

РЕЦЕНЗІЯ

рецензента Ляшенка Олексія Сергійовича

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 ступеня доктора філософії

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Актуальність теми дослідження.

На сучасному етапі розвитку інформаційних технологій питання забезпечення захищеності хмарних сервісів набувають особливої актуальності у зв'язку зі зростанням масштабів використання контейнеризованих платформ, мікросервісної архітектури та розподілених обчислювальних середовищ. Одночасно збільшується кількість складних кіберзагроз, для ефективного виявлення яких традиційні методи аналізу подій безпеки вже не забезпечують необхідного рівня точності та адаптивності.

Важливою особливістю сучасних хмарних систем є наявність значних масивів різномірних даних, що формуються API-запитами, журналами подій, телеметрією Kubernetes-кластерів і поведінковими характеристиками користувачів. Ефективне використання цих даних потребує застосування сучасних інтелектуальних методів аналізу, заснованих на машинному та глибокому навчанні, які дозволяють виявляти приховані аномальні закономірності та адаптуватися до постійних змін середовища функціонування.

У цьому аспекті дисертаційне дослідження, присвячене розробці моделі та методів інтелектуальної системи виявлення аномалій у хмарних сервісах, є своєчасним і науково обґрунтованим. Отримані результати мають як теоретичну цінність для розвитку інтелектуальних методів забезпечення кібербезпеки, так і практичне значення для створення сучасних систем моніторингу безпеки

хмарної інфраструктури. Тема дисертаційної роботи повністю відповідає профілю галузі знань 12 Інформаційні технології та спеціальності 125 Кібербезпека.

Оцінка змісту дисертації, її завершеності в цілому та оформлення

Дисертаційна робота побудована відповідно до поставленої мети та завдань дослідження і характеризується послідовною структурою та логічною організацією матеріалу. Послідовність викладу забезпечує цілісне розкриття теми: від аналізу сучасного стану проблеми та обґрунтування напрямів дослідження до розроблення нових моделей і методів, їх програмної реалізації та експериментальної перевірки.

Виклад матеріалу є аргументованим і системним. У роботі простежується чіткий взаємозв'язок між теоретичними положеннями, запропонованими методами та результатами експериментальних досліджень. Обрані автором підходи й методи дослідження є належним чином обґрунтованими та відповідають поставленим завданням.

Кожний розділ дисертації має завершений характер і логічно пов'язаний з іншими розділами. У роботі послідовно висвітлено результати аналізу існуючих підходів до виявлення аномалій у хмарних сервісах, запропоновано нові методи на основі моделей машинного навчання, розроблено модель інтелектуальної системи та наведено результати оцінювання ефективності запропонованих рішень.

Експериментальна частина дослідження містить достатній обсяг результатів, які підтверджують працездатність і ефективність розроблених моделей та методів. Отримані експериментальні дані є узгодженими з теоретичними положеннями дисертації та підтверджують досягнення поставленої мети дослідження.

Дисертаційну роботу оформлено відповідно до чинних вимог. Матеріал викладено грамотно, у науково-технічному стилі, із коректним використанням спеціальної термінології. Наведені рисунки, таблиці та схеми є інформативними,

органічно доповнюють викладений матеріал і полегшують сприйняття отриманих результатів.

У цілому дисертаційна робота є завершеним науковим дослідженням, яке характеризується внутрішньою логічною узгодженістю, належним рівнем наукового опрацювання матеріалу та високою якістю оформлення.

Основні наукові результати, одержані автором, та їх новизна.

У дисертаційній роботі отримано нові наукові результати, що мають важливе значення для розвитку моделей і методів інтелектуального виявлення аномалій у хмарних сервісах. Наукова новизна дисертаційного дослідження полягає в наступному:

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, одержані в дисертаційній роботі наукові результати є новими, сприяють подальшому розвитку моделей і методів інтелектуального виявлення аномалій у хмарних сервісах та мають практичну цінність для підвищення ефективності моніторингу й забезпечення безпеки сучасних хмарних середовищ.

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 науково-технічних конференцій.

Наукові публікації охоплюють основні етапи виконаного дослідження: аналіз сучасних підходів до виявлення аномалій у хмарних сервісах, розроблення моделі і методів інтелектуальної системи виявлення аномалій, а також оцінювання ефективності запропонованих рішень за результатами експериментальних досліджень.

Обсяг і зміст опублікованих праць свідчать про достатній рівень апробації результатів дисертаційної роботи, підтверджують їх обґрунтованість, достовірність і наукову новизну. Представлення результатів дослідження у фахових виданнях і на наукових конференціях забезпечило їх експертне

обговорення та засвідчило відповідність роботи сучасним вимогам до наукових досліджень.

Академічна доброчесність.

Аналіз тексту дисертаційної роботи та наукових публікацій здобувача підтверджує дотримання ним основних принципів академічної доброчесності та вимог наукової етики на всіх етапах проведення дослідження.

У дисертації забезпечено належне використання наукових праць інших авторів із відповідним посиланням на джерела інформації. Запозичені наукові положення, методи та результати досліджень оформлено відповідно до встановлених вимог, що свідчить про відсутність ознак академічного плагіату.

Наукові результати, отримані в межах виконаного дослідження, мають самостійний та оригінальний характер і відображають особистий внесок здобувача у вирішення актуальних наукових і практичних завдань. Запропоновані модель, методи та результати експериментальної перевірки підтверджують самостійність проведеної роботи та обґрунтованість отриманих висновків.

Основні положення дисертації представлено у наукових публікаціях здобувача та апробовано під час участі у наукових конференціях, що підтверджує авторство отриманих результатів і належний рівень їх наукового оприлюднення.

За підсумками проведеного аналізу не встановлено фактів порушення принципів академічної доброчесності, зокрема наявності ознак плагіату, неправомірного використання чужих результатів або некоректного оформлення запозичених матеріалів. Це підтверджує відповідність виконаного дослідження вимогам академічної етики, а також забезпечує достовірність, об'єктивність і відкритість представлених результатів.

Теоретичне та практичне значення дослідження.

Результати дисертаційної роботи формують наукову основу для подальшого розвитку інформаційних технологій виявлення аномалій у хмарних

сервісах та систем забезпечення кібербезпеки на основі методів машинного й глибокого навчання. У теоретичному аспекті дослідження сприяє розвитку існуючих підходів до побудови інтелектуальних систем моніторингу безпеки за рахунок інтеграції різнорідних джерел даних, урахування особливостей контейнеризованих середовищ і застосування адаптивних моделей аналізу поведінкових та мережевих характеристик.

Отримані наукові положення поглиблюють методологію використання методів штучного інтелекту для аналізу API-журналів, телеметрії Kubernetes-кластерів та поведінкових характеристик користувачів з метою своєчасного виявлення аномалій і кіберзагроз. Це створює передумови для подальших досліджень у напрямі розроблення адаптивних інтелектуальних систем моніторингу безпеки хмарної інфраструктури.

Практична значущість роботи полягає у можливості використання розроблених моделі і методів для вирішення прикладних задач виявлення аномалій у хмарних сервісах, аналізу подій інформаційної безпеки та моніторингу контейнеризованих середовищ. Запропоновані рішення можуть бути застосовані для автоматизації процесів аналізу API-трафіку, телеметрії Kubernetes-кластерів, виявлення поведінкових відхилень і своєчасного реагування на потенційні кіберзагрози в реальних умовах експлуатації хмарної інфраструктури.

Результати дослідження можуть бути інтегровані до систем моніторингу безпеки, платформ виявлення вторгнень, засобів аналізу журналів подій та інших інформаційно-аналітичних систем, що сприятиме підвищенню ефективності виявлення кіберзагроз, зниженню кількості хибних спрацювань і покращенню якості прийняття рішень у сфері кібербезпеки.

Крім того, окремі положення роботи можуть бути використані в освітньому процесі під час підготовки фахівців у галузі кібербезпеки, інформаційних технологій та штучного інтелекту, що сприятиме оновленню навчального матеріалу відповідно до сучасних наукових досягнень і практичних потреб у сфері захисту хмарних сервісів.

Зауваження.

Аналіз змісту та структури дисертаційної роботи, її теоретичних положень і практичних результатів свідчить про належний науковий рівень проведеного дослідження. Дисертація відповідає поставленій меті й завданням, матеріал викладено логічно та послідовно, а оформлення роботи відповідає встановленим вимогам. Разом із тим, у дисертації можна виокремити положення, що мають дискусійний характер, зокрема:

1. У роботі наведено результати експериментальної перевірки запропонованих методів, проте недостатньо висвітлено питання впливу налаштування гіперпараметрів моделі на якість виявлення аномалій. Більш детальний аналіз цього аспекту дозволив би оцінити чутливість запропонованих методів до зміни параметрів навчання.

2. У роботі наведено результати експериментів для підтвердження ефективності запропонованих методів, однак доцільно було б доповнити дослідження аналізом статистичної достовірності отриманих результатів, наприклад із використанням відповідних критеріїв перевірки статистичних гіпотез.

3. У дисертації достатньо детально розглянуто процес навчання моделі, проте питання періодичності її повторного навчання та підтримання актуальності в умовах зміни характеристик хмарного середовища висвітлено лише побіжно. Детальніший розгляд цього питання посилив би практичну цінність дослідження.

4. Під час опису експериментальних досліджень основну увагу приділено кінцевим результатам, однак більш детальне обґрунтування вибору окремих параметрів експериментального середовища сприяло б підвищенню відтворюваності проведених досліджень.

Проте наведені зауваження мають дискусійний характер, не є принциповими та не впливають на загальну позитивну оцінку дисертаційної роботи та окреслюють можливі напрями подальшого розвитку дослідження.

Загальна оцінка роботи.

Дисертаційна робота Свиридова Артема Сергійовича «Модель та методи інтелектуальної системи виявлення аномалій в хмарних сервісах» є завершеним та комплексним науковим дослідженням, присвяченим розв'язанню актуального науково-прикладного завдання – підвищенню ефективності виявлення аномалій у хмарних сервісах шляхом розроблення моделі та методів інтелектуальної системи виявлення аномалій у контейнеризованих і розподілених хмарних середовищах. У роботі виконано системний аналіз сучасного стану досліджень у сфері забезпечення безпеки хмарної інфраструктури, чітко сформульовано наукову проблему та забезпечено її послідовне вирішення.

Структура дисертації є логічною та узгодженою, а зміст розділів повністю відповідає поставленій меті та визначеним завданням дослідження. Робота вдало поєднує теоретичні розробки – зокрема створення функціонально-математичної моделі інтелектуальної системи та удосконалення методів аналізу API-журналів, поведінки користувачів і телеметрії Kubernetes – із їх практичною реалізацією та перевіркою за допомогою нейромережевого й імітаційного моделювання. Це забезпечує високу збалансованість між науковою новизною та прикладною спрямованістю отриманих результатів.

Виклад матеріалу здійснено на належному науковому рівні, із дотриманням вимог академічного стилю. Дисертація містить ґрунтовний аналіз літературних джерел, а також достатній обсяг експериментальних досліджень на реальних API-журналах та в Kubernetes-кластерах, що підтверджують достовірність і обґрунтованість отриманих результатів.

Отримані наукові положення, висновки та рекомендації характеризуються новизною, логічною завершеністю та практичною значущістю. Результати дослідження мають прикладну цінність для побудови адаптивних систем моніторингу безпеки хмарних сервісів, виявлення прихованих кіберзагроз і поведінкових відхилень у реальному часі, та вже впроваджені у практичну діяльність.

З урахуванням високого рівня наукової новизни, обґрунтованості та достовірності результатів, а також їх практичної цінності, дисертаційна робота

відповідає вимогам пунктів 6, 7, 8, 9 Порядку присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44.

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

Рецензент:

кандидат технічних наук, доцент,
декан факультету комп'ютерної інженерії та
інформаційних технологій Харківського
національного університету радіоелектроніки
кандидат технічних наук, доцент



Олексій ЛЯШЕНКО