

РЕЦЕНЗІЯ

рецензента Барковської Олеси Юріївни

кандидата технічних наук, доцента

на дисертаційну роботу Свиридова Артема Сергійовича

на тему: «Модель та методи інтелектуальної системи виявлення аномалій в
хмарних сервісах»

подану до захисту на здобуття наукового ступеня доктора філософії

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Актуальність теми дослідження.

Проблема забезпечення кібербезпеки хмарних сервісів сьогодні є однією з найважливіших у сфері інформаційних технологій. Інтенсивне використання контейнеризації, платформ Kubernetes та мікросервісної архітектури супроводжується збільшенням кількості потенційних векторів атак, що вимагає удосконалення існуючих підходів до моніторингу безпеки та виявлення аномальної активності.

Особливістю сучасних хмарних середовищ є формування великих обсягів різномірних даних, зокрема API-журналів, мережевої телеметрії, метрик контейнерів та поведінкових характеристик користувачів. Аналіз такої інформації традиційними методами є недостатньо ефективним через складність її структури, високу швидкість надходження та необхідність реагування в режимі реального часу.

У цих умовах особливої актуальності набуває застосування технологій штучного інтелекту та машинного навчання для автоматизації процесів аналізу даних і виявлення кіберзагроз. Запропоновані автором модель та методи інтелектуальної системи дозволяють інтегрувати різномірні джерела інформації, підвищити точність виявлення аномалій і забезпечити адаптивність системи до змін хмарного середовища. З огляду на це тема дисертаційної роботи є актуальною та повністю відповідає сучасним тенденціям розвитку кібербезпеки.

Оцінка змісту дисертації, її завершеності в цілому та оформлення.

Дисертаційна робота має чітку та логічно побудовану структуру, що складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Матеріал викладено послідовно, у науковому стилі, а структура роботи відповідає вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії. Наукові положення, сформульовані у дисертації, є достатньо обґрунтованими та підтверджуються результатами теоретичних досліджень, математичного й комп'ютерного моделювання, а також експериментальною перевіркою.

У роботі виконано комплексний аналіз сучасних підходів до виявлення аномалій у хмарних сервісах, забезпечення безпеки контейнеризованих середовищ і застосування методів машинного та глибокого навчання у системах кібербезпеки. На основі проведеного аналізу автором запропоновано модель інтелектуальної системи та методи виявлення аномалій за API-журналами і телеметричними даними Kubernetes-кластерів, що мають практичну спрямованість і можуть бути використані під час побудови сучасних систем моніторингу безпеки хмарної інфраструктури.

У вступі належним чином обґрунтовано актуальність теми дослідження, сформульовано мету, завдання, об'єкт і предмет дослідження, визначено наукову новизну та практичне значення отриманих результатів, а також наведено відомості щодо їх апробації та публікації.

У першому розділі дисертаційної роботи досліджено сучасний стан проблеми виявлення аномалій у хмарних сервісах. Проаналізовано існуючі підходи до забезпечення безпеки хмарної інфраструктури, методи аналізу API-журналів, телеметричних даних Kubernetes-кластерів, а також сучасні алгоритми машинного навчання, що застосовуються для виявлення аномальної активності. За результатами аналізу визначено основні недоліки існуючих підходів та обґрунтовано напрями подальших досліджень.

У другому розділі запропоновано метод виявлення аномалій у Kubernetes-кластерах на основі моделі LSTM Autoencoder. Обґрунтовано вибір інформативних ознак, описано процедури попередньої обробки даних,

формування навчальних вибірок та наведено результати експериментальної перевірки ефективності запропонованого методу.

У третьому розділі розроблено метод виявлення аномалій на основі API-журналів хмарних сервісів, який ґрунтується на аналізі поведінкових характеристик користувачів із використанням моделі LSTM Autoencoder. Представлено процес підготовки даних, побудови моделі та оцінювання її ефективності за результатами експериментальних досліджень.

У четвертому розділі запропоновано модель мультиагентної інтелектуальної системи виявлення аномалій у хмарних сервісах та описано її програмну реалізацію. Наведено архітектуру системи, принципи взаємодії її компонентів, а також результати апробації розроблених моделі і методів на реальних наборах даних.

Загалом дисертаційна робота характеризується логічною структурою, взаємопов'язаністю її розділів і належним рівнем обґрунтованості отриманих наукових результатів. Роботу оформлено відповідно до встановлених вимог, а виклад матеріалу є послідовним, чітким і зрозумілим.

Основні наукові результати, одержані автором, та їх новизна.

У дисертаційній роботі отримано нові наукові результати, які є вагомим внеском у розвиток моделей і методів інтелектуального виявлення аномалій у хмарних сервісах. Наукова новизна дисертаційного дослідження 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 мережових 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 мережових 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%.

Таким чином, результати дисертаційного дослідження мають наукову новизну, сприяють розвитку моделей і методів інтелектуального виявлення аномалій у хмарних сервісах та можуть бути використані для підвищення ефективності систем моніторингу й забезпечення кібербезпеки сучасної хмарної інфраструктури.

Наукові публікації.

Основні результати дисертаційного дослідження пройшли належну апробацію та висвітлені у наукових публікаціях і матеріалах наукових конференцій. Здобувачем виконано встановлені вимоги щодо оприлюднення результатів дисертаційної роботи.

За темою дисертації опубліковано 10 наукових праць, серед яких один розділ монографії, що індексується в наукометричній базі Scopus, чотири статті

у наукових фахових виданнях України категорії Б та п'ять тез доповідей у матеріалах міжнародних наукових конференцій.

Тематика опублікованих праць відображає основні напрями виконаного дослідження, зокрема аналіз сучасних підходів до виявлення аномалій у хмарних сервісах, розроблення моделі і методів інтелектуальної системи виявлення аномалій, застосування методів машинного навчання для аналізу API-журналів і телеметричних даних Kubernetes-кластерів, а також результати експериментальної перевірки запропонованих рішень.

Обсяг і зміст наукових публікацій свідчать про достатній рівень апробації результатів дисертаційного дослідження, підтверджують їх актуальність та відповідність сучасному рівню досліджень у цій галузі, а також засвідчують наукову новизну, обґрунтованість і достовірність отриманих результатів. Представлення результатів у фахових виданнях і на наукових конференціях забезпечило їх фахове обговорення та позитивно характеризує виконану дисертаційну роботу.

Академічна доброчесність.

Проведений аналіз дисертаційної роботи та наукових публікацій здобувача свідчить про дотримання принципів академічної доброчесності та вимог наукової етики під час виконання дисертаційної роботи.

У дисертації належним чином використано результати вітчизняних і зарубіжних наукових досліджень із обов'язковим посиланням на відповідні джерела. Використання наукових ідей, методів і результатів інших авторів здійснено відповідно до чинних вимог академічного цитування, що забезпечує дотримання норм академічної доброчесності.

Отримані у дисертації результати відображають особистий внесок здобувача у розроблення моделей та методів інтелектуальної системи виявлення аномалій у хмарних сервісах. Самостійність виконаного дослідження підтверджується запропонованими моделлю, методами, програмною реалізацією та результатами їх експериментальної перевірки.

За результатами аналізу дисертаційної роботи ознак порушення принципів академічної доброчесності не виявлено. Виконане дослідження відповідає вимогам академічної етики, а отримані результати є обґрунтованими та достовірними.

Теоретичне та практичне значення дослідження.

Результати виконаного дисертаційного дослідження мають вагомe теоретичне та практичне значення для розвитку методів і засобів забезпечення кібербезпеки хмарних сервісів. Сформульовані в роботі наукові положення сприяють подальшому розвитку моделей і методів інтелектуального виявлення аномалій, а також створюють наукове підґрунтя для вдосконалення систем моніторингу безпеки сучасної хмарної інфраструктури.

Отримані теоретичні результати спрямовані на вдосконалення методів аналізу API-журналів, телеметричних даних Kubernetes-кластерів та застосування моделей машинного і глибокого навчання для виявлення аномальної активності. Запропоновані підходи забезпечують підвищення точності виявлення кіберзагроз і покращують ефективність автоматизованого аналізу подій безпеки у хмарних середовищах.

Практична цінність роботи полягає у можливості використання розроблених моделі і методів під час створення та вдосконалення систем моніторингу кібербезпеки, платформ управління хмарною інфраструктурою та засобів аналізу подій інформаційної безпеки. Їх застосування дає змогу автоматизувати процеси збору й аналізу телеметричних даних, виявлення аномалій та підтримки прийняття рішень щодо реагування на потенційні кіберзагрози. Розроблені рішення можуть бути впроваджені у діяльність підприємств, що використовують хмарні технології, постачальників хмарних сервісів, центрів моніторингу кібербезпеки, а також організацій, які експлуатують розподілені інформаційні системи. Окремі результати дисертаційного дослідження можуть бути використані в освітньому процесі підготовки фахівців за спеціальністю 125 «Кібербезпека та захист інформації» під час викладання дисциплін, пов'язаних із безпекою хмарних обчислень,

аналізом даних та застосуванням методів штучного інтелекту в системах кібербезпеки.

Загалом результати дисертаційної роботи підтверджують доцільність використання запропонованих моделі і методів та їх практичну придатність для побудови ефективних систем виявлення аномалій і моніторингу безпеки хмарних сервісів.

Зауваження.

Дисертаційна робота справляє позитивне враження як за змістом, так і за рівнем виконання. Запропоновані наукові положення є логічно взаємопов'язаними, достатньо обґрунтованими та підтвердженими результатами проведених досліджень. Водночас окремі положення роботи доцільно розглядати як дискусійні, а саме:

1. У роботі достатньо детально описано процес формування порога прийняття рішення під час виявлення аномалій, однак доцільно було б детальніше обґрунтувати вибір його оптимального значення та проаналізувати вплив зміни цього параметра на показники якості роботи системи.

2. У дисертації основну увагу приділено аналізу журналів API та телеметричних даних Kubernetes-кластерів. Водночас перспективним виглядало б розширення дослідження шляхом включення додаткових джерел інформації, наприклад журналів операційних систем або засобів мережевого моніторингу, що могло б підвищити повноту аналізу подій безпеки.

3. У роботі наведено архітектуру програмної реалізації інтелектуальної системи, проте опис окремих програмних модулів і принципів їх взаємодії наведено досить стисло. Більш детальне висвітлення цих аспектів полегшило б відтворення запропонованого програмного рішення іншими дослідниками.

4. Експериментальна частина роботи підтверджує ефективність запропонованих методів, однак доцільно було б доповнити дослідження аналізом впливу різних типів аномалій або атак на якість їх виявлення. Такий аналіз дозволив би більш повно оцінити можливості запропонованої системи в різних сценаріях її використання.

Наведені зауваження мають переважно дискусійний характер та не впливають на загальну позитивну оцінку дисертаційної роботи.

Загальна оцінка роботи.

Дисертаційна робота Свиридова Артема Сергійовича «Модель та методи інтелектуальної системи виявлення аномалій в хмарних сервісах» є завершеним і комплексним науковим дослідженням, присвяченим розв'язанню актуального науково-прикладного завдання у сфері забезпечення кібербезпеки хмарних сервісів. У роботі виконано ґрунтовний аналіз сучасного стану наукових досліджень у галузі виявлення аномалій, сформульовано наукову проблему та запропоновано ефективні підходи до її вирішення.

Структура дисертації є логічною та послідовною, а зміст її розділів повною мірою відповідає поставленій меті й визначеним завданням дослідження. Робота вдало поєднує теоретичні розробки, пов'язані зі створенням моделі і методів інтелектуального виявлення аномалій, із програмною реалізацією та експериментальною перевіркою на реальних наборах даних. Такий підхід забезпечує належний баланс між науковою новизною та практичною цінністю отриманих результатів.

Матеріал дисертації викладено на належному науковому рівні з дотриманням встановлених вимог. Робота містить ґрунтовний огляд сучасних наукових джерел, а результати проведених експериментальних досліджень підтверджують обґрунтованість, достовірність та ефективність запропонованих моделі і методів.

Отримані наукові результати характеризуються новизною, логічною завершеністю та практичною значущістю. Запропоновані модель та методи можуть бути використані під час побудови та вдосконалення інтелектуальних систем виявлення аномалій, моніторингу стану хмарної інфраструктури та підвищення ефективності засобів забезпечення кібербезпеки хмарних сервісів.

З урахуванням наукової новизни, обґрунтованості та достовірності отриманих результатів, а також їх теоретичного і практичного значення, можна зробити висновок, що дисертаційна робота Свиридова Артема Сергійовича

«Модель та методи інтелектуальної системи виявлення аномалій в хмарних сервісах» відповідає вимогам пунктів 6, 7, 8 і 9 Порядку присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44.

Свиридов Артем Сергійович заслуговує на присудження ступеня доктора філософії за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології».

Рецензент:

кандидат технічних наук, доцент,
доцент кафедри електронних
обчислювальних машин Харківського
національного університету
радіоелектроніки



Олеся БАРКОВСЬКА