Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U005177

Особливі позначки: відкрита

Дата реєстрації: 07-09-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Свиридов Артем Сергійович
2. Artem Svyrydov

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека та захист інформації

Дата захисту: 07-09-2026

Спеціальність за освітою: Системне програмування

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 16654

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 28.23.25, 28.23.29, 28.23.37, 28.17.19

Тема дисертації:

1. Модель та методи інтелектуальної системи виявлення аномалій в хмарних сервісах

2. Model and methods of an intelligent anomaly detection system for cloud services

Реферат/анотація:

1. Свиридов А.С. Модель та методи інтелектуальної системи виявлення аномалій в хмарних сервісах. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека (12 – Інформаційні технології). – Харківський національний університет радіоелектроніки, Міністерство освіти і науки України, Харків, 2026. Актуальність роботи зумовлена стрімким розвитком хмарних технологій, широким впровадженням мікросервісної архітектури, контейнеризації та оркестрації застосунків, що супроводжується зростанням складності програмних систем і підвищенням рівня кіберзагроз. Сучасні хмарні середовища генерують значні обсяги різнорідних даних, зокрема API-журнали, мережеві події, телеметрію контейнерів і поведінкові дані користувачів, аналіз яких традиційними методами часто не забезпечує своєчасного виявлення аномалій, вторгнень і прихованих загроз. Існуючі підходи до моніторингу безпеки переважно мають обмежену адаптивність до динамічних змін середовища, складно масштабуються та недостатньо ефективно враховують поведінкові особливості сучасних розподілених систем. Використання методів штучного інтелекту та машинного навчання дозволяє

автоматизувати процес аналізу великих обсягів даних, виявляти приховані закономірності, поведінкові відхилення та аномальні патерни, що підвищує рівень безпеки, надійності та стійкості хмарних програмних застосунків. Метою дисертаційної роботи є 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. Об'єктом дослідження є процеси збору, обробки та аналізу журналів подій, API-трафіку, поведінкових характеристик користувачів і телеметрії хмарної інфраструктури в системах виявлення аномалій. Предметом дослідження є моделі та методи інтелектуальної інформаційної технології виявлення аномалій у хмарних сервісах на основі алгоритмів машинного та глибокого навчання, спрямовані на підвищення точності виявлення загроз, адаптивності систем безпеки та зниження ризиків функціонування програмних систем в умовах динамічних кіберзагроз. Наукова новизна отриманих результатів полягає в такому: 1. 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. 2. 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. 3. 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%.

2. Svyrydov A.S. Model and methods of an intelligent anomaly detection system for cloud services. – Qualifying scientific work on the rights of a manuscript. The dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 125 – Cyber security (12 – Information Technologies). – Kharkiv National University of Radio Electronics of the Ministry of Education and Science of Ukraine, Kharkiv, 2026. The relevance of the research is determined by the rapid development of cloud technologies, widespread adoption of microservice architecture, containerization, and orchestration of applications, which are accompanied by increasing software complexity and growing cybersecurity threats. Modern cloud environments generate large volumes of heterogeneous data, including API logs, network events, container telemetry, and user behavioral data, the analysis of which by traditional methods often fails to ensure timely detection of anomalies, intrusions, and hidden threats. Existing security monitoring approaches usually have limited adaptability to dynamic environmental changes, are difficult to scale, and insufficiently account for the behavioral characteristics of modern distributed systems. The application of artificial intelligence and machine learning methods makes it possible to automate the analysis of large-scale data, identify hidden patterns and anomalous behaviors, and improve the security, reliability, and resilience of cloud software applications. The purpose of the dissertation is to improve the efficiency of anomaly detection in cloud services through the development of models and methods of an intelligent information technology that ensure the integration of heterogeneous data, automated event analysis, and adaptive cyber threat detection in containerized and distributed environments. The object of research is the processes of collecting, processing, and analyzing event logs, API traffic, user behavioral characteristics, and cloud infrastructure telemetry in anomaly detection systems. The subject of research is the models and methods of an intelligent

information technology for anomaly detection in cloud services based on machine learning and deep learning algorithms aimed at improving threat detection accuracy, security system adaptability, and risk reduction in software systems under dynamic cyber threats. The scientific novelty of the obtained results is as follows: 1. A method for detecting anomalous behavior among users of web resources has been improved by creating an individual behavioral profile based on the integration of session duration, activity metrics, and sequences of transitions between web resources. Unlike existing approaches, this method comprehensively accounts for temporal, quantitative, and sequential features when constructing a profile of normal behavior and assessing anomalies, which increased the recall of anomaly detection by 11.0% and the F1 score by 11.4% compared to the One-Class SVM method. 2. We have improved the method for detecting anomalies in Kubernetes clusters by integrating network characteristics, container metrics, and cluster health indicators into a unified time series of features to form a profile of normal operation in a containerized environment. Unlike existing approaches, the method comprehensively accounts for the interrelationships between heterogeneous sources of telemetry data and their temporal dynamics when assessing anomalies, which has improved the quality of anomaly detection and enabled the detection of previously unknown attacks in dynamic Kubernetes environments. 3. The multi-agent intelligent anomaly detection system model for cloud environments has been further developed, distinguished by the integration of agents responsible for collecting network events, Kubernetes telemetry, API logs, and user behavioral data within a unified monitoring process. In contrast to centralized signature-based monitoring using Snort, the proposed model provides multi-level security event analysis and enables an 18% increase in cyber threat detection recall, a 23% reduction in false positive detections, and a 29% decrease in incident detection time.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Новий напрямок у науці і техніці

Публікації:

- 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: 10.1007/978-3-030-00253-4_8.

Наукова (науково-технічна) продукція: методи, теорії, гіпотези

Соціально-економічна спрямованість: забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Сєвєрінов Олександр Васильович

2. Oleksandr V. Sievierinov

Кваліфікація: к.т.н., доц., 20.02.12

Ідентифікатор ORCID ID: 0000-0002-6327-6405

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Бульба Сергій Сергійович

2. Serhii Bulba

Кваліфікація: к.т.н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0003-0358-7516

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Голубничий Дмитро Юрійович

2. Dmytro Y. Holubnychyi

Кваліфікація: к.т.н., доц.

Ідентифікатор ORCID ID: 0000-0002-6873-7004

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний економічний університет імені Семена Кузнеця

Код за ЄДРПОУ: 02071211

Місцезнаходження: проспект Науки, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Барковська Олеся Юріївна

2. Olesia Y. Barkovska

Кваліфікація: к.т.н., доц., 05.13.23

Ідентифікатор ORCID ID: 0000-0001-7496-4353

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Ляшенко Олексій Сергійович

2. Oleksii Liashenko

Кваліфікація: к.т.н., доцент, 05.13.07

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Аксак Наталія Георгіївна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Аксак Наталія Георгіївна
Відповідальний за підготовку облікових документів	Іванова Олена Олександрівна
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна