

ВІДГУК

ОФІЦІЙНОГО ОПОНЕНТА

кандидата технічних наук, доцента

Голубничого Дмитра Юрійовича

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

1. Актуальність теми дослідження.

Актуальність теми дисертаційного дослідження обумовлена стрімким розвитком хмарних обчислень, широким впровадженням мікросервісної архітектури, контейнеризації та платформ оркестрації, зокрема Kubernetes, що супроводжується суттєвим зростанням кількості й складності кіберзагроз. Забезпечення безпеки сучасних хмарних сервісів є одним із пріоритетних напрямів розвитку інформаційних технологій, оскільки компрометація API-інтерфейсів, контейнеризованих застосунків і компонентів хмарної інфраструктури може призводити до порушення функціонування критично важливих інформаційних систем. У межах спеціальності 125 «Кібербезпека» особливої актуальності набуває розробка інтелектуальних моделей і методів аналізу великих обсягів різномірних даних для своєчасного виявлення аномалій та кіберзагроз.

Однією з основних проблем сучасних систем моніторингу безпеки є недостатня ефективність традиційних сигнатурних і статистичних методів в умовах динамічної хмарної інфраструктури. Постійна зміна конфігурації контейнеризованих середовищ, масштабування мікросервісів, зростання обсягів API-трафіку та телеметричних даних, а також поява нових типів атак істотно ускладнюють процес своєчасного виявлення аномальної активності. Це зумовлює необхідність застосування сучасних методів машинного та глибокого

навчання, здатних адаптуватися до змін середовища, аналізувати часові залежності та виявляти раніше невідомі кіберзагрози.

Окремо слід зазначити, що тематика та спрямованість дисертаційного дослідження узгоджуються з положеннями наказу Адміністрації Держспецв'язку від 14.09.2024 № 505 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту при використанні технології хмарних обчислень та Методичних рекомендацій щодо оцінки відповідності хмарних послуг рівням безпеки (впевненості)». Зокрема, розглянуті у дисертації питання моніторингу хмарної інфраструктури, аналізу подій безпеки, використання телеметрії Kubernetes-кластерів, API-журналів і поведінкових даних користувачів відповідають сучасним підходам до забезпечення кіберзахисту хмарних сервісів та оцінювання їхньої безпеки.

Запропонований у дисертаційній роботі підхід, що ґрунтується на застосуванні моделей машинного та глибокого навчання, зокрема LSTM Autoencoder, дозволяє підвищити ефективність виявлення аномальної активності, забезпечити адаптивність системи до змін хмарного середовища та покращити моніторинг кібербезпеки в режимі, наближеному до реального часу.

Таким чином, дисертаційне дослідження, присвячене розробці моделі та методів інтелектуальної системи виявлення аномалій у хмарних сервісах, є своєчасним, має вагоме наукове і практичне значення та повною мірою відповідає актуальним завданням галузі знань 12 «Інформаційні технології» та спеціальності 125 «Кібербезпека».

2. Ступінь обґрунтованості наукових положень.

Наукові положення, висновки та практичні рекомендації, наведені у дисертаційній роботі, загалом є обґрунтованими та підтверджуються результатами теоретичних і експериментальних досліджень. Мета роботи логічно узгоджується з поставленими завданнями, а отримані результати повністю відповідають сформульованим цілям дослідження.

У першому розділі дисертації виконано ґрунтовний аналіз сучасних підходів до забезпечення безпеки хмарних сервісів, особливостей функціонування Kubernetes-кластерів, мікросервісної архітектури та

контейнеризованих середовищ. Розглянуто існуючі методи виявлення аномалій і системи моніторингу безпеки, проаналізовано їх переваги та недоліки, що дозволило обґрунтувати необхідність використання методів машинного та глибокого навчання для аналізу подій безпеки.

У другому розділі запропоновано удосконалений метод виявлення аномалій у Kubernetes-кластерах, який базується на інтеграції мережових характеристик, метрик контейнерів і показників стану кластера. Запропонований підхід використовує модель LSTM Autoencoder для аналізу часових послідовностей, що забезпечує підвищення ефективності виявлення аномальної активності в контейнеризованому середовищі.

У третьому розділі розроблено метод виявлення аномалій у API-журналах хмарних сервісів шляхом аналізу поведінкових характеристик користувачів. Запропоновано механізм формування поведінкових профілів, що враховує часові, кількісні та послідовнісні ознаки користувацької активності. Проведені експериментальні дослідження підтвердили ефективність запропонованого підходу та його переваги порівняно з існуючими рішеннями.

У четвертому розділі розроблено модель інтелектуальної системи виявлення аномалій у хмарних сервісах та реалізовано її програмний прототип. Запропонована архітектура інтегрує модулі збору API-журналів, телеметрії Kubernetes, машинного навчання та засоби візуалізації результатів моніторингу. Проведені експериментальні дослідження підтвердили працездатність системи та можливість її практичного використання.

Таким чином, основні наукові положення дисертаційної роботи є достатньо аргументованими, підтверджуються результатами експериментального моделювання, програмної реалізації та апробації отриманих результатів.

3. Новизна отриманих результатів.

Достовірність наукових положень забезпечується їх теоретичним обґрунтуванням, підтверджується результатами імітаційного моделювання та апробацією основних результатів дослідження на міжнародних науково-

технічних і науково-практичних конференціях. Основними науковими результатами, що характеризують новизну дисертаційної роботи, є такі:

- 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 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.

- 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, отримані в дисертаційній роботі результати характеризуються науковою новизною на рівні удосконалення методів і подальшого розвитку моделі інтелектуальної системи виявлення аномалій в

хмарних сервісах на основі методів машинного та глибокого навчання та мають практичне значення для побудови інтелектуальних систем моніторингу безпеки хмарної інфраструктури.

4. Аналіз наукових публікацій.

Апробацію результатів дисертаційної роботи здійснено шляхом їх висвітлення у наукових публікаціях та доповідями на міжнародних науково-технічних конференціях. За результатами проведених досліджень опубліковано 10 наукових праць, серед яких один розділ колективної монографії, що індексується у базі Scopus, чотири статті у наукових фахових виданнях України категорії Б та п'ять публікацій у матеріалах міжнародних науково-технічних конференцій.

Опубліковані праці повною мірою відображають основні етапи виконаного дослідження – від аналізу сучасних підходів до забезпечення безпеки хмарних сервісів і виявлення аномалій до розроблення методів аналізу API-журналів, телеметрії Kubernetes-кластерів, моделі інтелектуальної системи виявлення аномалій та результатів їх експериментальної перевірки. У публікаціях висвітлено питання застосування методів машинного і глибокого навчання, аналізу поведінкових характеристик користувачів, обробки телеметричних даних та побудови систем моніторингу безпеки хмарної інфраструктури.

Наведені публікації свідчать про достатній рівень апробації результатів дисертаційної роботи та підтверджують їх оприлюднення у професійному науковому середовищі. Представлення результатів дослідження на наукових форумах та їх оприлюднення у фахових виданнях забезпечило належну наукову експертизу й обговорення отриманих результатів у професійній спільноті.

5. Дотримання норм академічної доброчесності.

Ознайомлення з дисертаційною роботою та науковими публікаціями здобувача дає підстави стверджувати, що дослідження виконано з дотриманням принципів академічної доброчесності. У дисертації коректно використано результати власних і сторонніх наукових досліджень із належним посиланням на використані джерела, що відповідає загальноприйнятим вимогам щодо цитування та використання наукових матеріалів. Наукові результати,

представлені у дисертації, отримані автором самостійно та відображають його особистий внесок у розв'язання актуальної науково-прикладної задачі, пов'язаної з розробленням моделі й методів інтелектуальної системи виявлення аномалій у хмарних сервісах. Основні положення роботи пройшли апробацію шляхом публікації у фахових наукових виданнях та представлення на міжнародних науково-технічних конференціях. За результатами аналізу дисертаційної роботи ознак порушення принципів академічної доброчесності не виявлено.

6. Значущість наукового дослідження.

Дисертаційна робота має вагоме теоретичне та практичне значення. Теоретичні результати дослідження сприяють подальшому розвитку моделей і методів інтелектуального виявлення аномалій у хмарних сервісах, а також розширюють науково-методичні засади застосування методів машинного та глибокого навчання для аналізу різнорідних даних у системах кібербезпеки. Запропоновані автором модель мультиагентної інтелектуальної системи та удосконалені методи аналізу API-журналів, поведінкових характеристик користувачів і телеметрії Kubernetes-кластерів доповнюють сучасні підходи до побудови адаптивних систем моніторингу безпеки хмарної інфраструктури.

Практична цінність дисертаційної роботи полягає у можливості використання отриманих результатів під час створення та модернізації систем моніторингу безпеки хмарних сервісів, платформ виявлення аномалій і програмних комплексів захисту контейнеризованих середовищ. Запропоновані рішення можуть бути використані для автоматизованого аналізу API-трафіку, моніторингу Kubernetes-кластерів, своєчасного виявлення кіберзагроз та підвищення ефективності функціонування систем кіберзахисту.

Отримані результати можуть бути використані у подальших наукових дослідженнях, а також впроваджені у практичну діяльність підприємств і організацій, що використовують хмарні технології, розробляють системи кібербезпеки або експлуатують контейнеризовану інфраструктуру. Крім того, результати роботи доцільно застосовувати під час розроблення інтелектуальних систем моніторингу безпеки, платформ аналізу подій кібербезпеки та

програмних засобів виявлення аномальної активності у розподілених інформаційних середовищах.

7. Зауваження та дискусійні положення.

Аналіз змісту дисертаційної роботи, її структури, теоретичних положень, розробленої моделі, методів та результатів експериментальних досліджень дає підстави загалом позитивно оцінити виконане дослідження. Дисертаційна робота є завершеною науковою працею, у якій послідовно вирішено поставлені завдання, а отримані результати відповідають визначеній меті дослідження. Матеріал викладено логічно, у науковому стилі, державною мовою, а оформлення дисертації відповідає встановленим вимогам.

Водночас, високо оцінюючи науковий рівень і практичну цінність виконаної роботи, доцільно висловити окремі зауваження та побажання, зокрема:

1. У роботі наведено результати експериментальної перевірки запропонованих методів на реальних наборах даних, однак порівняння виконано з обмеженою кількістю сучасних моделей глибокого навчання. Зокрема, доцільним було б доповнити дослідження порівняльним аналізом із сучасними трансформерними архітектурами або іншими актуальними методами виявлення аномалій, що дозволило б більш повно оцінити переваги запропонованого підходу.

2. Під час дослідження основну увагу приділено оцінюванню якості виявлення аномалій за показниками Accuracy, Precision, Recall та F1-score. Разом з тим доцільно було б доповнити експериментальні дослідження аналізом часових характеристик роботи системи, зокрема продуктивності та затримки виявлення аномалій у режимі реального часу, що має важливе значення для практичного впровадження запропонованих рішень.

3. У дисертаційній роботі достатньо детально описано процес формування ознак і підготовки даних, однак недостатньо уваги приділено аналізу впливу окремих груп ознак (API-журналів, телеметрії Kubernetes та мережевих характеристик) на кінцеву якість виявлення аномалій. Проведення такого

дослідження дозволило б більш обґрунтовано оцінити внесок кожного джерела даних у загальну ефективність системи.

4. Запропонована модель інтелектуальної системи передбачає інтеграцію кількох агентів збору та аналізу даних, однак у роботі лише стисло розглянуто питання відмовостійкості та функціонування системи у випадку втрати окремих джерел телеметрії або тимчасової недоступності компонентів хмарної інфраструктури. Більш детальний аналіз цих аспектів міг би посилити практичну складову дослідження.

Разом із тим наведені зауваження мають переважно рекомендаційний характер, не впливають на загальну позитивну оцінку дисертаційної роботи та окреслюють можливі напрями подальшого розвитку дослідження.

8. Загальна оцінка роботи.

Дисертаційна робота Свиридова Артема Сергійовича «Модель та методи інтелектуальної системи виявлення аномалій у хмарних сервісах» є завершеною науковою працею, у якій розв'язано актуальне науково-прикладне завдання у сфері кібербезпеки, що характеризується належним рівнем наукової обґрунтованості, методологічної цілісності та практичної спрямованості. Це дає підстави розглядати дисертацію як цілісне, логічно структуроване та завершене наукове дослідження.

Автором виконано ґрунтовний аналіз сучасного стану досліджень у галузі виявлення аномалій у хмарних сервісах, технологій контейнеризації та забезпечення безпеки Kubernetes-середовищ, на підставі якого визначено основні напрями власних наукових досліджень. У роботі вдало поєднано теоретичні дослідження, пов'язані з розробленням моделі і методів інтелектуального виявлення аномалій, із їх програмною реалізацією та експериментальною перевіркою на реальних наборах даних. Такий підхід забезпечив належне поєднання наукової новизни, практичної значущості та достовірності отриманих результатів.

Робота вирізняється комплексним підходом до розв'язання поставлених наукових завдань, що дозволило досягти визначеної мети дослідження та отримати науково обґрунтовані результати, підтверджені експериментальними

дослідженнями, програмною реалізацією та апробацією запропонованих рішень. Дисертація має чітку структуру та логічну послідовність викладу матеріалу: у кожному розділі послідовно сформульовано відповідні завдання, обґрунтовано вибір методів дослідження, наведено результати їх реалізації та виконано аналіз отриманих результатів.

Основні наукові положення, висновки та рекомендації є належним чином аргументованими й підтверджуються результатами теоретичних досліджень, математичного та комп'ютерного моделювання, а також експериментальної перевірки на реальних наборах даних. Дисертаційна робота містить ґрунтовний аналіз сучасних наукових досліджень у галузі кібербезпеки хмарних сервісів, що дозволило автору обґрунтувати власні наукові рішення та визначити особистий 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, вважаю, що дисертаційна робота Свиридова Артема Сергійовича на тему «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, а її автор заслуговує на присудження ступеня доктора філософії за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології».

Офіційний опонент:

кандидат технічних наук, доцент,

доцент кафедри інформаційних систем

Харківського національного економічного

університет імені Семена Кузнеця

кандидат технічних наук, доцент



Дмитро ГОЛУБНИЧИЙ