

## АНОТАЦІЯ

*Дрозд А.І.* Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія. – Хмельницький національний університет, Хмельницький, 2026.

У роботі подано результати дослідження, спрямованого на підвищення ефективності протидії зловмисним діям у корпоративних мережах шляхом удосконалення архітектури та методів функціонування обманних систем з приманками і пастками (ОСПП). Запропоновано оновлену архітектуру таких систем, у якій синтезовано популяційні алгоритми, зокрема алгоритм молі й полум'я, що забезпечує оптимізацію формування послідовностей кроків у процесі реалізації комп'ютерних атак і дій зловмисного програмного забезпечення. Завдяки цьому досягається уникнення повного перебору можливих варіантів, прискорення збіжності рішень під час динамічних змін у середовищі корпоративної мережі та врахування потенційної здатності зловмисників здійснювати двоцільові атаки.

У дисертації здійснено аналіз архітектури сучасних обманних систем, методів їх організації функціонування, методів виявлення комп'ютерних атак та типів популяційних алгоритмів, які можуть бути синтезовані в архітектурі ОСПП. В роботі представлено архітектуру ОСПП, в якій синтезовано алгоритм молі і полум'я для покращення їх функціонування під час атак, моделі двоцільових комп'ютерних атак, метод синтезу алгоритму дискретної оптимізації молі й полум'я в архітектурі ОСПП, метод організації функціонування ОСПП в корпоративних мережах, метод виявлення атак відмова в обслуговуванні у мережах на основі статистичних показників, а також розроблено відповідну обманну систему, здійснено постановку експериментів та проведені дослідження із розробленою системою.

*Об'єктом дослідження* є процес організації обманних систем з приманками і пастками для виявлення комп'ютерних атак та зловмисного програмного забезпечення в корпоративних мережах.



*Предметом дослідження є методи організації обманних систем з приманками і пастками для виявлення комп'ютерних атак та зловмисного програмного забезпечення в корпоративних мережах.*

*Метою дисертаційного дослідження є покращення протидії комп'ютерним атакам та зловмисному програмному забезпеченню в корпоративних мережах шляхом оптимізації кроків обманних систем з приманками і пастками за рахунок синтезу популяційних алгоритмів в центрах прийняття рішень.*

Наукова новизна отриманих результатів полягає в наступному:

1) удосконалено архітектуру обманних систем з приманками і пастками, в якій на відміну від відомих варіантів архітектури, здійснено синтез популяційних алгоритмів, зокрема алгоритму молі і полум'я, для оптимізації формування послідовності наступних кроків при здійсненні КА та дій ЗПЗ, уникнення повного перебору варіантів, швидкої збіжності обраних кроків при триваючих впливах та зміни послідовності кроків з врахуванням поточних змін в оточуючому середовищі корпоративних мереж, а також врахування потенційної спроможності зловмисників до здійснення двоцільових КА;

2) розроблено новий метод синтезу алгоритму дискретної оптимізації молі й полум'я в архітектурі обманних систем з приманками і пастками, який, на відміну від відомих, характеризується формуванням дискретного простору пошуку з координатним поданням об'єктів, синтезом спірального сліду на основі секторного оцінювання потенційних кроків і кутових характеристик, урахуванням часу як параметра зміни кроків та динамічним переміщенням молі й полум'я для уникнення передчасної збіжності до локальних оптимумів, що дало змогу розробляти обманні системи, які забезпечують довготривале й адаптивне функціонування у процесі протидії зловмисникам у корпоративних мережах за рахунок зміни кроків для опрацювання подій;

3) розроблено новий метод організації функціонування обманних систем з приманками і пастками в корпоративних мережах, в якому на відміну від відомих, в архітектурі обманних систем синтезовано популяційні алгоритми, зокрема алгоритм молі і полум'я, для здійснення ними вибору наступних кроків для уникнення реалізації зловмисниками двоцільових атак, що дає змогу уникати повного перебору варіантів з можливих кроків, швидкої збіжності обраних кроків при триваючих



впливах та зміну послідовності кроків з врахуванням поточних змін в оточуючому середовищі корпоративних мереж та ускладнює дії за рахунок прийняття рішень на основі популяційних алгоритмів з можливістю самостійно блокувати або активувати сервери чи комп'ютерні станції, приманки чи пастки під час встановлення потенційно зловмисних впливів в корпоративних мережах;

4) розроблено новий метод виявлення атак відмови в обслуговуванні у мережах на основі статистичних показників, який на відміну від відомих, базується на обчисленні статистичних ознак мережного IP-трафіку при розбитті потоку пакетів на часові вікна, і встановлює динамічні зміни трафіку на рівні всього аналізованого періоду, що дозволяє підвищити достовірність виявлення атак відмова в обслуговуванні.

Практичне значення отриманих результатів. Розроблено обманну систему з приманками і пастками для виявлення КА та ЗПЗ в корпоративних мережах, особливістю якої є прийняття в ній рішень щодо наступних кроків та їх коригування з використанням алгоритму дискретної оптимізації молі і полум'я, а також імплементацією в її компонентах методу виявлення комп'ютерних атак на основі аналізу їх статичних показників.

Синтез популяційних алгоритмів в архітектурі обманних систем для прийняття ними рішень дав змогу формувати послідовності кроків систем так, щоб залучати зловмисників при проведенні КА. Також, в процесі синтезу алгоритму молі і полум'я в архітектуру обманних систем було здійснено розроблення його кроків та адаптації для реалізації саме для задач дискретної оптимізації, що є основою для здійснення аналогічних кроків в процесі деталізації інших популяційних алгоритмів натхнених живою природою.

За результатами проведених експериментальних досліджень встановлено, що розроблена ОСПП забезпечує коректне функціонування в умовах динамічної зміни оточуючого середовища корпоративних мереж, ефективно залучення приманок і пасток для виконання задач виявлення інфікованих програм, а також вибір наступних кроків для виконання.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «Nolt technologies» (м. Хмельницький, Акт від 16.02.2026), ТОВ «ІТТ» (м. Хмельницький Акт від 16.02.2026), а також, в освітньому процесі Хмельницького національного



університету (Акт від 25.02.2026) при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для здобувачів спеціальності F7 Комп'ютерна інженерія, зокрема в курсах «Безпека та захист комп'ютерних систем», «Моделювання та методи оптимізації в наукових та експериментальних дослідженнях», «Методології забезпечення якості, надійності, гарантоздатності та безпеки комп'ютерних систем та мереж» та в освітній процес у блоці військово-спеціальних дисциплін другої кафедри Другого навчально-наукового інституту Воєнної академії імені Євгенія Березняка (Акт від 18.12.2025), які використані при удосконаленні навчально-лабораторного комплексу.

У вступі представлено обґрунтування актуальності наукової задачі, що полягає у підвищенні ефективності протидії зловмисним діям у корпоративних мережах шляхом удосконалення архітектури та методів функціонування ОСПП. Важливим напрямком досліджень визначено обманні системи, рішення в яких формуються на основі популяційних алгоритмів. Продемонстровано зв'язок тематики дослідження з напрямками наукових досліджень науковців з цієї тематики, представлено основні наукові результати роботи, їх практичне використання, перелік підприємств та установ, в яких впроваджено результат роботи.

У першому розділі проведено аналіз предметної області дослідження, існуючих обманних систем, приманок і пасток, методів, що застосовуються для виявлення комп'ютерних атак та зловмисного програмного забезпечення. Проаналізовано типи популяційних алгоритмів та їх особливості.

У другому розділі розроблено моделі двоцільових атак на корпоративні мережі та запропоновано удосконалену архітектуру ОСПП, в якій на відміну від відомих варіантів архітектури, здійснено синтез популяційних алгоритмів, зокрема алгоритму молі і полум'я, для оптимізації формування послідовності наступних кроків при здійсненні КА та дій ЗПЗ, уникнення повного перебору варіантів, швидкої збіжності обраних кроків при триваючих впливах та зміну послідовності кроків з врахуванням поточних змін в оточуючому середовищі корпоративних мереж, а також врахування потенційної спроможності зловмисників до здійснення двоцільових КА;

У третьому розділі представлено розроблений метод синтезу дискретного алгоритму молі й полум'я, який відрізняється формуванням дискретного простору пошуку, координатним поданням об'єктів, використанням секторного оцінювання



потенційних кроків, побудовою спірального сліду та урахуванням часу як параметра зміни кроків. Запропоноване динамічне переміщення молі та полум'я дозволяє уникати передчасної збіжності до локальних оптимумів і забезпечує довготривале адаптивне функціонування обманних систем за рахунок раціонального вибору послідовностей кроків під час опрацювання подій. Також, представлено розроблений метод організації функціонування обманних систем у корпоративних мережах, у межах якого популяційні алгоритми забезпечують автономний вибір подальших дій обманних компонентів з урахуванням змін у мережному середовищі. Це дає змогу ускладнювати діяльність зловмисників, запобігати реалізації двоцільових атак, формувати рішення без повного перебору варіантів та автоматично активувати або блокувати сервери чи станції залежно від характеру виявлених впливів.

У четвертому розділі представлено розроблений метод виявлення атак відмова в обслуговуванні, який ґрунтується на аналізі статистичних характеристик мережного трафіку, що формується при поділі потоку пакетів на часові вікна. Метод забезпечує відстеження динаміки змін трафіку на рівні всього досліджуваного періоду та підвищує достовірність і оперативність виявлення атак типу Denial of Service. Також, описано розроблені програмні частини обманних систем, особливості їх реалізації та використані бібліотеки для їх реалізації, що забезпечують працездатність реалізованої системи. Представлено проведені експерименти, оцінювання ефективності обманної системи, проведено аналіз з отриманих результатів.

У висновках представлено отримані наукові та практичні результати проведеного дослідження.

У додатках представлено наукові публікації, в яких відображено наукові результати роботи, акти впровадження результатів роботи, лістинг розробленого програмного забезпечення.

Ключові слова: комп'ютерні системи; корпоративні мережі; комп'ютерні станції; обманні системи; популяційні алгоритми; алгоритм молі і полум'я; пастка; приманка; зловмисне програмне забезпечення; комп'ютерні атаки; системи виявлення вторгнень; архітектура систем.



## ANNOTATION

*Drozd A.I.* Methods and systems for detecting computer attacks in corporate networks based on population algorithms. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in the field of knowledge 12 Information technologies in the specialty 123 Computer engineering. – Khmelnytskyi National University, Khmelnytskyi, 2026.

The paper presents the results of a study aimed at increasing the effectiveness of countering malicious actions in corporate networks by improving the architecture and methods of operation of deceptive systems with baits and traps. An updated architecture of such systems is proposed, in which population algorithms are synthesized, in particular, the moth and flame algorithm, which ensures optimization of the formation of sequences of steps in the process of implementing computer attacks and actions of malicious software. Thanks to this, it is possible to avoid a complete search of possible options, to accelerate the convergence of decisions during dynamic changes in the corporate network environment, and to take into account the potential ability of attackers to carry out dual-purpose attacks.

The dissertation analyzes the architecture of modern deception systems, methods of organizing their operation, methods of detecting computer attacks, and types of population algorithms that can be synthesized in the architecture of deception systems with decoys and traps. The work presents the architecture of deception systems with baits and traps, in which the algorithm of moth and fire is synthesized to improve their functioning during attacks, models of dual-target computer attacks, the method of synthesis of the algorithm of discrete optimization of moths and flames in the architecture of deception systems with baits and traps, the method of organizing the functioning of deception systems with baits and traps in corporate networks, the method of detecting denial of service attacks in networks based on statistical indicators, as well as a suitable cheating system was developed, experiments were set up and research was conducted with the developed system.

The object of the study is the process of organizing deceptive systems with baits and traps to detect computer attacks and malicious software in corporate networks.

The subject of the study is methods of organizing deceptive systems with baits and traps for detecting computer attacks and malicious software in corporate networks.

The aim of the dissertation research is to improve countermeasures against computer attacks and malicious software in corporate networks by optimizing the steps of deception



systems with decoys and traps due to the synthesis of population algorithms in decision-making centers.

The scientific novelty of the obtained results is as follows:

1) the architecture of deception systems with decoys and traps has been improved, in which, in contrast to known architectural options, the synthesis of population algorithms, in particular the moth and fire algorithm, has been carried out to optimize the formation of the sequence of the next steps in the implementation of KA and malicious software actions, avoiding a complete search of options, rapid convergence of the selected steps with ongoing influences and changing the sequence of steps taking into account current changes in the surrounding environment of corporate networks, as well as taking into account the potential ability of attackers to carry out dual-purpose KA;

2) a new method of synthesis of the discrete moth and flame algorithm in the architecture of decoy systems with decoys and traps has been developed, which, unlike the known ones, is characterized by the formation of a discrete search space with a coordinate representation of objects, the synthesis of a spiral trail based on the sectoral evaluation of potential steps and angular characteristics, taking into account time as a parameter of step change and dynamic movement of the moth and flame to avoid premature convergence to local optima, which made it possible to develop deceptive systems that ensure long-term and adaptive functioning in the process of countering intruders in corporate networks by changing the steps for processing events;

3) a new method of organizing the functioning of deception systems with baits and traps in corporate networks has been developed, in which, unlike the known, the architecture of deception systems synthesizes population algorithms, in particular the moth and fire algorithm, for their selection of the next steps to avoid the implementation of dual-purpose attacks by criminals, which makes it possible to avoid a complete selection of options from possible steps, rapid convergence of the selected steps with ongoing influences and a change in the sequence of steps taking into account current changes in the surrounding environment of corporate networks and complicates actions due to decision-making based on population algorithms with the ability to independently block or activate servers or computer stations, baits or traps during the establishment of potentially malicious influences in corporate networks;



4) a new method of detecting denial-of-service attacks in networks based on statistical indicators has been developed, which, unlike the known ones, is based on the calculation of statistical characteristics of network IP traffic when dividing the flow of packets into time windows, and establishes dynamic changes traffic at the level of the entire analyzed period, which allows to increase the reliability of detection of denial of service attacks.

Practical significance of the obtained results. A deceptive system with decoys and traps has been developed for the detection of KA and malicious software actions in corporate networks, the feature of which is decision-making in it regarding the next steps and their adjustment using the algorithm of discrete optimization of moths and flames, as well as the implementation in its components of the method of detecting computer attacks based on the analysis of their static indicators.

The synthesis of population algorithms in the architecture of deceptive systems for their decision-making made it possible to form a sequence of steps of the systems in such a way as to overwhelm the attackers during the execution of the KA. Also, in the process of synthesizing the moth and flame algorithm into the architecture of deceptive systems, its steps were developed and adapted for implementation specifically for discrete optimization problems, which is the basis for implementing similar steps in the process of detailing other population algorithms inspired by living nature.

According to the results of experimental studies, it was established that the developed deception system with baits and traps ensures correct functioning in the conditions of dynamic changes in the surrounding environment of corporate networks, effective involvement of baits and traps to perform the tasks of detecting infected programs, as well as the selection of the next steps for implementation.

The theoretical and practical results of the research are implemented in "Nolt technologies" LLC (Khmelnyskyi, act dated 18.02.2026), ITT LLC (Khmelnyskyi, act dated 16.02.2026), as well as in the educational process of the Khmelnyskyi National University (Act dated 25.02.2026) in the teaching of disciplines at the Department of Computer Engineering and Information Systems for students of the F7 Computer Engineering specialty, in particular in the courses "Security and protection of computer systems", "Modeling and optimization methods in scientific and experimental research", "Methodologies for ensuring the quality, reliability, warranty and security of computer systems and networks" and in the educational process in the block of military special



disciplines of the second department of the Second Educational and Scientific Institute of the Yevgeny Bereznyak Military Academy (Act dated 18.12.2025), which were used in the improvement of the educational and laboratory complex.

The introduction presents the justification of the relevance of the scientific task, which consists in increasing the effectiveness of countering malicious actions in corporate networks by improving the architecture and methods of functioning of deceptive systems with baits and traps. Deception systems, in which solutions are formed on the basis of population algorithms, are defined as an important area of research. The connection of the research topic with the directions of scientific research of scientists on this topic is demonstrated, the main scientific results of the work, their practical use, the list of enterprises and institutions in which the results of the work are implemented are presented.

In the first chapter, an analysis of the subject area of research, existing deception systems, decoys and traps, methods used to detect computer attacks and malicious software is carried out. The types of population algorithms and their features are analyzed.

In the second chapter, models of dual-target attacks on corporate targets are developed and an improved architecture of deception systems with baits and traps is proposed, in which, in contrast to known architecture options, a synthesis of population algorithms, in particular the moth and fire algorithm, is carried out to optimize the formation of the sequence of the next steps in the implementation of KA and malicious software actions, avoiding a complete search of options, rapid convergence of the selected steps with ongoing influences and changing the sequence of steps taking into account current changes in the environment of corporate networks, as well as taking into account the potential ability of attackers to carry out dual-purpose KA.

The third chapter presents the developed method of synthesis of the discrete moth and flame algorithm, which is distinguished by the formation of a discrete search space, coordinate representation of objects, the use of sectorial evaluation of potential steps, the construction of a spiral trace and taking into account time as a parameter of step change. The proposed dynamic movement of moths and flames avoids premature convergence to local optima and ensures long-term adaptive functioning of deception systems due to the rational selection of sequences of steps during event processing. Also, a developed method of organizing the functioning of deception systems in corporate networks is presented, within which population algorithms provide autonomous selection of further actions of



deception components, taking into account changes in the network environment. This makes it possible to complicate the activities of attackers, prevent the implementation of dual-target attacks, form solutions without exhaustively sorting out options, and automatically activate or block servers or stations depending on the nature of the detected impacts.

The fourth chapter presents the developed method of detecting denial of service attacks, which is based on the analysis of statistical characteristics of network traffic, which is formed when the packet flow is divided into time windows. The method provides tracking of the dynamics of traffic changes at the level of the entire investigated period and increases the reliability and efficiency of detection of Denial of Service attacks. Also, the developed software parts of cheating systems, the peculiarities of their implementation and the libraries used for their implementation, which ensure the functionality of the implemented system, are described. The conducted experiments, evaluation of the effectiveness of the cheating system, and analysis of the obtained results are presented.

The scientific and practical results of the conducted research are presented in the conclusions.

The appendices present scientific publications that reflect the scientific results of the work, acts of implementation of the results of the work, and a listing of the developed software.

Keywords: computer systems; corporate networks; computer stations; deception systems; population algorithms; moth and flame algorithm; trap; lure; malicious software; computer attacks; intrusion detection systems; systems architecture.

## СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

*Наукові праці, в яких опубліковані основні наукові результати дисертації*

1. Савенко О.С., Дрозд А.І., Медзатий Д.М. Концептуальна архітектура обманних систем з приманками і пастками на основі популяційних алгоритмів. *Вимірювальна та обчислювальна техніка в технологічних процесах. Measuring and computing devices in technological processes*. 2025. №84(4). С. 127-151. DOI: <https://doi.org/10.31891/2219-9365-2025-84-15>

2. Дрозд А. Метод виявлення комп'ютерних атак типу відмови в обслуговуванні на основі статистичних показників мережного трафіку. *Information Technology:*



*Computer Science, Software Engineering and Cyber Security*. 2025. № 4, С. 79–89. DOI: <https://doi.org/10.32782/IT/2025-4-10>

3. Савенко О.С., Дрозд А.І., Коробчинський М.В. Метод синтезу популяційних алгоритмів в архітектурі обманних систем з приманками і пастками. *Вимірювальна та обчислювальна техніка в технологічних процесах. Measuring and computing devices in technological processes*. 2025. №82(2). С. 459–474. DOI: <https://doi.org/10.31891/2219-9365-2025-82-64>

4. RAMSKYI I., DROZD A., LYHUN O., PONOCHOVNA O. SYSTEM FOR CYBERSECURITY EVALUATION OF CORPORATE NETWORKS. *Computer Systems and Information Technologies*. 2025. № 2. С. 123–131. DOI: <https://doi.org/10.31891/csit-2025-2-14>

5. Дрозд А.І. Метод організації функціонування обманних систем з приманками і пастками в корпоративних мережах. *Вісник Хмельницького національного університету. Технічні науки*. 2025. № 359 (6.2). С. 445–457. DOI: <https://doi.org/10.31891/2307-5732-2025-359-135>

6. Savenko O., Rusyn B., Lysenko S., Ciszewski T., Savenko B., Drozd A., Nicheporuk A., Sachenko A. Synthesis of a Moth and Flame Algorithm for Incorporation into the Architecture of Deceptive Systems with Baits and Traps. *Applied Sciences*. 2026. 16(5). 2415. DOI: <https://doi.org/10.3390/app16052415>

*Праці, які засвідчують апробацію матеріалів дисертації*

7. Rehida, P., Savenko, O., Sachenko, A., Drozd, A., Vizhevski, P. A trust model that ensures the correctness of computing in grid computing system. (2024) *CEUR Workshop Proceedings*, 3675, pp. 388-401. *The 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2024)*: CEUR-Workshop Proceedings. Vol. 3675. (Khmelnyskyi, March 2024). Khmelnyskyi, 2024. Pp. 388-401. URL: <https://ceur-ws.org/Vol-3675/paper28.pdf> (Scopus)

8. Denysiuk D., Sochor T., Kapustian M., Kashtalian A., Drozd A. A method for detecting botnets in IT infrastructure using a neural network. (2024) *CEUR Workshop Proceedings*, 3736, pp. 282-292. *The 1th Proceedings of the 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhys 2024)*. Khmelnyskyi, Ukraine, June 28,



2024 : CEUR-Workshop Proceedings. Vol. 3736. (Khmelnyskyi, Ukraine, June 28, 2024). Khmelnyskyi, 2024. Pp. 282-292. URL: <https://ceur-ws.org/Vol-3736/paper21.pdf> (Scopus)

9. Sierhieiev Y., Savenko O., Paiuk V., Drozd A. Effectiveness and improvement of Static Application Security Testing (SAST) in the context of SQL Injection vulnerabilities // *Proceedings of 2024 IEEE 14th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024, Athens, Greece, October 11-13, 2024)* DOI: [10.1109/DESSERT65323.2024.11122171](https://doi.org/10.1109/DESSERT65323.2024.11122171) (Scopus)

10. Semeniuk B., Kashtalian A., Martiniuk D., Drozd A., Abdel-Badeeh M. Salem. Detection of computer attacks based on sonification of network traffic. *Intelitsis '25: The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security*, April 04, 2025, Khmelnyskyi, Ukraine. URL: <https://ceur-ws.org/Vol-3963/paper21.pdf> (Scopus)

11. Kozelskyi O., Drozd A., Savenko B., Gaj P. A model for probabilistic monitoring and proactive restart of real-time operating systems under intensive state changes in cyber-physical systems. *Proceedings of the 2nd International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS 2025)* Khmelnyskyi, Ukraine on July 4, 2025. Pp. 198-210. URL: <https://ceur-ws.org/Vol-4013/paper16.pdf> (Scopus)

*Публікації, які додатково відображають наукові результати дисертації*

12. Свідоцтво про реєстрацію авторського права на твір № 142624 Україна. Комп'ютерна програма «Програмне забезпечення функціонування обманних систем в корпоративних мережах з прийняттям рішень на основі популяційних алгоритмів» / Дрозд А. І., Савенко О. С., Нічепорук А. О., Регіда П. Г. 13.02.2026.