

АНОТАЦІЯ

Бохонько О.О. Методи та засоби синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія. – Хмельницький національний університет, Хмельницький, 2026.

Дослідження відомих методів та засобів виявило системний недолік – наявні рішення демонструють низьку ефективність синтезу систем, стійкої до атак соціальної інженерії, оскільки не включають комплексно в процес такого синтезу стійкої до атак архітектури, достовірність забезпечення виявлення атак, адаптивність, масштабованість, живучість та ефективність прийняття колективних рішень.

Таким чином, на даний момент часу існує суперечність між потребою в синтезі комп'ютерних системи, стійких до атак соціальної інженерії, з одного боку, і недосконалістю методів та засобів забезпечення стійкості РКС в умовах атак соціальної інженерії, з іншого боку. Відтак, підвищення стійкості розподілених комп'ютерних систем до атак соціальної інженерії є актуальною науково-прикладною задачею, одним із шляхів розв'язання якої є розроблення методів і засобів синтезу розподілених комп'ютерних систем, стійких до атак соціальної інженерії.

Зазначена науково-прикладна задача відповідає предметній області Стандарту вищої освіти України зі спеціальності 123 – Комп'ютерна інженерія для третього (освітньо-наукового) рівня вищої освіти, зокрема, такому об'єкту вивчення та діяльності, як «комп'ютерні системи,..., комп'ютерні мережі, методи та способи подання, отримання, зберігання, передавання, опрацювання та захисту в них інформації,..., архітектура та організація їх функціонування; інформаційні процеси, технології, методи, способи, інструментальні засоби та системи для дослідження, проектування, налагодження, виробництва й експлуатації комп'ютерів та комп'ютерних систем і мереж, ..., забезпечення якості, надійності та безпеки».

Об'єктом дослідження є процес процес синтезу стійких до атак соціальної інженерії розподілених комп'ютерних систем.

Предметом дослідження моделі, методи та засоби синтезу стійких до атак соціальної інженерії розподілених комп'ютерних систем.

Метою дослідження є підвищення стійкості до атак соціальної інженерії розподілених комп'ютерних систем шляхом розроблення методів та засобів синтезу стійких до атак соціальної інженерії РКС, які комплексно забезпечують достовірність виявлення атак, адаптивність, масштабованості, живучість та ефективність прийняття колективних рішень вузлів РКС.

Для досягнення поставленої мети були розв'язані такі задачі:

- проведено аналіз відомих методів і засобів забезпечення стійкості розподілених комп'ютерних систем до атак соціальної інженерії;
- розроблено формальну модель розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії, яка описує колективну поведінку агентів у динамічному середовищі шляхом узгодженого прийняття рішень, обміну інформацією та адаптивного керування ресурсами з метою максимізації глобальної функції корисності, що відображає стійкість системи до атак соціальної інженерії, забезпечення достовірного виявлення загроз, підтримання безперервності функціонування, збереження живучості за умов часткової компрометації вузлів і масштабування системи;
- розроблено архітектуру стійкої до атак соціальної інженерії розподіленої комп'ютерної системи, яка базується на ієрархічній багатоагентній основі з застосуванням підкріплювальним навчанням, що дає змогу адаптивно зменшувати невизначеність у процесі виявлення атак та підвищувати точність виявлення та класифікації атак соціальної інженерії;
- розроблено метод виявлення кібератак соціальної інженерії в розподілених комп'ютерних системах на основі унікального лінгвістичного ідентифікатора формулювання, який ґрунтується на формуванні спеціалізованої множини унікальних мовних ідентифікаторів, застосуванні методу k-найближчих сусідів, що уможливорює раннє виявлення мовних та семантичних маніпуляцій у сценаріях атак на розподіленої комп'ютерної системи;

- розроблено метод забезпечення масштабованості архітектури РКС, стійкої до атак соціальної інженерії на основі популяційної моделі багатоагентної системи та середнього поля, що забезпечує формування оптимальної політики поведінки репрезентативного агента, інтеграцію архітектурних параметрів та гарантовану масштабованість системи при зростанні кількості вузлів і інтенсивності атак;

- розроблено метод комплексного оцінювання стійкості РКС до атак соціальної інженерії, базований на багатовимірній системі критеріїв адаптивності, масштабованості, живучості та достовірності виявлення деструктивних впливів, із формуванням узагальненої метрики ефективності на основі нормованих вагових коефіцієнтів;

- розроблено архітектуру програмної реалізації розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії, яка включає агента прийняття рішень, сервісних агентів, компоненти моніторингу станів, менеджер взаємодії та модулі мовного/семантичного аналізу; проведено експериментальні дослідження її характеристик у сценаріях впливів атак соціальної інженерії та оцінено покращення показників стійкості системи.

У дисертаційній роботі вперше розроблено метод забезпечення масштабованості архітектури РКС, стійкої до атак соціальної інженерії, який на відміну від відомих підходів поєднує принципи динамічної декомпозиції, багатоагентної взаємодії та адаптивного перерозподілу ресурсів з урахуванням поведінкових характеристик користувачів і загроз, що дає змогу забезпечити керовану масштабованість розподіленої системи без зниження рівня захищеності, підвищити її живучість за умов зростання кількості вузлів розподіленої КС та інтенсивності атак соціальної інженерії.

У дисертаційній роботі вперше розроблено метод комплексного оцінювання стійкості РКС до атак соціальної інженерії, який на відміну від відомих методів ґрунтується на багатовимірній системі формалізованих критеріїв адаптивності, масштабованості, живучості та достовірності виявлення, що дозволило отримати єдину універсальну метрику оцінювання стійкості РКС до атак соціальної інженерії.

У дисертаційній роботі набула подальшого розвитку архітектура стійкої до

атак соціальної інженерії розподіленої комп'ютерної системи, яка на відміну від відомих базується на ієрархічній багатоагентній основі з застосуванням підкріплювальним навчанням, ентропійно-орієнтованими функціями винагороди, апіорними знаннями у вигляді графа знань та модально-специфічними сервісними агентами, що дає змогу адаптивно зменшувати невизначеність у процесі виявлення атак, скорочувати кількість діалогових кроків і підвищувати точність виявлення та класифікації атак соціальної інженерії.

У дисертаційній роботі також удосконалено метод виявлення кібератак соціальної інженерії в розподілених комп'ютерних системах на основі унікального лінгвістичного ідентифікатора формулювання, який на відміну від відомих підходів ґрунтується на формуванні спеціалізованої множини унікальних мовних ідентифікаторів, їх попередній лінгвістичній нормалізації, експертному маркуванні та застосуванні методу k-найближчих сусідів із подальшим адаптивним налаштуванням гіперпараметрів і порогових значень довіри, що дає змогу підвищити точність та стійкість виявлення атак соціальної інженерії, зменшити кількість хибних спрацьовувань, забезпечити раннє реагування та інтеграцію результатів у контури захисту розподіленої комп'ютерної системи.

Практична цінність отриманих результатів полягає в реалізації усіх теоретичних положень, поданих в дисертаційному дослідженні, у прикладні рішення та можливості їх безпосереднього впровадження й використання на підприємствах.

За результатами виконаних досліджень здобувачем реалізовано розподілену комп'ютерну систему, стійку до атак соціальної інженерії. Практична цінність роботи полягає у можливості використання отриманих результатів для розроблення корпоративних політик безпеки, побудови симуляційних тренажерів для дослідження взаємодії користувачів із атаками соціальної інженерії, створення інтелектуальних агентів для кіберзахисту та оптимізації архітектур розподілених систем з урахуванням ризиків. Запропоновані методи можуть застосовуватися у банківській,

телекомунікаційній, енергетичній та державній сферах, де критично важливо забезпечити стійкість систем до складних поведінкових загроз.

Результати дисертаційної роботи впроваджено у (Додаток Б): ПП «АВІВІ» (акт впровадження від 08.1.2025 р.); ТОВ «ДЖІ ЕМ ХОСТ» (акт впровадження від 30.12.2025 р.); у навчальному процесі Хмельницького національного університету (акт впровадження від 30.09.2025 р.); при виконанні держбюджетної теми Хмельницького національного університету «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (ДР № 0124U000980).

Основні результати дисертації опубліковані у 9 наукових працях, серед яких 5 статей у фахових наукових журналах України, включених на дату опублікування до переліку наукових фахових видань України категорії Б; 4 публікації, які засвідчують апробацію матеріалів дисертації (статті в матеріалах конференцій, що індексуються в наукометричній базі Scopus).

Ключові слова: розподілені комп'ютерні системи, соціальна інженерія, багатоагентна система, синтез архітектури, середнє поле; навчання з підкріпленням, агент, унікальний лінгвістичний ідентифікатор формулювання, виявлення атак, адаптивність, масштабованість, живучість та ефективність прийняття колективних рішень.

ANNOTATION

Bohonko O.O. Methods and Means of Synthesis of Distributed Computer Systems Resistant to Social Engineering Attacks. – Qualification Scientific Work as a Manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 123 – Computer Engineering. – Khmelnytskyi National University, Khmelnytskyi, 2026.

The study of known methods and tools revealed a systemic drawback – the available solutions demonstrate the low efficiency of synthesis of systems resistant to social engineering attacks, since they do not comprehensively include in the process of such synthesis of attack-resistant architecture, the reliability of providing attack

detection, adaptability, scalability, survivability and efficiency of collective decision-making.

Thus, at this point in time, there is a contradiction between the need for the synthesis of computer systems resistant to social engineering attacks, on the one hand, and the imperfection of methods and means of ensuring the stability of the RCS in the face of social engineering attacks, on the other hand. Therefore, increasing the resilience of distributed computer systems to social engineering attacks is an urgent scientific and applied task, one of the ways to solve which is the development of methods and means of synthesis of distributed computer systems resistant to social engineering attacks.

This scientific and applied task corresponds to the subject area of the Standard of Higher Education of Ukraine in the specialty 123 – Computer Engineering for the third (educational and scientific) level of higher education, in particular, such an object of study and activity as "computer systems,..., computer networks, methods and methods of representing, receiving, storing, transmitting, processing and protecting information in them,..., architecture and organization of their functioning; information processes, technologies, methods, methods, tools and systems for research, design, adjustment, production and operation of computers and computer systems and networks, ..., ensuring quality, reliability and safety".

The object of the study is the process of synthesis of distributed computer systems resistant to social engineering attacks.

The subject of the study is models, methods and means of synthesis of distributed computer systems resistant to social engineering attacks.

The purpose of the study is to increase the resistance to social engineering attacks of distributed computer systems by developing methods and means of synthesis of social engineering RKS resistant to social engineering attacks, which comprehensively ensure the reliability of attack detection, adaptability, scalability, survivability and efficiency of collective decision-making of RKS nodes.

To achieve this goal, the following tasks were solved:

- an analysis of known methods and means of ensuring the resilience of distributed computer systems to social engineering attacks has been carried out;

- a formal model of a distributed computer system resistant to social engineering attacks has been developed, which describes the collective behavior of agents in a dynamic environment through coherent decision-making, information exchange and adaptive resource management in order to maximize the global utility function, reflecting the resilience of the system to social engineering attacks, ensuring reliable threat detection, maintaining continuity of functioning, maintaining survivability under conditions of partial compromise of nodes and scaling of the system;

- an architecture of a distributed computer system based on a hierarchical multi-agent basis with the use of reinforcement learning has been developed, which makes it possible to adaptively reduce uncertainty in the process of detecting attacks and increase the accuracy of detection and classification of social engineering attacks;

- a method for detecting social engineering cyberattacks in distributed computer systems based on a unique linguistic formulation identifier has been developed, which is based on the formation of a specialized set of unique language identifiers, the use of the k-nearest neighbor method, which allows early detection of linguistic and semantic manipulations in scenarios of attacks on a distributed computer system;

- a method has been developed to ensure the scalability of the RCS architecture, resistant to social engineering attacks based on the population model of a multi-agent system and the middle field, which ensures the formation of an optimal policy of behavior of a representative agent, the integration of architectural parameters and guaranteed scalability of the system with an increase in the number of nodes and the intensity of attacks;

- a method of comprehensive assessment of the resistance of the RCS to social engineering attacks was developed, based on a multidimensional system of criteria for adaptability, scalability, survivability and reliability of detecting destructive influences, with the formation of a generalized performance metric based on normalized weight factors;

- the architecture of the software implementation of a distributed computer system resistant to social engineering attacks was developed, which includes a decision-making agent, service agents, state monitoring components, an interaction manager and language/semantic analysis modules; experimental studies of its

characteristics in scenarios of the impact of social engineering attacks have been carried out and the improvement of the system's resilience indicators has been evaluated.

In the dissertation, for the first time, a method was developed to ensure the scalability of the RCS architecture, resistant to social engineering attacks, which, in contrast to well-known approaches, combines the principles of dynamic decomposition, multi-agent interaction and adaptive redistribution of resources, taking into account the behavioral characteristics of users and threats, which makes it possible to ensure controlled scalability of the distributed system without reducing the level of security, to increase its survivability under the conditions of growth in the number of nodes of distributed CS and the intensity of social engineering attacks.

In the dissertation, for the first time, a method of comprehensive assessment of the resistance of the RCS to social engineering attacks was developed, which, unlike the known methods, is based on a multidimensional system of formalized criteria for adaptability, scalability, survivability and reliability of detection, which made it possible to obtain a single universal metric for assessing the resistance of the RCS to social engineering attacks.

In the dissertation, the architecture of an attack-resistant social engineering distributed computer system was further developed, which, unlike the well-known ones, is based on a hierarchical multi-agent basis with the use of reinforcement learning, entropy-oriented reward functions, a priori knowledge in the form of a knowledge graph and modal-specific service agents, which makes it possible to adaptively reduce uncertainty in the process of detecting attacks, reduce the number of dialog steps and improve the accuracy of detecting and classifying social engineering attacks.

The dissertation also improves the method for detecting social engineering cyberattacks in distributed computer systems based on a unique linguistic formulation identifier, which, unlike known approaches, is based on the formation of a specialized set of unique language identifiers, their preliminary linguistic normalization, expert labeling and the application of the k-nearest neighbor method, followed by adaptive adjustment of hyperparameters and trust thresholds, which makes it possible to increase the accuracy and resilience of detecting social engineering attacks, reduce the number

of false positives, ensure early response and integration of results into the protection loops of a distributed computer system.

The practical value of the results obtained lies in the implementation of all theoretical provisions presented in the dissertation research into applied solutions and the possibilities of their direct implementation and use at enterprises.

According to the results of the research, the applicant implemented a distributed computer system resistant to social engineering attacks. The practical value of the work lies in the possibility of using the results obtained to develop corporate security policies, build simulation simulators to study user interaction with social engineering attacks, create intelligent agents for cyber defense, and optimize distributed system architectures taking into account risks. The proposed methods can be applied in the banking, telecommunications, energy and public spheres, where it is critically important to ensure the resilience of systems to complex behavioral threats.

The results of the dissertation work were implemented in (Annex B): PE "AVIVI" (act of implementation dated 08.01.2025); LLC "GM HOST" (act of implementation dated 30.12.2025); in the educational process of Khmelnytskyi National University (act of implementation dated 30.09.2025); in the implementation of the state budget theme of Khmelnytskyi National University "System for detecting RFPs and computer attacks in corporate networks using false attack objects and traps" (DR No. 0124U000980).

The main results of the dissertation were published in 9 scientific papers, including 5 articles in professional scientific journals of Ukraine, included as of the date of publication in the list of scientific professional publications of Ukraine of category B; 4 publications certifying the approbation of the dissertation materials (articles in conference proceedings indexed in the scientometric database Scopus).

Keywords: distributed computer systems, social engineering, multi-agent system, synthesis of architecture, middle field; reinforcement learning, agent, unique linguistic formulation identifier, attack detection, adaptability, scalability, survivability and efficiency of collective decision-making.

Список публікацій здобувача за темою дисертації

Статті у наукових виданнях, включених до Переліку наукових фахових видань України:

1. Лисенко С., Атаманюк О., Бохонько О., Воробйов В. Дослідження методів виявлення кіберзагроз типу RANSOMWARE на основі застосування HONEYROT. *Вісник ХНУ*. 2023. №1, (317). С. 300-309. <https://doi.org/10.31891/2307-5732-2023-317-1-300-309>
2. Лисенко С., Бохонько О. Методи виявлення кібератак соціальної інженерії. *Вісник ХНУ*. 2023. №327(5(2)). С. 231-236. <https://doi.org/10.31891/2307-5732-2023-327-5-231-236>.
3. Бохонько О., Лисенко С. Моделі атак соціальної інженерії. *Measuring and computing devices in technological processes*. 2025. № (1), С. 432–444. <https://doi.org/10.31891/2219-9365-2025-81-55> .
4. Бохонько О. Лисенко С. Метод синтезу розподіленої комп'ютерної системи, стійкої до атак соціальної інженерії. *Measuring and computing devices in technological processes*, vol. 84(4), pp. 152–163. <https://doi.org/10.31891/2219-9365-2025-84-16> .
5. Bokhonko O., Atamaniuk O. Method for synthesis of a scalable architecture of a distributed computer systems, resistant to social engineering attacks. *Computer Systems and Information Technologies*. 2025. Vol.4. pp. 60-76. <https://doi.org/10.31891/csit-2025-4-7>

Праці, які засвідчують апробацію матеріалів дисертації

6. Lysenko S., Bokhonko O., Savenko O., Vorobiov V., Gaj P., Wołoszyn J. Social Engineering Attacks Detection Approach. *Proceedings of 2023 IEEE 13th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2023, Athens, Greece, October 13-15, 2023)*. Pp. 318-329.
7. Lysenko S., Bokhonko O., Vorobiyov V., Gaj P. A Method for identifying cyberattacks based on the use of social engineering over the phone. *CEUR-WS*. 2024. Vol. 3675. Pp. 318-329. URL: <https://ceur-ws.org/Vol-3675/paper23.pdf> .
8. Lysenko S., Bokhonko O., Savenko O., Gaj P., Social Engineering Attacks Models. *Proceedings of 2024 IEEE 14th International Conference on*

Dependable Systems, Services and Technologies (DeSSerT-2024, Athens, Greece, October 11-13, 2024).

9. Bokhonko O., Atamaniuk O., Sochor T. Model of a distributed heterogeneous system resistant to leakage of confidential information *CEUR-WS*. 2025. Vol. 3963. Pp. 363-376. URL: <https://ceur-ws.org/Vol-3963/paper29.pdf> .