ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

на тему «Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів»
здобувача наукового ступеня доктора філософії Дрозда Андрія Ігоровича
з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

Публічна презентація проведена на кафедрі комп'ютерної інженерії та інформаційних систем
(назва)
«_4_»_березня_ 2026 р., протокол №_18_.

1. Обґрунтування вибору теми дослідження. Комп'ютерні атаки (КА) на корпоративні мережі здійснюються постійно та безперервно вдосконалюються. Хоча для їх протидії застосовуються сучасні засоби безпеки, зловмисники добре обізнані з комерційними рішеннями, можуть їх аналізувати та з часом знаходити способи обходу. У результаті ефективність захисту знижується, що потребує постійного оновлення та вдосконалення систем безпеки, зокрема шляхом забезпечення їх непередбачуваної поведінки для зловмисників. Водночас така недетермінованість не повинна зменшувати ефективність виявлення КА та зловмисного програмного забезпечення (ЗПЗ).

Окремим напрямом захисту є обманні системи, приманки та пастки (ОСПП). Оскільки вони також є доступними для аналізу, виникає потреба в удосконаленні їх архітектури та функціонування, а також у поєднанні в цілісні ОСПП. Актуальним завданням є забезпечення їх недетермінованої роботи та ефективного керування приманками і пастками в корпоративних мережах.

Перспективним підходом до розв'язання цієї задачі є використання популяційних алгоритмів у підсистемах прийняття рішень. Вони дають змогу оптимізувати вибір наступних кроків системи, уникати локальних оптимумів і забезпечувати довготривалу протидію атакам. Особливо доцільними є алгоритми, натхненні живою природою, поведінка яких є складною для прогнозування. Одним із таких є алгоритм молі і полум'я, що забезпечує пошук глобального оптимуму. Проте більшість його реалізацій орієнтовані на неперервний простір, тоді як у задачах вибору кроків і приманок простір є дискретним, що потребує відповідної адаптації алгоритму.

Таким чином, постає необхідність удосконалення або створення нової архітектури обманних систем, здатної адекватно реагувати на події в мережі та

водночас залишатися складною для аналізу зловмисниками. Відсутність ефективних алгоритмів, які поєднували б оптимальність і недетермінованість, зумовлює актуальність дослідження. Отже, важливою науковою задачею є покращення протидії КА та ЗПЗ у корпоративних мережах шляхом оптимізації кроків ОСПП на основі синтезу популяційних алгоритмів у центрах прийняття рішень.

2. Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконувалось у рамках науково-дослідної тематики Хмельницького національного університету: держбюджетної науково-дослідної теми №2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (номер держреєстрації 0124U000980); держбюджетної науково-дослідної теми №1Б-2026 «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (номер держреєстрації 0126U002082), в яких автор дисертації був виконавцем.

3. Наукова новизна отриманих результатів. Наукова новизна отриманих результатів полягає у розробленні методів синтезу обманних систем для виявлення КА з використанням популяційних алгоритмів, а також розроблено відповідні засоби і проведено з ними експериментальні дослідження.

Отримано такі наукові результати:

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.

4. Теоретичне та практичне значення результатів дисертації. 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 оманних систем для прийняття ними рішень дав змогу формувати послідовності кроків систем так, щоб заплувати 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 натхненних живою природою.

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

5. Використання результатів роботи. 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 удосконалені навчально-лабораторного комплексу.

6. Особиста участь автора в одержанні наукових та практичних результатів, що викладені в дисертаційній роботі.

Повнота викладення матеріалів дисертації в роботах, опублікованих автором. За результатами проведених досліджень основні наукові результати опубліковано у шести наукових статтях в чотирьох фахових наукових журналах України та одному міжнародному науковому журналі, що індексується в наукометричній базі Scopus. Апробація засвідчена публікаціями п'яти праць в матеріалах міжнародних конференцій, які проіндексовано у наукометричній базі Scopus. Опубліковано одне свідоцтво про реєстрацію авторського права на твір (програму).

У роботах, опублікованих одноосібно автором, отримано наступні результати: розроблено метод виявлення комп'ютерних атак типу відмови в обслуговуванні на основі статистичних показників мережного трафіку; розроблено метод організації функціонування ОСПП в корпоративних мережах.

У роботах, які опубліковані у співавторстві, автору належать основні ідеї, теоретична та практична розробка положень, відображених у характеристиці наукової новизни отриманих результатів, а саме: розроблено архітектуру обманних систем з приманками на основі використання популяційних алгоритмів в підсистемі прийняття рішень для вибору наступних кроків систем із множини наявних кроків; розроблено метод синтезу популяційних алгоритмів в архітектурі ОСПП, зокрема алгоритм дискретної оптимізації молі і полум'я; визначено стратегію та основні кроки методу для здійснення оцінювання рівнів кібербезпеки у вузлах корпоративних мереж; проведено аналіз готових засобів для розгортання бінарного класифікатора; визначено стратегію застосування штучних нейромереж

в кроки методу виявлення бот-мереж в корпоративну ІТ-інфраструктуру; визначено стратегію тестування безпеки застосунків в корпоративних мережах; визначено статистичні показники комп'ютерних атак на основі мережного трафіку; визначено показники операційних систем реального часу, які впливають на зміну стану операційного середовища систем; розроблено архітектуру програмного забезпечення та програмний код обманних систем в корпоративних мережах з прийняттям рішень на основі популяційних алгоритмів.

Результати дисертації опубліковано в повному обсязі.

Дисертаційна робота виконана _на кафедрі комп'ютерної інженерії та інформаційних систем,_____

(*назва кафедри (відділу), назва установи)*

Наукові керівники:

доктор технічних наук, професор, професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Савенко Олег Станіславович;

доктор технічних наук, професор начальник другої кафедри Другого навчально-наукового інституту Воєнної академії імені Євгенія Березняка Коробчинський Максим Володимирович.

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Дрозда А.І._____

(прізвище, ініціали здобувача)

є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають посилання на відповідне джерело.

Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення.

Дотримання академічної доброчесності. Роботу Дрозда А.І. перевірено на плагіат програмним засобом «StrikePlagiarism». Результати схожості тексту: укр. мовою – 8,34 %; англ. мовою – 9.99%. Зазначені результати схожості тексту є допустими. Аналіз тексту дисертації, який було перевірено, показав повтори за ключовими термінами, переліком джерел та стандартним ключовим словам, які використано для оформлення дисертації.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковано _12_ наукових праць, у тому числі _0_монографій, _6_статей у наукових фахових виданнях (з них _6_ статей у

періодичних наукових виданнях інших держав, які входять до ОЕСР та/або Європейського Союзу, фахових виданнях України категорії «А», або закордонних виданнях, що входять до WoS або Scopus) _0_ патентів України, _5_публікацій в збірниках матеріалів конференцій.

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 *– розроблено архітектуру обманних систем з приманками на основі використання популяційних алгоритмів в підсистемі прийняття рішень для вибору наступних кроків систем із множини наявних кроків*

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- *- розроблено метод синтезу популяційних алгоритмів в архітектурі ОСПП, зокрема алгоритм дискретної оптимізації молі і полум'я*

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 *– визначено стратегію та основні кроки методу для здійснення оцінювання рівнів кібербезпеки у вузлах корпоративних мереж*

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 - *розроблено метод синтезу популяційних алгоритмів в архітектурі ОСПП, зокрема алгоритм дискретної оптимізації молі і полум'я*

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. (Khmelnytskyi, March 2024). Khmelnytskyi, 2024. Pp. 388-401. URL: https://ceur-ws.org/Vol-3675/paper28.pdf *(Scopus)* – *проведено аналіз готових засобів для розгортання бінарного класифікатора*

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)*. Khmelnytskyi, Ukraine, June 28, 2024 : CEUR-Workshop Proceedings. Vol. 3736. (Khmelnytskyi, Ukraine, June 28, 2024). Khmelnytskyi, 2024. Pp. 282-292. URL: https://ceur-ws.org/Vol-3736/paper21.pdf *(Scopus)* – *визначено стратегію застосування штучних нейромереж в кроки методу виявлення бот-мереж в корпоративну IT-інфраструктуру*

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 *(Scopus)* – *визначено стратегію тестування безпеки застосунків в корпоративних мережах*

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, Khmelnytskyi, Ukraine. URL: https://ceur-ws.org/Vol-3963/paper21.pdf *(Scopus)* – *визначено статистичні показники комп'ютерних атак на основі мережного трафіку*

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)* Khmelnytskyi, Ukraine on July 4, 2025. Pp. 198-210. URL: https://ceur-ws.org/Vol-4013/paper16.pdf *(Scopus)* –

визначено показники операційних систем реального часу, які впливають на зміну стану операційного середовища систем

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. 13.02.2025. – *розроблено архітектуру програмного забезпечення та програмний код обманних систем в корпоративних мережах з прийняттям рішень на основі популяційних алгоритмів* .

Апробація дисертації. Апробацію основних положень, ідей, висновків дисертаційної роботи проведено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем у Хмельницькому національному університеті. Наукові результати роботи доповідались на таких конференціях: 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, March 28, 2024); 6th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, April 04, 2025,); 14th International Conference on Dependable Systems, Services and Technologies (IEEE, DeSSerT, Athens, Greece, October 11-13, 2024); 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS, Khmelnytskyi, Ukraine, June 28, 2024); 2nd International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS, Khmelnytskyi, Ukraine, July 4, 2025).

8. Оцінка мови, стилю та оформлення дисертації. Дисертацію написано грамотною українською мовою. Стиль викладення матеріалів досліджень, наукових положень, висновків та рекомендацій забезпечує легкість і доступність їх сприйняття. Дисертацію оформлено згідно вимог, передбачених Наказом МОН України від 12.01.2017 р. № 40 (із змінами, внесеними згідно з Наказом Міністерства освіти і науки України № 759 від 31.05.2019) «Про затвердження Вимог до оформлення дисертації».

ВВАЖАТИ, що дисертаційна робота ____ *Дрозда А.І.*_____
(прізвище, ініціали здобувача)
«Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів»,_____
(назва)
яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам пп. 6, 7, 8, 9 Постанови Кабінету Міністрів України від 12 січня 2022 р. № 44 «ПОРЯДОК присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» *(із змінами, внесеними згідно з Постановами КМ* № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024*)*, та відповідає напрямку наукового дослідження освітньо-наукової програми Хмельницького національного університету зі спеціальності *123 Комп'ютерна інженерія*._____
(шифр, назва)

РЕКОМЕНДУВАТИ:

Дисертаційну роботу «*Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів*»,
назва роботи
подану _____*Дроздом Андрієм Ігоровичем*_____
прізвище, ім'я, по батькові
на здобуття ступеня доктора філософії, до захисту.

Головуюча публічної презентації,
завідувачка кафедри КІІС,
___*доктор філософії,*
(науковий ступінь,
_____*доцент*___ _____ *Ольга ПАВЛОВА*
вчене звання, посада) *підпис* *Ім'я ПРІЗВИЩЕ*

Підпис дійсний
Засвідчую
Начальник відділу кадрів
І.С. Малиновська
ВІДДІЛ КАДРІВ