ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА

кандидата технічних наук, доцента

Бульби Сергія Сергійовича

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.

Сучасний розвиток хмарних технологій, широке використання мікросервісної архітектури та контейнеризованих середовищ суттєво змінюють підходи до побудови інформаційних систем, водночас підвищуючи вимоги до забезпечення їх кібербезпеки. Зростання кількості API-взаємодій, динамічність Kubernetes-кластерів та постійне збільшення обсягів телеметричних даних створюють нові виклики для систем моніторингу та виявлення кіберзагроз. У зв'язку з цим актуальними є дослідження, спрямовані на створення інтелектуальних методів аналізу різнорідних потоків даних і своєчасного виявлення аномальної активності.

Традиційні засоби виявлення вторгнень, які переважно базуються на сигнатурному аналізі або статичних правилах, не забезпечують необхідного рівня адаптивності до сучасних умов функціонування хмарної інфраструктури. Особливо це стосується виявлення нових або раніше невідомих атак, що потребує використання методів машинного та глибокого навчання, здатних аналізувати часові залежності, поведінкові характеристики користувачів і телеметрію контейнеризованого середовища.

Запропоновані у дисертаційній роботі модель і методи інтелектуальної системи виявлення аномалій орієнтовані на комплексне використання API-журналів, мережевих подій, телеметрії Kubernetes та поведінкових даних

користувачів, що дозволяє підвищити ефективність моніторингу безпеки хмарних сервісів. Таким чином, тема дисертаційного дослідження є актуальною, має істотне наукове та практичне значення і відповідає сучасним напрямам розвитку спеціальності 125 «Кібербезпека».

Методологія наукових досліджень

Методологія дисертаційного дослідження є логічно побудованою та відповідає поставленій меті й сформульованим завданням. Вона ґрунтується на комплексному застосуванні методів системного аналізу, математичного моделювання, машинного та глибокого навчання, а також сучасних підходів до експериментальної перевірки отриманих результатів.

У першому розділі дисертації виконано комплексний аналіз сучасного стану досліджень у галузі забезпечення безпеки хмарних сервісів, контейнеризованих середовищ і Kubernetes-кластерів. Проаналізовано існуючі методи виявлення аномалій, особливості використання API-журналів, телеметричних даних та поведінкового аналізу користувачів, визначено їх переваги, обмеження та перспективи застосування методів машинного навчання для розв'язання задач виявлення кіберзагроз.

У другому розділі запропоновано метод виявлення аномалій у Kubernetes-кластерах, який базується на комплексному аналізі мережевих характеристик, телеметрії контейнерів і показників функціонування кластера. Для аналізу часових залежностей використано модель LSTM Autoencoder, обґрунтовано вибір ознак, описано процедури підготовки даних та визначення порогового значення для виявлення аномальної активності.

У третьому розділі розроблено метод виявлення аномалій за API-журналами хмарних сервісів, що базується на аналізі поведінкових характеристик користувачів. Запропоновано підхід до формування поведінкових профілів із використанням часових, кількісних та послідовнісних ознак, а також застосовано модель LSTM Autoencoder для виявлення відхилень від нормальної поведінки користувачів.

У четвертому розділі запропоновано модель мультиагентної інтелектуальної системи виявлення аномалій у хмарних сервісах та реалізовано її програмну архітектуру. Розроблена система забезпечує автоматизований збір API-журналів і телеметричних даних, їх попередню обробку, аналіз із використанням методів глибокого навчання, а також візуалізацію результатів моніторингу безпеки.

Ефективність запропонованих моделей і методів підтверджено результатами експериментальних досліджень на реальних наборах даних, що засвідчили їх здатність забезпечувати високі показники точності виявлення аномальної активності в хмарних сервісах.

Таким чином, методологія дослідження відзначається системністю, послідовністю та достатнім рівнем наукової обґрунтованості, а отримані результати підтверджують достовірність сформульованих висновків і практичну цінність запропонованих моделі та методів для забезпечення кібербезпеки хмарної інфраструктури.

Новизна представлених досліджень.

Достовірність отриманих наукових результатів підтверджується їх теоретичним обґрунтуванням, узгодженістю з результатами експериментальних досліджень та імітаційного моделювання, а також апробацією основних положень дисертації на наукових конференціях. Основними результатами дисертаційної роботи, що мають наукову новизну, є:

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%.

Таким чином, результати дисертаційного дослідження характеризуються науковою новизною, роблять внесок у розвиток моделей і методів інтелектуального виявлення аномалій у хмарних сервісах та мають практичну цінність для створення й удосконалення систем моніторингу кібербезпеки хмарної інфраструктури.

Практична цінність дисертаційного дослідження

Дисертаційна робота має вагому практичну цінність, оскільки запропоновані автором модель та методи інтелектуальної системи виявлення аномалій орієнтовані на використання у сучасних хмарних сервісах і контейнеризованих середовищах, де особливо важливими є своєчасне виявлення кіберзагроз та забезпечення безперервності функціонування інформаційної інфраструктури.

Розроблені підходи можуть бути використані під час побудови та вдосконалення систем моніторингу безпеки хмарних сервісів, аналізу API-журналів, контролю стану Kubernetes-кластерів і виявлення аномальної активності користувачів та компонентів інфраструктури. Використання методів машинного і глибокого навчання, а також комплексний аналіз різнорідних джерел даних сприяють підвищенню ефективності автоматизованого виявлення потенційних кіберзагроз.

Практична значущість отриманих результатів підтверджується можливістю їх інтеграції до сучасних систем моніторингу інформаційної безпеки, платформ управління хмарною інфраструктурою та засобів централізованого аналізу подій кібербезпеки. Реалізований програмний прототип забезпечує автоматизований збір і обробку телеметричних даних, аналіз API-журналів, виявлення аномалій та візуалізацію результатів моніторингу.

Запропоновані модель та методи можуть бути використані підприємствами, що експлуатують хмарні сервіси, розробниками програмного забезпечення, постачальниками хмарних платформ, а також організаціями, діяльність яких пов'язана із забезпеченням кібербезпеки розподілених інформаційних систем.

Окремі результати дисертаційного дослідження можуть бути використані в освітньому процесі підготовки фахівців за спеціальністю «Кібербезпека» під час викладання дисциплін, пов'язаних із кібербезпекою хмарних технологій, аналізом даних та застосуванням методів машинного навчання у системах захисту інформації.

Аналіз наукових публікацій.

За тематикою дисертаційного дослідження автором опубліковано 10 наукових праць, серед яких один розділ монографії, що індексується у наукометричній базі Scopus, чотири статті у наукових фахових виданнях України категорії Б та п'ять тез доповідей.

Зміст опублікованих праць повною мірою відображає основні етапи та результати дисертаційного дослідження. У публікаціях висвітлено питання аналізу сучасних підходів до виявлення аномалій у хмарних сервісах, розроблення методів аналізу API-журналів і телеметрії Kubernetes-кластерів, застосування методів машинного та глибокого навчання, а також результати експериментальної перевірки запропонованих моделі і методів.

Аналіз наукових публікацій дає підстави стверджувати, що їх зміст відповідає темі дисертації, відображає основні наукові результати роботи та достатньою мірою підтверджує особистий внесок здобувача у виконане дослідження.

Апробація результатів дослідження

Апробація результатів дисертаційного дослідження здійснювалася шляхом їх представлення на міжнародних наукових конференціях, де основні положення роботи були оприлюднені, обговорені та отримали фахову оцінку наукової спільноти. Результати дослідження пройшли належну апробацію також шляхом їх публікації у фахових наукових виданнях, що свідчить про їх відповідність сучасному рівню наукових досліджень та вимогам до дисертаційних робіт.

Таким чином, результати дисертаційної роботи пройшли достатню апробацію, що підтверджує їх обґрунтованість, достовірність і практичну значущість.

Дотримання норм академічної доброчесності.

Проведений аналіз дисертаційної роботи та наукових публікацій здобувача свідчить про те, що дослідження виконано з дотриманням принципів академічної доброчесності та вимог наукової етики. У роботі використано результати вітчизняних і зарубіжних наукових досліджень із належним посиланням на першоджерела, а цитування та використання наукових матеріалів здійснено відповідно до встановлених академічних норм.

Наукові результати, наведені у дисертації, отримані автором самостійно та відображають його особистий внесок у розроблення моделі і методів

інтелектуальної системи виявлення аномалій у хмарних сервісах. За результатами ознайомлення з дисертаційною роботою та науковими публікаціями здобувача підстав вважати, що під час виконання дослідження були порушені принципи академічної доброчесності, не встановлено.

Зауваження.

Проведений аналіз змісту дисертаційної роботи, її структури, теоретичних положень, запропонованих моделі і методів, а також результатів їх експериментальної перевірки дає підстави загалом позитивно оцінити виконане дослідження. Дисертація є завершеною науковою працею, у якій послідовно вирішено поставлені наукові завдання, а отримані результати відповідають визначеній меті дослідження. Матеріал викладено логічно, у науковому стилі, державною мовою, а оформлення роботи відповідає встановленим вимогам. Водночас, високо оцінюючи науковий рівень і практичне значення дисертації, доцільно висловити окремі зауваження, які мають переважно дискусійний характер, зокрема:

1. У дисертаційній роботі наведено результати експериментальних досліджень для обраних наборів даних, однак недостатньо висвітлено питання універсальності запропонованих методів щодо їх застосування в інших типах хмарних платформ або середовищ контейнеризації. Розширення такого аналізу дозволило б краще оцінити можливості масштабування запропонованих рішень.

2. Автором детально описано архітектуру мультиагентної системи, проте взаємодію окремих агентів під час виникнення складних або комбінованих атак розглянуто лише в загальному вигляді. Більш детальний аналіз сценаріїв їхньої спільної роботи міг би посилити практичну складову дослідження.

3. У роботі основну увагу приділено виявленню аномалій, тоді як питання подальшої автоматизованої реакції на виявлені інциденти або інтеграції з системами реагування на кіберзагрози висвітлено стисло. Розгляд таких аспектів міг би розширити можливості практичного використання запропонованої системи.

4. У дисертації запропоновано програмну реалізацію інтелектуальної системи, однак окремі питання, пов'язані з розгортанням програмного забезпечення у промислових умовах, зокрема вимоги до обчислювальних ресурсів і особливості інтеграції з існуючою хмарною інфраструктурою, розглянуто недостатньо детально. Їх більш повне висвітлення підвищило б практичну цінність роботи.

Наведені зауваження мають переважно дискусійний характер, не є принциповими, не впливають на загальну позитивну оцінку дисертаційного дослідження та окреслюють можливі напрями його подальшого розвитку.

Загальна оцінка роботи.

Дисертаційна робота Свиридова Артема Сергійовича «Модель та методи інтелектуальної системи виявлення аномалій в хмарних сервісах» є завершеним науковим дослідженням, у якому вирішено актуальне науково-прикладне завдання у сфері кібербезпеки хмарних сервісів. Робота характеризується належним рівнем наукової обґрунтованості, методологічної цілісності та практичної спрямованості, що дає підстави розглядати її як самостійне, логічно побудоване й завершене дисертаційне дослідження.

У дисертації виконано ґрунтовний аналіз сучасних підходів до виявлення аномалій у хмарних сервісах, забезпечення безпеки контейнеризованих середовищ та використання методів машинного навчання для аналізу поведінки користувачів і компонентів хмарної інфраструктури. На основі проведеного аналізу автором запропоновано власні модель та методи, які поєднують теоретичні розробки з програмною реалізацією та експериментальною перевіркою на реальних наборах даних. Такий підхід забезпечив отримання результатів, що мають наукову новизну та практичну цінність для побудови сучасних систем моніторингу кібербезпеки хмарних сервісів.

Дисертаційна робота вирізняється комплексним і послідовним підходом до розв'язання поставлених наукових завдань, що дозволило досягти визначеної мети дослідження та отримати науково обґрунтовані результати, підтверджені експериментальними дослідженнями та їх практичною апробацією. Побудова

дисертації є логічною та послідовною: у кожному розділі сформульовано відповідні завдання, обґрунтовано використані методи, наведено результати досліджень і виконано їх аналіз.

Основні наукові положення, висновки та рекомендації достатньо аргументовані й підтверджені результатами теоретичних досліджень, математичного та комп'ютерного моделювання, а також експериментальної перевірки запропонованих моделі і методів. Проведений аналіз сучасних наукових праць дозволив автору обґрунтувати актуальність дослідження та визначити власний внесок у розвиток моделей і методів інтелектуального виявлення аномалій у хмарних сервісах.

Враховуючи наукову новизну, обґрунтованість і достовірність отриманих результатів, їх теоретичне та практичне 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».

Офіційний опонент:
кандидат технічних наук, доцент, доцент
кафедри комп'ютерної інженерії та
програмування Національного технічного
університету «Харківський політехнічний
інститут»
кандидат технічних наук, доцент Сергій БУЛЬБА