у процесі виявлення та нейтралізації поліморфних вірусів. На основі попередніх досліджень автора [4, 5, 18-20] розроблена архітектура MAS для виявлення поліморфних вірусів. Основні компоненти такої системи відображені на рисунку 1.

Як відображено на рисунку 1, ІА складається з наступних модулів:

1) модуль аналізу – сканує систему на предмет наявності підозрілих або шкідливих активностей, аналізує файлову систему, пам'ять, мережевий трафік, поведінку процесів. При цьому можуть використовуватися сигнатурний аналіз (порівняння з базою відомих вірусів), аналіз поведінки

(пошук аномалій, підозрілих дій), евристичний аналіз (виявлення нових вірусів на основі ознак). Іншими словами, відбувається збір даних, пов'язаних із ЗПЗ, і проводиться детальний аналіз для визначення природи загрози, її джерела та потенційного впливу;

2) модуль класифікації поліморфних вірусів за рівнями складності – здійснює нечітку класифікацію виявлених поліморфних вірусів згідно його належності до різних рівнів складності та визначає їх рівень небезпеки;

3) модуль прийняття рішення – визначається оптимальна реакція та нейтралізація (карантин, видалення, оповіщення, блокування), відбувається оновлення бази знань та стратегій виявлення.

Алгоритм роботи представленої MAS відображено на рисунку 2.

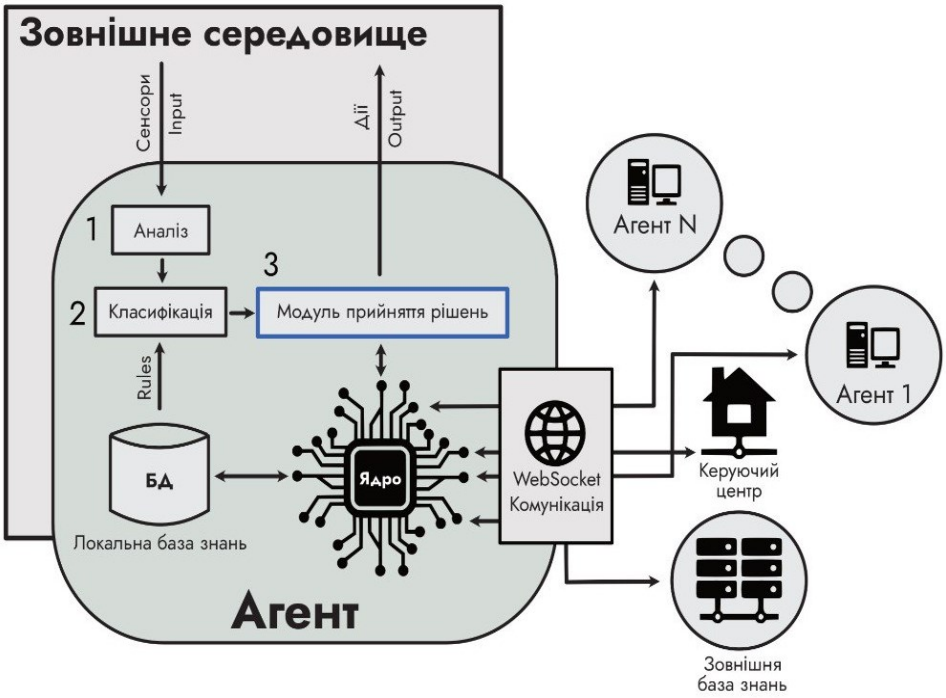

Рис.1. Архітектура мультиагентної системи виявлення поліморфних вірусів

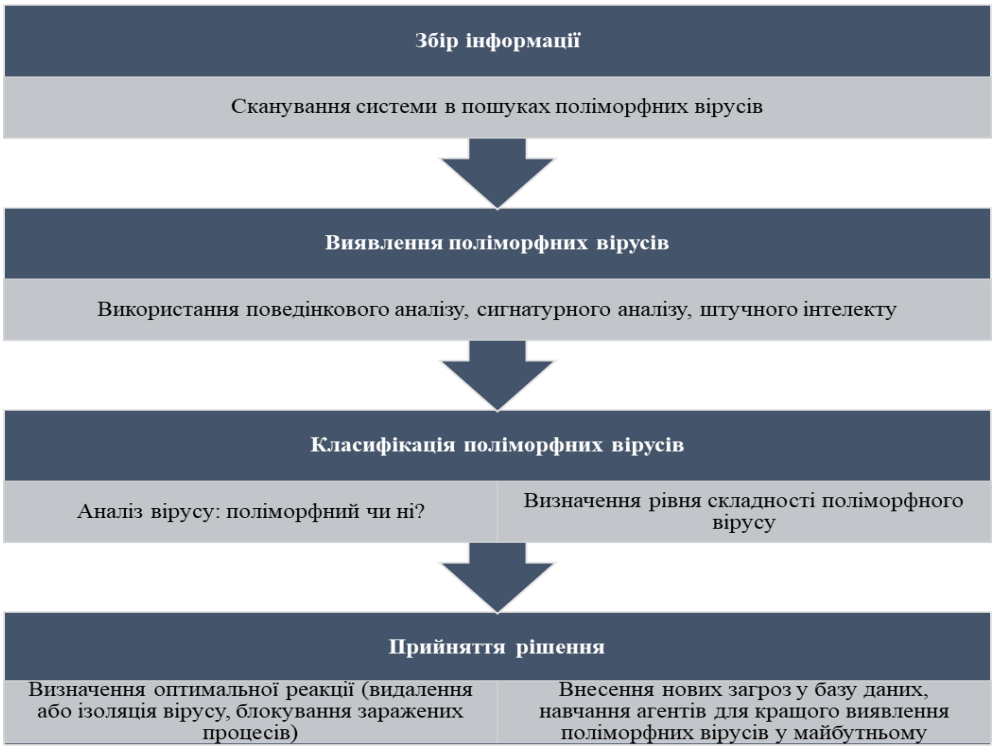

Рис. 2. Алгоритм роботи запропонованої MAS

MAS моделюється як сукупність агентів $A = \{A_1, A_2, ..., A_n\}$, які взаємодіють із комп'ютерною системою та один з одним.

MAS визначається кортежем:

$$MAS = \langle A, S, D, T, R, O, P, \pi \rangle, \quad (1)$$

де $A = \{A_1, A_2, ..., An\}$ – множина агентів; S – множина станів комп'ютерної системи; D_i – множина можливих дій агента A_i; $T : S \times A_1 \times A_2 \times ... \times A_n \rightarrow P(S)$ – функція переходу між станами; $R : S \times A_1 \times A_2 \times ... \times A_n \rightarrow R$ – функція винагороди, яка оцінює ефективність вибраних дій; $O : A \times S \rightarrow P(O)$ – функція спостереження, яка визначає, яку інформацію отримує кожен агент; $P(s'/s, a_1, ..., a_n)$ – ймовірність переходу в стан s' після виконання дій агентами; $\pi_i : S \rightarrow A_i$ – стратегія агента A_i, яка визначає, яку дію він обирає в кожному стані.

Агенти діють у середовищі та можуть співпрацювати або конкурувати. Вони функціонують згідно алгоритму:

1. Агент спостерігає стан s частково через $O(A_i, s)$.
2. Агент вибирає дію a_i відповідно до своєї стратегії $\pi_i(s)$.
3. Агент отримує винагороду $R(s, a_1, ..., a_n)$.
4. Система переходить у новий стан s′ згідно з функцією переходу $P(s'/s, a_1, ..., a_n)$.

Формально, оптимальна стратегія для агента A_i визначається як:

$$\pi_i^* = arg \max_{\pi_i} E(\sum_{t=0}^{\infty} \gamma^t R(s_t, a_{1,t}, \dots, a_{n,t}), \quad (2)$$

де γ – коефіцієнт дисконтування (важливість майбутніх винагород); E – математичне очікування.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У дослідженні запропонована модель MAS для виявлення поліморфних вірусів, яка включає: множину агентів; множину станів комп'ютерної системи; множину можливих дій агента; функцію переходу між станами; функцію винагороди, яка оцінює ефективність вибраних дій; функцію спостереження, яка визначає, яку інформацію отримує кожен агент; ймовірність переходу в новий стан після виконання дій агентами; стратегію агента, яка визначає, яку дію він обирає в кожному стані. Інтелектуальний агент даної MAS складається з наступних модулів: модуль аналізу, модуль класифікації поліморфних вірусів за рівнями складності, модуль прийняття рішення. Алгоритм роботи запропонованої MAS: збір інформації, виявлення поліморфних вірусів, класифікація поліморфних вірусів, прийняття рішення.

Література

1. Abidar R., Moummadi K., Moutaouakkil F., Medromi H. Intelligent and Pervasive Supervising Platform for Information System Security Based on Multi-Agent Systems. *International Review on Computers and Software (IRECOS)*. 2015. Vol. 10 (1). URL: https://doi.org/10.15866/irecos.v10i1.4699
2. Ahmed M., Kazar O., Harous S. Cyber-physical system model based on multi-agent system. *IET Cyber-Physical Systems: Theory & Applications*, 2024, pp. 1-11. https://doi.org/10.1049/cps2.12096
3. Brahmi I., Ben Yahia S., Aouadi H., Poncelet P. (2012). Towards a Multiagent-Based Distributed Intrusion Detection System Using Data Mining Approaches. *Lecture Notes in Computer Science*. 2012. Vol. 7103. URL: https://doi.org/10.1007/978-3-642-27609-5_12
4. Chaikovskyi M., Chaikovska I., Sochor T., Martyniuk I., Lyhun O. Comprehensive approach to the detection and analysis of polymorphic malware. CEUR Workshop Proceedings (ISSN 1613-0073). 2024. Vol.3736. P.312-323. URL: https://ceur-ws.org/Vol-3736/paper23.pdf
5. Chaikovskyi M., Chaikovska I., Sochor T., Martyniuk I., Lyhun O. Modeling the detection process of polymorphic malware based on the Lotka-Volterra Model. *CEUR Workshop Proceedings* (ISSN 1613-0073). - 2024. - Vol.3899. - P.244-253. URL: https://ceur-ws.org/Vol-3899/paper22.pdf
6. Dunets O., Wolff C., Sachenko A., Hladiy G., Dobrotvor I. Multi-agent system of IT project planning. *In Proc. of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Bucharest, Romania, 2017, pp. 548-552. doi: https://doi.org/10.1109/IDAACS.2017.8095141
7. Harshvardhan U., Rastgoftar H. Multi-Layer Continuum Deformation Optimization of Multi-Agent Systems. *IFAC-PapersOnLine*. no. 56 (2), 2023, pp. 10222-10227. https://doi.org/10.1016/j.ifacol.2023.10.901
8. Kashtalian A., Lysenko S., Savenko B., Sochor T., Kysil T. Principle and method of deception systems synthesizing for malware and computer attacks detection. *Radioelectronic and Computer Systems*. 2023, no. 4, pp. 112-151. https://doi.org/10.32620/reks.2023.4.10
9. Kashtalian A., Lysenko S., Savenko O., Nicheporuk A., Sochor T., Avsiyevych V. Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*. 2024, no. 1, pp. 152-175. https://doi.org/10.32620/reks.2024.1.13
10. Lysenko S., Pomorova O., Savenko O., Kryshchuk A., Bobrovnikova K. 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, 2015, pp. 453–458.

11. Lysenko S., Savenko B. Distributed Discrete Malware Detection Systems Based on Partial Centralization and Self-Organization. *International Journal of Computing*. 2023. Vol. 22. Pp. 117-139. DOI: https://doi.org/10.47839/ijc.22.2.3082

12. Lysenko S., Savenko O., Bobrovnikova K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. *CEUR-WS*, no.2104, 2018, pp. 688-695.

13. Markowsky G., Savenko O., Lysenko S., Nicheporuk A. The technique for metamorphic viruses' detection based on its obfuscation features analysis, CEUR-WS 2104 (2018): 680–687.

14. Marques R.S., Epiphaniou G., Al-Khateeb H. et al. A flow-based multi-agent data exfiltration detection architecture for ultra-low latency networks. *ACM Transactions on Internet Technology*. 2021. Vol. 21 (4). 103. URL: https://doi.org/10.1145/3419103

15. Monga R., Karlapalem K. MASFMMS: Multi Agent Systems Framework for Malware Modeling and Simulation. *Lecture Notes in Computer Science*. 2009. Vol. 5269. URL: https://doi.org/10.1007/978-3-642-01991-3_8

16. 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, no. 370, pp.243-254. https://doi.org/10.1007/978-3-642-38865-1_16

17. Singh V. K., Ozen A., Govindarasu M. A Hierarchical Multi-Agent Based Anomaly Detection for Wide-Area Protection in Smart Grid. *2018 Resilience Week (RWS)*, Denver, CO, USA. 2018. Pp. 63-69. URL: https://doi.org/10.1109/RWEEK.2018.8473514

18. Савенко О., Чайковський М. Метод нечіткої класифікації зловмисного програмного забезпечення з використанням інтелектуального агента. Information Technology: Computer Science, Software Engineering and Cyber Security. 2024. № 3. С. 140-148. URL: https://journals.politehnica.dp.ua/index.php/it/article/view/644/574

19. Чайковський М. Комплексний підхід до виявлення та аналізу поліморфного зловмисного програмного забезпечення. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». 2024. № 2. С. 42-50. URL: https://doi.org/10.31891/2219-9365-2024-78-5

20. Чайковський М.Ю. Прогнозування кількості атак зловмисного програмного забезпечення у світі. Актуальні проблеми комп'ютерних наук АПКН-2024 : матеріали XVI всеукр. наук.-практ. конф., м. Хмельницький, 15-16 лист. 2024 р. / Хмельницький національний університет. Хмельницький, 2024. С. 534-536.