ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації «модель та методи інтелектуальної системи виявлення аномалій в хмарних сервісах» здобувача ступеня доктора філософії Свиридова Артема Сергійовича за спеціальністю 125 Кібербезпека галузі знань 12 Інформаційні технології

Публічна презентація проведена на розширеному засіданні кафедри безпеки інформаційних технологій «30» червня 2026 р., протокол № 13.

1. Актуальність теми дисертації.

Зі стрімким розвитком хмарних технологій та масовим переходом до мікросервісної архітектури суттєво збільшується складність забезпечення кібербезпеки сучасних обчислювальних середовищ. З впровадженням платформ оркестрації контейнерів, зокрема Kubernetes, та постійною еволюцією кіберзагроз (включаючи атаки на API й загрози типу Zero-day) динамічно зростають сукупні вимоги до систем моніторингу та захисту. Наявність засобів обробки великих обсягів телеметрії та журналів подій у режимі реального часу є вже необхідністю в сучасних реаліях. Особливо дана проблематика є критичною в умовах обмеженої ефективності традиційних сигнатурних і правил-орієнтованих засобів захисту, оскільки в динамічних хмарних середовищах збільшується вірогідність пропуску нових типів атак. Одним із перспективних підходів до вирішення цієї проблеми є розроблення інтелектуальних систем виявлення аномалій на основі моделей глибокого навчання. Саме тому обрана тема є актуальною як для теоретичного дослідження моделей глибокого навчання при виявленні аномалій, так і для практичного застосування в сучасних хмарних сервісах.

2. Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри.

Науковий напрямок кафедри безпеки інформаційних технологій – дослідження та розробка математичних основ та

концептуальних положень процесного підходу до захисту інформації. Тема дисертаційної роботи відповідає науковому напрямку кафедри.

3. Мета і завдання дослідження.

Мета дослідження – підвищення ефективності виявлення аномалій у хмарних сервісах шляхом розробки моделі і методів інтелектуальної інформаційної системи, що забезпечують інтеграцію різнорідних даних, автоматизований аналіз подій та адаптивне виявлення кіберзагроз у контейнеризованих і розподілених середовищах.

Для досягнення зазначеної мети поставлені основні завдання дослідження:

- проаналізувати сучасний стан проблеми виявлення аномалій у хмарних сервісах та існуючі підходи до забезпечення безпеки контейнеризованих і розподілених середовищ з урахуванням обмежень традиційних методів моніторингу та аналізу кіберзагроз;
- удосконалити метод виявлення аномалій у API-журналах і поведінці користувачів шляхом інтеграції поведінкових, мережевих та часових характеристик із використанням алгоритмів машинного навчання;
- удосконалити метод виявлення аномалій у Kubernetes-кластерах на основі аналізу телеметрії контейнеризованого середовища та застосування моделей глибокого навчання, зокрема LSTM Autoencoder;
- розробити математичну модель інтелектуальної системи виявлення аномалій, що забезпечує інтеграцію API-журналів, мережевих подій, телеметрії Kubernetes-кластерів і поведінкових даних у межах єдиного аналітичного процесу;
- реалізувати програмну архітектуру інтелектуальної системи та здійснити її експериментальну верифікацію у хмарному контейнеризованому середовищі з використанням сучасних метрик оцінювання ефективності виявлення аномалій.

4. Особистий внесок здобувача в отриманні наукових результатів.

Всі основні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. У роботах [1], [6], [10] здобувачем досліджено методи виявлення аномалій у API-журналах; виконано аналіз особливостей обробки API-трафіку, проведено експериментальне моделювання процесів аналізу журналів подій та обґрунтовано можливість

використання методів машинного навчання для автоматизованого виявлення аномальної активності у програмних системах. У роботах [2], [7] здобувачем розроблено метод виявлення аномалій у поведінці користувачів вебсайтів; сформовано підхід до аналізу поведінкових сценаріїв, реалізовано алгоритми обробки поведінкових характеристик користувачів та проведено експериментальне оцінювання ефективності запропонованого підходу. У роботах [3], [9] здобувачем запропоновано метод виявлення аномалій у Kubernetes-кластерах із використанням моделі LSTM Autoencoder; здійснено формування наборів ознак на основі телеметрії контейнеризованих середовищ, реалізовано моделі аналізу часових послідовностей подій та виконано оцінювання точності виявлення аномальної активності у Kubernetes-середовищах. Окремі підходи до аналізу мережевого трафіку та обробки великих обсягів даних у розподілених інфраструктурах, представлені у роботі [5], використано як додаткову методологічну основу дослідження. У роботах [4], [8] здобувачем розроблено архітектуру мультиагентної системи виявлення аномалій із використанням методів машинного навчання; сформовано функціональну та структурну модель системи, визначено взаємозв'язки між модулями збору даних, аналізу подій, виявлення аномалій і моніторингу безпеки у розподілених програмних середовищах.

5. Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій.

Достовірність результатів підтверджується узгодженістю теоретичних розрахунків з моделюванням та експериментами, проведеними на програмному прототипі. Порівняння теоретичних прогнозів із моделями конкурентних робіт і з емпіричними даними показало близьку збіжність, а розбіжності залишилися у межах статистичної похибки, що свідчить про коректність припущень і адекватність вибраних алгоритмів.

Здобувач коректно вводить нові поняття. Припущення, введені в дисертації, логічні та правомірні. Основні висновки і рекомендації, що сформульовані в роботі, мають як теоретичне, так і експериментальне обґрунтування на базі методів обчислювального експерименту.

6. Ступінь новизни основних результатів дисертації порівняно з відомими дослідженнями аналогічного характеру.

При розв'язанні сформульованої наукової задачі в роботі отримано нові наукові результати:

- удосконалено метод виявлення аномальної поведінки користувачів вебресурсів шляхом формування індивідуального поведінкового профілю на основі інтеграції часових характеристик сесій, показників активності та послідовностей переходів між вебресурсами. На відміну від існуючих підходів, метод забезпечує комплексне врахування часових, кількісних і послідовнісних ознак під час побудови профілю нормальної поведінки та оцінювання аномальності, що дозволило підвищити повноту виявлення аномалій на 11,0% та F1-міру на 11,4% порівняно з методом One-Class SVM;

- удосконалено метод виявлення аномалій у Kubernetes-кластерах шляхом інтеграції мережевих характеристик, метрик контейнерів та показників стану кластера в єдині часові послідовності ознак для формування профілю нормального функціонування контейнеризованого середовища. На відміну від існуючих підходів, метод забезпечує комплексне врахування взаємозв'язків між різнорідними джерелами телеметричних даних та їх часової динаміки під час оцінювання аномальності, що дозволило підвищити якість виявлення аномальної активності та забезпечити виявлення раніше невідомих атак у динамічних середовищах Kubernetes;

- отримала подальший розвиток модель мультиагентної інтелектуальної системи виявлення аномалій у хмарних середовищах, яка відрізняється інтеграцією агентів збору мережевих подій, телеметрії Kubernetes, API-журналів та поведінкових даних користувачів у межах єдиного процесу моніторингу. На відміну від централізованого сигнатурного моніторингу на базі Snort, запропонована модель забезпечує багаторівневий аналіз подій безпеки та дозволяє підвищити повноту виявлення кіберзагроз на 18%, зменшити кількість хибнопозитивних спрацювань на 23% і скоротити час виявлення інцидентів на 29%.

7. Практична цінність результатів дослідження та їх впровадження.

Результати дисертаційної роботи впроваджено на підприємстві ТОВ «РЕІНВЕНТІНГ СОФТВЕР ДЕВЕЛОПМЕНТ» для використання при розробці та застосуванні методів і моделей інтелектуальної системи виявлення аномалій у хмарних сервісах, зокрема для аналізу API-журналів,

телеметрії Kubernetes - кластерів та підвищення ефективності моніторингу безпеки програмних систем.

8. Перелік наукових праць, що відображають основні результати дисертації.

Матеріали дисертації викладено у 10-и публікаціях, з них – 1 розділ монографії, що індексується в Scopus та 4 статті у наукових фахових виданнях України категорії Б; 5 тез доповідей у матеріалах міжнародних науково-технічних конференцій.

1. Мартовицький В. В., Свиридов А. С., Авдєєв О. В., Гудзинський І. М., Коротецький О. В. Дослідження методів виявлення аномалій у API журналах для забезпечення безпеки та надійності програмних систем // Вісник Херсонського національного технічного університету. 2025. Т. 2, № 1(92). С. 142–148. DOI: https://doi.org/10.35546/kntu2078-4481.2025.1.2.19.

2. Свиридов А. С., Гусейнов Р. Б., Винниченко С. М. Метод виявлення аномалій у поведінці користувача вебсайту // Herald of Khmelnytskyi National University. Technical Sciences. 2026. Т. 363, № 2. С. 211–219. DOI: https://doi.org/10.31891/2307-5732-2026-363-28.

3. Свиридов А. С., Сєвєрінов О. В. Метод виявлення аномалій у Kubernetes-кластерах з використанням LSTM Autoencoder // Herald of Khmelnytskyi National University. Technical Sciences. 2026. Т. 361, № 1. С. 501–509. DOI: https://doi.org/10.31891/2307-5732-2026-361-70.

4. Свиридов А. С., Гудзинський І. М. Архітектура мультиагентної системи виявлення вторгнень із використанням машинного навчання // Вісник Херсонського національного технічного університету. 2026. Т. 1, № 2(97). С. 360–366. DOI: https://doi.org/10.35546/kntu2078-4481.2026.2.44.

5. Kuchuk G., Kovalenko A., Elyasi Komari I., Svyrydov A., Kharchenko V. Improving Big Data Centers Energy Efficiency: Traffic Based Model and Method // Advances in Computer Science for Engineering and Education II. Cham : Springer, 2019. P. 77–88. DOI: https://doi.org/10.1007/978-3-030-00253-4_8.

6. Сєвєрінов О. В., Свиридов А. С. Виявлення аномалій у API журналах для підвищення безпеки програмних систем // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доповідей тринадцятої міжнародної науково-технічної конференції,

27–28 листопада 2025 р. Харків, 2025. Т. 3, секц. 4. С. 35. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/97139.

7. Свиридов А. С. Метод виявлення аномалій у поведінці користувачів вебсайтів // Science and education: synergy of innovation : Proceedings of the 8th International scientific and practical conference, Berlin, Germany, 23–25 March 2026. Berlin : MDPC Publishing, 2026. P. 198. URL: https://sci-conf.com.ua/viii-mizhnarodna-naukovo-praktichna-konferentsiya-science-and-education-synergy-of-innovation-23-25-03-2026-berlin-nimechchina-arhiv/.

8. Свиридов А. С. Архітектура мультиагентної системи виявлення вторгнень із використанням машинного навчання // Scientific development in a changing world : Proceedings of the 3rd International scientific and practical conference, Lviv, Ukraine, 16–18 March 2026. Львів : SPC "Sci-conf.com.ua", 2026. P. 330. URL: https://sci-conf.com.ua/iii-mizhnarodna-naukovo-praktichna-konferentsiya-scientific-development-in-a-changing-world-16-18-03-2026-lviv-ukrayina-arhiv/.

9. Свиридов А. С. Метод виявлення аномалій у Kubernetes-кластерах з використанням LSTM Autoencoder // European science and innovation congress : Proceedings of the 4th International scientific and practical conference, Barcelona, Spain, 9–11 March 2026. Barcelona : Barca Academy Publishing, 2026. P. 169. URL: https://sci-conf.com.ua/iv-mizhnarodna-naukovo-praktichna-konferentsiya-european-science-and-innovation-congress-9-11-03-2026-barselona-ispaniya-arhiv/.

10. Свиридов А. С., Сєвєрінов О. В. Дослідження методів виявлення аномалій у API журналах для забезпечення безпеки та надійності програмних систем // Сучасні проблеми інфокомунікацій, радіоелектроніки та наносистем: тези доповідей шістнадцятої міжнародної науково-технічної конференції, 29–30 квітня 2026 р. Харків, 2026. Т. 3, секц. 4. С. 112–113. URL: https://openarchive.nure.ua/server/api/core/bitstreams/0209b944-1967-4af8-b449-d5b52322b2de/content.

9. Апробація основних результатів дослідження.

Основні положення дисертаційної роботи представлено на наступних міжнародних науково-технічних конференціях і форумах:

- на Тринадцятій міжнародній науково-технічній конференції

«Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління», 27–28 листопада 2025 р.;

- на Міжнародній науково-практичній конференції «Science and education: synergy of innovation», Berlin, Germany, 2026 р.;
- на Міжнародній науково-практичній конференції «Scientific development in a changing world», Lviv, Ukraine, 2026 р.;
- на Міжнародній науково-технічній конференції «European science and innovation congress», Barcelona, Spain, 2026 р.;
- на Шістнадцятій міжнародній науково-технічній конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління», 29 – 30 квітня 2026 р.

10. Оцінка структури дисертації, її мови та стилю викладення.

Дисертаційна робота є доступною для розуміння. Дисертант вільно володіє науково-технічною термінологією. Матеріал дисертації викладено послідовно та продумано, із чітким розумінням цілей та методів дослідження.

У ході обговорення дисертації до неї були висунуті деякі зауваження, але це не змінює суті самої роботи.

З урахуванням зазначеного на засіданні кафедри безпеки інформаційних технологій, **вважати, що**:

1. Дисертація Свиридова Артема Сергійовича «Модель та методи інтелектуальної системи виявлення аномалій в хмарних сервісах» є завершеною науковою працею, у якій розв'язано конкретну науково-прикладну задачу виявлення аномалій у хмарних сервісах та контейнеризованих середовищах, що має важливе значення для галузі знань 12 Інформаційні технології.

2. У 10 наукових публікаціях повністю відображені основні результати дисертації, із них 4 статті у наукових фахових виданнях України; 1 розділ монографії, який входять до міжнародної наукометричної бази Scopus.

3. Дисертація відповідає вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України

від 12.01.2022 № 44 та наказу Міністерства освіти і науки України від 12.01.2017 № 40 «Про затвердження вимог до оформлення дисертації».

4. З урахуванням наукової зрілості та професійних якостей Свиридова Артема Сергійовича дисертація на тему «Модель та методи інтелектуальної системи виявлення аномалій в хмарних сервісах» рекомендується для подання до розгляду та захисту у разовій СВР.

Рішення прийнято одноголосно

Завідувач кафедри
безпеки інформаційних технологій
д.т.н., професор Генадій ХАЛІМОВ

Експерти:
к.т.н., доцент Олексій ЛЯШЕНКО

к.т.н., доцент Олександр ФЕДЮШИН