УДК 004.9 DOI https://doi.org/10.35546/kntu2078-4481.2026.2.44

А. С. СВИРИДОВ
аспірант кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-9830-4103

І. В. ГУДЗИНСЬКИЙ
аспірант кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0009-0008-8409-7220

АРХІТЕКТУРА МУЛЬТИАГЕНТНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ІЗ ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

У статті розглядається проблема побудови ефективної системи виявлення вторгнень у хмарних та розподілених середовищах на основі мультиагентної архітектури з використанням методів машинного навчання. Актуальність дослідження зумовлена стрімким розвитком хмарних технологій, зростанням кількості та складності кіберзагроз, а також підвищеними вимогами до безперервності та безпеки функціонування розподілених інформаційних систем. Показано обмеженість традиційних сигнатурних підходів, які значною мірою залежать від своєчасного оновлення баз правил і демонструють недостатню ефективність при виявленні нових або модифікованих атак. Запропонований підхід поєднує сигнатурний механізм аналізу відомих загроз із поведінковим моделюванням на основі методів машинного навчання. Така інтеграція забезпечує можливість виявлення як відомих атак, так і невідомих інцидентів типу zero-day шляхом фіксації статистично значущих відхилень від сформованих базових профілів функціонування системи та користувачів у режимі реального часу. Особливістю роботи є формування двох взаємодоповнювальних моделей: профілю поведінки користувачів і профілю функціонування системи в цілому. Для їх побудови створено спеціалізований датасет нормальної роботи, що відображає типові сценарії експлуатації хмарної інфраструктури та характерні параметри навантаження. Це дозволяє враховувати специфіку конкретного середовища, підвищувати точність детекції, зменшувати кількість хибнопозитивних спрацювань і забезпечувати адаптивність системи до змін умов експлуатації. Архітектура рішення базується на мультиагентному підході з розподілом функцій між інтелектуальними агентами, які виконують збір даних, попередню обробку, аналітичну інтерпретацію подій, формування сповіщень та адаптивне оновлення бази знань. Реалізація багаторівневої структури забезпечує масштабованість, гнучкість конфігурації, відмовостійкість і можливість інтеграції з існуючими системами моніторингу хмарної інфраструктури. Отримані результати експериментальних досліджень підтверджують ефективність запропонованої моделі для підвищення рівня кібербезпеки хмарних сервісів і своєчасного виявлення кіберінцидентів.

Ключові слова: *мультиагентна система, виявлення вторгнень, машинне навчання, хмарні сервіси, поведінковий аналіз, базовий профіль, кібербезпека, zero-day атаки.*

A. S. SVYRYDOV
Postgraduate Student at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-9830-4103

I. V. HUDZYNSKYI
Postgraduate Student at the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0009-0008-8409-7220

ARCHITECTURE OF A MULTI-AGENT INTRUSION DETECTION SYSTEM BASED ON MACHINE LEARNING

The article addresses the problem of building an effective intrusion detection system in cloud and distributed environments based on a multi-agent architecture using machine learning methods. The relevance of the study is driven by the rapid development of cloud technologies, the growing number and complexity of cyber threats, and the increased requirements for the continuity and security of distributed information systems. The limitations of traditional signature-based approaches are demonstrated, as they largely depend on timely updates of rule databases and show insufficient

 ISSN 2078-4481

effectiveness in detecting new or modified attacks. The proposed approach combines a signature-based mechanism for analyzing known threats with behavioral modeling based on machine learning methods. This integration enables the detection of both known attacks and unknown zero-day incidents by identifying statistically significant deviations from the established baseline profiles of system and user behavior in real time. A distinctive feature of the work is the formation of two complementary models: the user behavior profile and the overall system functioning profile. To construct these models, a specialized dataset of normal system operation was created, reflecting typical cloud infrastructure usage scenarios and characteristic workload parameters. This approach makes it possible to account for the specifics of a particular environment, improve detection accuracy, reduce the number of false positives, and ensure system adaptability to changing operating conditions. The architecture of the solution is based on a multi-agent approach with functional distribution among intelligent agents that perform data collection, preprocessing, analytical interpretation of events, alert generation, and adaptive knowledge base updating. The implementation of a multi-level structure ensures scalability, configuration flexibility, fault tolerance, and the possibility of integration with existing cloud infrastructure monitoring systems. The obtained experimental results confirm the effectiveness of the proposed model in improving the cybersecurity level of cloud services and ensuring timely detection of cyber incidents.

Key words: *multi-agent system, intrusion detection, machine learning, cloud services, behavioral analysis, baseline profile, cybersecurity, zero-day attacks.*

Постановка проблеми

Стрімке зростання інтернет-охоплення та цифрових сервісів призводить до постійного збільшення обсягів даних і мережевого трафіку. За аналітикою DataReportal, у 2024 році кількість користувачів інтернету сягнула 5,35 млрд (приблизно 66,2% населення світу), що підкреслює масштаби та безперервність онлайн-активності [1]. Також звіти “Data Never Sleeps” демонструють, що лише за одну хвилину в мережі відбуваються сотні мільйонів дій (перегляди відео, повідомлення, транзакції тощо), тобто потік даних має практично безперервний характер [2]. У таких умовах зростає й “поверхня атаки”, а кіберзлочинність еволюціонує разом із цифровою інфраструктурою.

Паралельно з цифровою трансформацією ускладнюються й методи зловмисників. ENISA у своєму щорічному огляді загроз фіксує стабільну присутність критичних класів атак (зокрема загрози доступності, ransomware та атаки на дані) і підкреслює розвиток тактик та інструментів атакувальників [3]. Всесвітній економічний форум також наголошує на зростанні складності кіберландшафту, що посилюється геополітичними чинниками, ланцюгами постачання та швидким впровадженням нових технологій [4]. Практичні наслідки відображаються і в оцінках збитків: за даними щорічного звіту FBI IC3, заявлені втрати від інтернет-злочинів у 2024 році перевищили 16 млрд доларів США, що підкреслює фінансову вагу проблеми для організацій і користувачів [5].

У цьому контексті системи виявлення мережевих вторгнень (NIDS) залишаються одним із ключових інструментів захисту інфраструктури, адже дозволяють ідентифікувати підозрілу активність у трафіку та підтримувати реагування на інциденти. Водночас розвиток NIDS стримується низкою чинників: високою швидкістю та обсягом трафіку, потребою в обробці подій у (майже) реальному часі, швидкою зміною профілю легітимної активності та появою нових атак, а також проблемами якості даних для навчання моделей (зокрема дисбалансом класів і недостатньою “свіжістю” наборів даних) [6]. Окремим викликом залишається відсутність чітких і практично перевірених архітектур, які системно поєднують переваги сигнатурного та аномалійного підходів для виявлення як відомих, так і невідомих (zero-day) атак. Дослідження останніх років показують, що гібридні архітектури потенційно здатні підвищувати покриття атак і стійкість до нових сценаріїв, але їх реальна ефективність значною мірою залежить від даних, обчислювальних обмежень і коректної інтеграції компонентів у робочий контур моніторингу [7].

Аналіз останніх досліджень і публікацій

У сучасних наукових дослідженнях спостерігається зростаючий інтерес до проблеми виявлення мережевих атак та побудови ефективних систем Network Intrusion Detection Systems (NIDS). Значна кількість робіт останніх років присвячена застосуванню класичних алгоритмів машинного навчання, зокрема Random Forest, SVM, k-NN та градієнтного бустингу. Водночас дослідники відзначають, що традиційні підходи значною мірою залежать від ручного відбору ознак і мають обмежену здатність до узагальнення в умовах динамічного мережевого середовища. Крім того, використання застарілих наборів даних негативно впливає на достовірність експериментальних результатів. Це зумовило необхідність розроблення нових методологічних підходів, орієнтованих на сучасні типи атак і великі обсяги трафіку.

Останніми роками особлива увага приділяється застосуванню методів глибинного навчання для виявлення вторгнень. У роботі [8] здійснено систематичний аналіз сучасних DL-підходів до IDS та визначено ключові проблеми: дисбаланс класів, складність інтерпретації моделей, високу обчислювальну вартість і залежність від якості даних. Автори наголошують, що, незважаючи на високі показники точності, глибинні моделі часто демонструють зниження ефективності при перенесенні на інші середовища.

Важливим напрямом досліджень є створення сучасних репрезентативних наборів даних для IoT та IIoT-середовищ. У статті [9] представлено набір даних CICIoT2023, який містить реалістичні сценарії атак у середовищі Інтернету речей та орієнтований на тестування моделей у режимі реального часу. Автори демонструють,

що використання актуальних даних суттєво впливає на достовірність оцінювання моделей. Аналогічно, у роботі [10] запропоновано Edge-IIoTset – комплексний набір даних для централізованого та федеративного навчання, що враховує специфіку промислових IoT-систем. Недоліком більшості досліджень із використанням нових датасетів залишається обмежена перевірка моделей у різних мережевих топологіях і відсутність довготривалого тестування.

У дослідженні [11] запропоновано підхід до розв'язання проблеми дисбалансу класів за допомогою регуляризованих генеративних змагальних мереж (GAN). Запропонований метод дозволяє покращити виявлення рідкісних атак шляхом синтетичної генерації зразків шкідливого трафіку. Експериментальні результати демонструють підвищення повноти виявлення, однак метод характеризується значною складністю налаштування та підвищеними обчислювальними витратами.

У статті [12] розглянуто проблему концепт-дрейфу в потокових даних, що є критичною для систем реального часу. Автори аналізують адаптивні алгоритми класифікації, здатні автоматично перебудовувати модель при зміні статистичних характеристик трафіку. Попри позитивні результати, зазначається, що такі підходи можуть збільшувати час реакції системи та вимагати додаткових ресурсів.

Окремий напрям становлять гібридні архітектури, які поєднують сигнатурний та аномалійний підходи. У роботі [13] запропоновано гібридну модель IDS, що інтегрує оптимізовану SVM із метаевристичним алгоритмом оптимізації. Автори демонструють підвищення точності класифікації порівняно з традиційними методами. Проте запропонована модель має складну архітектуру та потребує ретельного налаштування параметрів, що ускладнює її практичне впровадження.

Отже, узагальнюючи результати останніх досліджень, можна зробити висновок, що сучасний розвиток NIDS орієнтований на застосування глибинного навчання, використання актуальних наборів даних та впровадження гібридних архітектур. Водночас залишаються невирішеними проблеми дисбалансу даних, концепт-дрейфу, високої обчислювальної складності та узагальнюваності моделей у реальних мережевих умовах, що визначає актуальність подальших досліджень у цьому напрямі.

Формулювання мети дослідження

Метою роботи є розробка мультиагентної моделі виявлення аномалій у хмарних сервісах, орієнтованої на забезпечення своєчасного виявлення кіберінцидентів у режимі, наближеному до реального часу. Запропонований підхід передбачає інтеграцію кількох інтелектуальних агентів, кожен з яких відповідає за аналіз окремих типів даних (мережевий трафік, журнали подій, поведінкові характеристики користувачів, системні метрики), з подальшою агрегацією результатів для підвищення точності та зниження рівня хибних спрацювань.

Викладення основного матеріалу дослідження

Стрімкий розвиток хмарних обчислень зумовив широке впровадження моделей IaaS, PaaS та SaaS у корпоративному та державному секторах. Хмарні сервіси забезпечують гнучкість, масштабованість і економічну ефективність, однак водночас створюють нові виклики у сфері інформаційної безпеки. Динамічний розподіл ресурсів, багатокористувацьке середовище, віртуалізація та висока інтенсивність мережевого трафіку ускладнюють своєчасне виявлення загроз і аномальної активності.

Традиційні системи виявлення вторгнень, побудовані на централізованих або сигнатурних підходах, часто демонструють обмежену ефективність у хмарних середовищах. Вони можуть не враховувати специфіку розподіленої інфраструктури, швидку зміну конфігурацій та появу нових, раніше невідомих типів атак. Крім того, централізована обробка великих обсягів телеметричних даних призводить до затримок у прийнятті рішень та зростання навантаження на обчислювальні ресурси.

У зв'язку з цим актуальності набувають підходи, що базуються на використанні інтелектуальних агентів, здатних автономно аналізувати дані, взаємодіяти між собою та адаптуватися до змін середовища. Мультиагентні системи дозволяють розподілити функції моніторингу між окремими компонентами, кожен з яких відповідає за аналіз певного типу даних – мережевого трафіку, журналів подій, поведінкових характеристик користувачів або системних показників. Така архітектура сприяє підвищенню масштабованості, гнучкості та відмовостійкості системи виявлення аномалій.

Запропонована у статті мультиагентна модель орієнтована на інтеграцію методів машинного та глибинного навчання для аналізу різнорідних потоків даних у хмарному середовищі. Передбачається, що кооперативна взаємодія агентів із використанням механізмів обміну знаннями дозволить підвищити точність виявлення аномалій, зменшити кількість хибних спрацювань та скоротити час реагування на інциденти.

Таким чином, дослідження спрямоване на розробку адаптивної, масштабованої та ефективної моделі виявлення аномалій у хмарних сервісах, що враховує сучасні вимоги до безпеки розподілених обчислювальних середовищ і здатна функціонувати в умовах постійної зміни мережевих характеристик та загроз.

На рис. 1 представлено модель запропонованої системи виявлення вторгнень, призначеної для забезпечення виявлення як відомих, так і невідомих атак (0-day) у будь-якому типі комп'ютерної мережі. Запропонована архітектура переважно базується на трьох рівнях, які взаємодіють між собою для виконання завдань із виявлення кібератак.

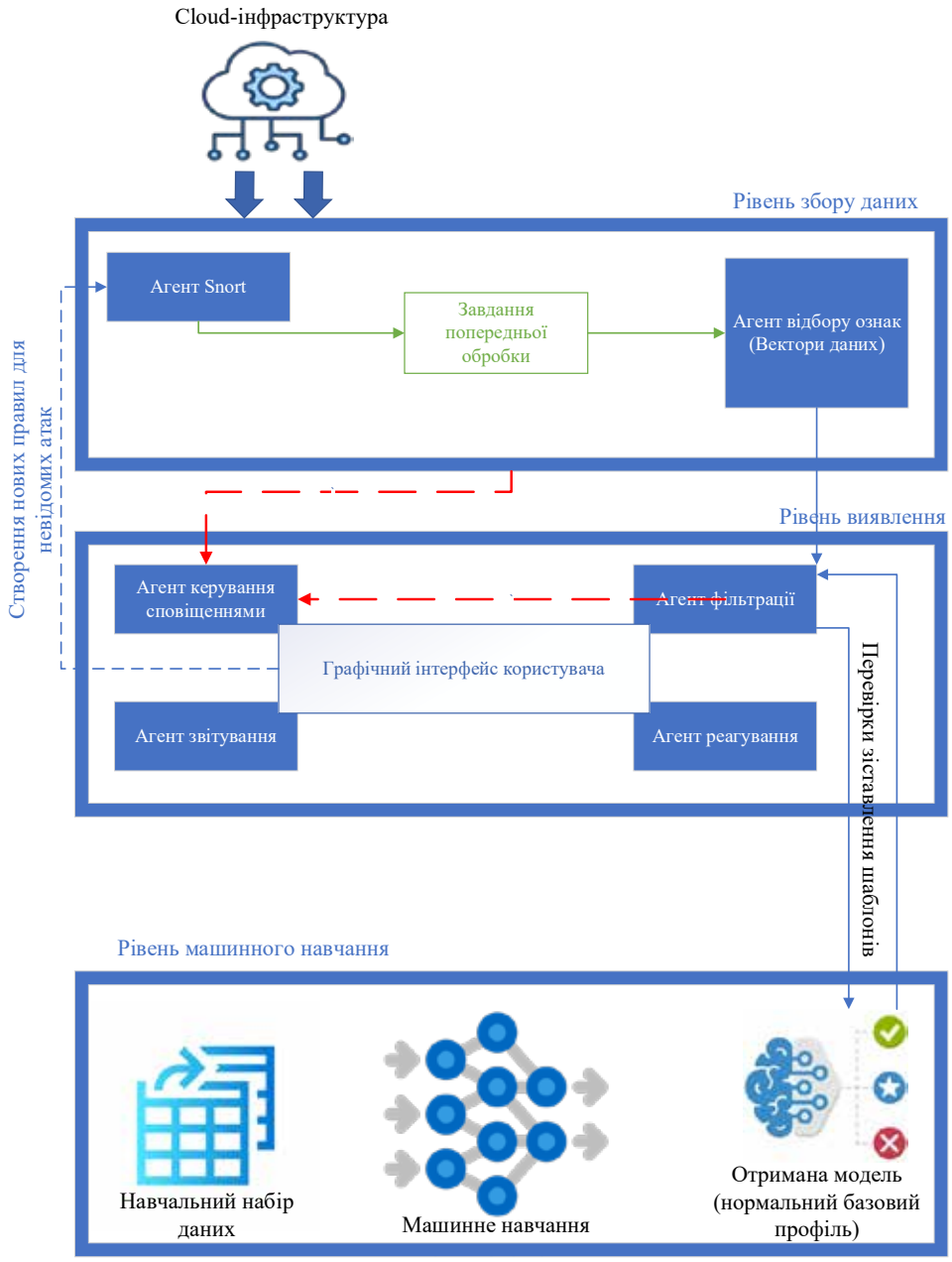

Рис. 1. Архітектура мультиагентної системи виявлення вторгнень із використанням машинного навчання

Запропонована система складається з трьох основних рівнів: рівня збору даних, рівня виявлення та рівня машинного навчання.

Рівень збору даних – цей рівень відповідає за отримання та попередню обробку мережевого трафіку в хмарній інфраструктурі. На даному етапі здійснюється захоплення мережевих пакетів, їх очищення, нормалізація та підготовка до подальшого аналізу. Також виконується відбір ознак для перетворення мережевого трафіку у вектори даних, які можуть бути використані алгоритмами машинного навчання. До складу рівня збору даних входять:

– агент Snort, що здійснює моніторинг трафіку та базову обробку пакетів;
– модуль завдань попередньої обробки, який виконує очищення та структуризацію даних;
– агент відбору ознак, що формує вектори даних для подальшого аналізу.

Рівень виявлення – цей рівень призначений для виявлення відхилень від нормального профілю мережевої активності. Його функціонування базується на моделі машинного навчання, сформованій на основі навчального набору даних, що містить нормальний (безпечний) мережевий трафік. У межах цього рівня реалізовано такі компоненти:

– агент фільтрації, який виконує перевірку відповідності поточного трафіку сформованому базовому профілю;

– агент керування сповіщеннями, що генерує повідомлення у разі виявлення аномалії або вторгнення;
– агент звітування, який формує аналітичні звіти для адміністратора безпеки;
– агент реагування, що ініціює відповідні дії у випадку інциденту;
– графічний інтерфейс користувача, через який адміністратор взаємодіє із системою.

У разі виявлення відхилень від нормального базового профілю система може ініціювати створення нових правил для невідомих атак та передавати інформацію для подальшого вдосконалення моделі.

Рівень машинного навчання – цей рівень забезпечує навчання системи на основі нормальної мережевої поведінки. Використовуючи методи керованого машинного навчання, система аналізує навчальний набір даних, що містить легітимний трафік, і формує модель нормального базового профілю. Отримана модель використовується на рівні виявлення для перевірки відповідності поточних мережевих подій сформованому профілю та для визначення аномалій. У разі необхідності модель може бути перенавчена з урахуванням нових даних, що забезпечує адаптивність системи в умовах змінного хмарного середовища.

Запропонована система повинна регулярно проходити навчання на основі даних, що відображають нормальну поведінку користувачів та штатне функціонування системи в цілому, без ознак будь-яких кібератак або зловмисної активності. Для цього було сформовано спеціальний датасет нормальної роботи системи, який включає журнали подій, інформацію про активність користувачів, системні метрики, характеристики доступу до ресурсів та інші параметри, що описують стандартні сценарії експлуатації.

Процес навчання запропонованої системи складається з шести основних етапів:

1. Збір даних. Система здійснює накопичення даних, що характеризують типову поведінку користувачів (час входу, частота запитів, доступ до сервісів, шаблони дій) та нормальну роботу інфраструктури. На основі цих даних формується датасет нормальної роботи, який відображає допустимі сценарії функціонування системи.

2. Попередня обробка. Для підготовки даних до використання алгоритмами машинного навчання виконуються процедури очищення та трансформації: видалення пропущених або аномальних значень, нормалізація та масштабування ознак, агрегація подій у часові інтервали, кодування категоріальних параметрів. Також здійснюється поділ датасету на навчальну та валідаційну вибірки.

3. Моделювання поведінки. На цьому етапі застосовуються алгоритми машинного навчання для формування двох типів базових моделей:
– профілю поведінки користувачів, що описує типові шаблони їх дій;
– профілю функціонування системи, який характеризує нормальні параметри роботи інфраструктури.

Проводиться порівняння кількох алгоритмів із метою вибору моделі, яка забезпечує найвищу точність та мінімальний рівень хибних спрацювань.

4. Тестування та валідація. Після навчання моделі оцінюються за відповідними метриками (точність, повнота, F-міра, рівень хибнопозитивних спрацювань, час реагування). Це дозволяє визначити найбільш ефективний алгоритм для формування базових профілів.

5. Формування базових профілів. На основі відібраного алгоритму створюються еталонні моделі, які описують нормальну поведінку користувачів і стабільну роботу системи. Ці профілі зберігаються як базові шаблони для подальшого моніторингу.

6. Використання базових моделей. Сформовані профілі застосовуються у процесі експлуатації системи для виявлення відхилень від встановлених норм. У разі фіксації аномальної активності (нетипових дій користувача або нестандартних системних параметрів) система генерує попередження та ініціює механізми реагування. Такий підхід дозволяє ефективно виявляти як внутрішні порушення політик доступу, так і невідомі атаки (0-day), що проявляються через зміну поведінкових характеристик.

Принцип виявлення у запропонованій моделі NIDS ґрунтується на попередньому навчанні системи на даних, що відображають нормальну поведінку користувачів і штатне функціонування системи без ознак кібератак. Сформована в результаті навчання модель розглядається як базовий профіль (baseline), з яким система порівнює поточні події та активність у режимі реального часу.

Виявлення вторгнень здійснюється за такими етапами:

Крок 1 – Моніторинг і збір даних. На цьому етапі система здійснює безперервний моніторинг подій, що відбуваються в хмарному середовищі: дії користувачів, звернення до сервісів, зміни конфігурацій, системні журнали та мережеві запити. Для фіксації подій використовується відповідний агент збору даних, який акумулює інформацію про поточну активність.

Крок 2 – Перевірка за сигнатурами. Отримані події перевіряються на відповідність відомим шаблонам атак, що містяться в базі правил (базі знань сигнатур). Якщо подія відповідає відомій сигнатурі загрози, система негайно генерує сповіщення адміністратора безпеки про виявлену атаку.

Крок 3 – Попередня обробка даних. Якщо подія не розпізнана як відома загроза, вона передається на етап попередньої обробки. Виконуються операції очищення, нормалізації, агрегування та відбору ознак. Дані перетворюються у вектори ознак, придатні для аналізу алгоритмами машинного навчання.

Крок 4 – Порівняння з базовими профілями. Після перетворення подій у формат векторів ознак агент фільтрації перевіряє їх відповідність раніше сформованим базовим профілям поведінки користувачів і функціонування системи. Можливі два варіанти:

– якщо подія відповідає встановленому профілю нормальної роботи, система не генерує попередження;

– якщо зафіксовано відхилення від базових моделей, формується сповіщення для адміністратора безпеки з метою подальшого аналізу.

Крок 5 – Актуалізація бази знань. У разі виявлення відхилення адміністратор проводить діагностику та аналіз підозрілої події. За необхідності він може оновити базу правил або створити нові сигнатури для запобігання подібним інцидентам у майбутньому. Виявлені події можуть відповідати атакам типу zero-day, для яких ще не існує офіційних оновлень або сигнатур. Таким чином, система забезпечує не лише виявлення аномалій, а й поступове вдосконалення механізмів захисту шляхом збагачення бази знань.

Запропонований підхід поєднує сигнатурний аналіз і поведінкове моделювання, що дозволяє забезпечити виявлення як відомих загроз, так і нових або невідомих атак, які проявляються через відхилення від сформованих базових профілів.

Ключовою особливістю моделі є попереднє формування профілів нормальної роботи користувачів та системи в цілому на основі спеціально створеного датасету штатного функціонування. Це забезпечує адаптивність системи до специфіки конкретного хмарного середовища та зменшує кількість хибних спрацювань. Реалізація багаторівневої архітектури з розподілом функцій між агентами підвищує масштабованість, гнучкість і стійкість системи до змін навантаження.

Таким чином, запропонована модель створює основу для побудови інтелектуальної, самонавчальної системи захисту хмарної інфраструктури, здатної своєчасно реагувати на кіберінциденти та поступово вдосконалювати власні механізми виявлення загроз.

Висновки

У статті розроблено та обґрунтовано мультиагентну модель виявлення аномалій у хмарних сервісах, орієнтовану на забезпечення своєчасного виявлення кіберінцидентів у динамічному розподіленому середовищі. Запропонований підхід поєднує сигнатурний механізм аналізу відомих загроз із поведінковим моделюванням на основі машинного навчання, що дозволяє виявляти як відомі атаки, так і невідомі (zero-day) інциденти через фіксацію відхилень від базових профілів.

Особливістю роботи є формування двох взаємодоповнювальних базових моделей: профілю поведінки користувачів та профілю функціонування системи в цілому. Для цього було створено датасет нормальної роботи системи, що відображає типові сценарії експлуатації хмарної інфраструктури. Такий підхід дозволяє враховувати специфіку конкретного середовища, підвищувати точність виявлення та зменшувати кількість хибнопозитивних спрацювань.

Запропонована архітектура базується на розподілі функцій між інтелектуальними агентами, які виконують збір даних, попередню обробку, аналіз, формування сповіщень і адаптивне оновлення бази знань. Реалізація багаторівневої структури забезпечує масштабованість, гнучкість і можливість інтеграції з існуючими системами моніторингу хмарної інфраструктури.

Список використаної літератури

1. Digital 2024 deep-dive: The state of internet adoption. DataReportal, 2024. URL: https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption (дата звернення: 20.02.2026).

2. Data never sleeps 12.0. Domo, 2024. URL: https://www.domo.com/data-never-sleeps (дата звернення: 20.02.2026).

3. ENISA threat landscape 2024. European Union Agency for Cybersecurity (ENISA), 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 20.02.2026).

4. 2024 Internet crime report / Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). 2025. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf (дата звернення: 20.02.2026).

5. Luo Y. et al. Current status, challenges, and future trends of deep learning-based intrusion detection models. Journal of Imaging. 2024. Vol. 10, № 10. P. 254. DOI: https://doi.org/10.3390/jimaging10100254.

6. Global cybersecurity outlook 2025. World Economic Forum, 2025. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025 (дата звернення: 20.02.2026).

7. Yang L., Moubayed A., Shami A. MTH-IDS: A multi-tiered hybrid intrusion detection system for internet of vehicles. arXiv. 2021. URL: https://arxiv.org/abs/2105.13289 (дата звернення: 20.02.2026).

8. Luo Y. et al. Deep Learning for Network Intrusion Detection: A Review of Recent Developments and Future Directions. IEEE Access. 2023. Vol. 11. P. 10234–10255. DOI: https://doi.org/10.1109/ACCESS.2023.3241254.

9. Pinto Neto E. C. et al. CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. Sensors. 2023. Vol. 23, № 13. Art. 5941. DOI: https://doi.org/10.3390/s23135941.

10. Ferrag M. A. et al. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. IEEE Access. 2022. Vol. 10. P. 40281–40306. DOI: https://doi.org/10.1109/ACCESS.2022.3165809.

11. Chapaneri R., Shah S. Enhanced Detection of Imbalanced Malicious Network Traffic with Regularized Generative Adversarial Networks. Journal of Network and Computer Applications. 2022. Art. 103368. DOI: https://doi.org/10.1016/j.jnca.2022.103368.

12. Khanna S. Concept Drift-Based Intrusion Detection for Evolving Data Stream Classification in IDS: Approaches and Comparative Study. The Computer Journal. 2024. Vol. 67, № 7. P. 2529–2547. DOI: https://doi.org/10.1093/comjnl/bxae023.

13. Elsedimy E. I., Elhadidy H., Abohashish S. M. M. A Novel Intrusion Detection System Based on a Hybrid Quantum Support Vector Machine and Improved Grey Wolf Optimizer. Cluster Computing. 2024. DOI: https://doi.org/10.1007/s10586-024-04458-8.

References

1. DataReportal (2024) *Digital 2024 deep-dive: The state of internet adoption*. Retrieved from: https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption (accessed 20 February 2026).

2. Domo (2024) *Data never sleeps 12.0*. Retrieved from: https://www.domo.com/data-never-sleeps (accessed 20 February 2026).

3. European Union Agency for Cybersecurity (ENISA) (2024) *ENISA threat landscape 2024*. Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (accessed 20 February 2026).

4. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3) (2025) *2024 Internet crime report*. Retrieved from: https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf (accessed 20 February 2026).

5. Luo Y., et al. (2024) Current status, challenges, and future trends of deep learning-based intrusion detection models. *Journal of Imaging*, vol. 10, no. 10, p. 254. doi: 10.3390/jimaging10100254

6. World Economic Forum (2025) *Global cybersecurity outlook 2025*. Retrieved from: https://www.weforum.org/publications/global-cybersecurity-outlook-2025 (accessed 20 February 2026).

7. Yang L., Moubayed A., Shami A. (2021) MTH-IDS: *A multi-tiered hybrid intrusion detection system for internet of vehicles*. arXiv. Working paper 2105.13289. Retrieved from: https://arxiv.org/abs/2105.13289 (accessed 20 February 2026).

8. Luo Y., et al. (2023) Deep Learning for Network Intrusion Detection: A Review of Recent Developments and Future Directions. *IEEE Access*, vol. 11, pp. 10234–10255. doi: 10.1109/ACCESS.2023.3241254

9. Pinto Neto E. C., et al. (2023) CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. *Sensors*, vol. 23, no. 13, art. 5941. doi: 10.3390/s23135941

10. Ferrag M. A., et al. (2022) Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access*, vol. 10, pp. 40281–40306. doi: 10.1109/ACCESS.2022.3165809

11. Chapaneri R., Shah S. (2022) Enhanced Detection of Imbalanced Malicious Network Traffic with Regularized Generative Adversarial Networks. *Journal of Network and Computer Applications*, art. 103368. doi: 10.1016/j.jnca.2022.103368

12. Khanna S. (2024) Concept Drift-Based Intrusion Detection for Evolving Data Stream Classification in IDS: Approaches and Comparative Study. *The Computer Journal*, vol. 67, no. 7, pp. 2529–2547. doi: 10.1093/comjnl/bxae023

13. Elsedimy E. I., Elhadidy H., Abohashish S. M. M. (2024) A Novel Intrusion Detection System Based on a Hybrid Quantum Support Vector Machine and Improved Grey Wolf Optimizer. *Cluster Computing*. doi: 10.1007/s10586-024-04458-8

Дата першого надходження статті до видання: 23.02.2026
Дата прийняття статті до друку після рецензування: 27.03.2026
Дата публікації (оприлюднення) статті: 07.05.2026