УДК 004.056.5:004.89

Н.П. Юрчук,
К. Д. Кириченко

АРХІТЕКТУРНО-ФУНКЦІОНАЛЬНА ОРГАНІЗАЦІЯ АДАПТИВНИХ СИСТЕМ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ НА ОСНОВІ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Вінницький національний технічний університет

Анотація

Обґрунтовано архітектурно-функціональну структуру адаптивних систем виявлення вторгнень (IDS), що базуються на ієрархічній взаємодії сенсорно-колекторних, діагностичних, когнітивних та оркестраційних доменів. Окрему увагу приділено формалізації циклу адаптивної безпеки на засадах continual learning, що забезпечує безперервне самонавчання системи без зупинки процесів моніторингу. Запропоновано механізми реалізації концепції «активної оборони» для проактивного блокування кіберзагроз та наведено математичний апарат оцінювання ефективності інтелектуальних модулів.

Ключові слова: штучний інтелект, кібербезпека, архітектура IDS, інтелектуальна рекурсія, активна оборона, виявлення аномалій, адаптивні системи безпеки.

ARCHITECTURAL AND FUNCTIONAL ORGANIZATION OF ADAPTIVE CYBER THREAT DETECTION SYSTEMS BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Abstract

The article substantiates the architectural and functional model of adaptive Intrusion Detection Systems (IDS) based on the hierarchical interaction of sensor-collector, diagnostic, cognitive, and orchestration domains. The proposed architecture integrates intelligent data processing modules that enable automated detection and classification of cyber threats in real time. Particular attention is given to the formalization of an adaptive security cycle based on the principles of continual learning, which ensures continuous model updating without interrupting monitoring processes. In addition, mechanisms for implementing the Active Defense concept aimed at proactive mitigation of cyber threats are described. The effectiveness of the proposed intelligent modules is evaluated using a mathematical framework.

Keywords: artificial intelligence, cybersecurity, IDS architecture, intelligent recursion, active defense, anomaly detection, adaptive security systems.

Вступ

Стрімка цифровізація економіки та державних інституцій зумовила зростання кількості та складності кібератак, що створює суттєві ризики для інформаційної безпеки організацій та критичної інфраструктури. Традиційні методи захисту, засновані на сигнатурному аналізі, стають недостатньо ефективними проти атак нульового дня (Zero-day) та складних цілеспрямованих загроз (APT) [1]. У зв'язку з цим виникає необхідність впровадження інтелектуальних систем, здатних до автономного виявлення аномалій та адаптації до нових типів втручань. Технології штучного інтелекту (ШІ), зокрема машинного навчання (ML) та глибокого навчання (DL), демонструють високий потенціал у розпізнаванні прихованих закономірностей у великих масивах мережевого трафіку.

Метою роботи є обґрунтування архітектурно-функціональної структури адаптивних систем виявлення вторгнень (IDS) та формалізація механізмів їх функціонування на засадах безперервного адаптивного навчання для забезпечення проактивного захисту інформаційної інфраструктури в умовах динамічного ландшафту кіберзагроз.

Результати дослідження

Інтелектуальні системи виявлення кіберзагроз (Intrusion Detection Systems, IDS), що базуються на методах штучного інтелекту, являють собою складні адаптивні інформаційно-аналітичні комплекси, здатні розширити функціональні можливості традиційних систем кіберзахисту. На відміну від класичних сигнатурних систем, що функціонують переважно у реактивному режимі та орієнтуються на виявлення вже відомих шаблонів атак, системи IDS на основі ШІ забезпечують перехід до проактивної моделі захисту. Така модель передбачає не лише оперативне виявлення інцидентів

інформаційної безпеки, але й прогнозування потенційних загроз, аналіз поведінкових патернів мережевої активності і превентивне блокування шкідливих дій ще на етапі їх формування.

Теоретико-методологічний базис дослідження ґрунтується на формалізації циклу адаптивної безпеки, що передбачає встановлення безперервного зворотного зв'язку між виконавчими компонентами та інтелектуальним аналітичним ядром системи. Такий механізм забезпечує динамічну самоадаптацію архітектури у процесі експлуатації: алгоритми машинного навчання здійснюють автоматичну корекцію прогнозних моделей, спираючись на актуальні масиви даних про кіберінциденти та нетипові зміни в параметрах мережевого середовища.

Визначальною функціональною перевагою даної моделі є реалізація процесів донавчання без інкрементального призупинення моніторингу, що гарантує безперервність контролю інформаційних потоків та нівелює ризики пропуску критичних подій безпеки, що є особливо актуальним для гетерогенних систем із високою інтенсивністю трафіку.

Архітектура інтелектуальної системи виявлення загроз ґрунтується на ієрархічній взаємодії чотирьох основних функціональних доменів (табл. 1), що забезпечують повний цикл обробки інформації – від первинного збору телеметрії до автоматизованого реагування на інциденти. Така структурна декомпозиція дозволяє розділити функціональні ролі компонентів системи та підвищити її масштабованість, гнучкість і здатність до інтеграції з іншими елементами інфраструктури кіберзахисту.

Таблиця 1 – Функціональна декомпозиція модулів ШІ-системи виявлення загроз

Типи модулів	Основні функції	Технологічний стек
Сенсорно-колекторні	Високошвидкісний збір телеметричних даних із мережевих вузлів, серверів та прикладних систем; нормалізація логів, агрегування мережевих пакетів і формування структурованих потоків даних для подальшого аналізу.	SIEM platforms, розширені eBPF-based probes
Діагностичні (аналіз аномалій)	Ідентифікація відхилень у поведінкових моделях користувачів, пристроїв та сервісів; аналіз статистичних і часових закономірностей мережевого трафіку в межах концепції UEBA.	Методи машинного навчання без учителя: Isolation Forest, One-class SVM
Когнітивні (класифікатори)	Категоризація інцидентів інформаційної безпеки, визначення типу атаки та рівня критичності загрози на основі аналізу багатовимірних даних.	Глибоке навчання: CNN для аналізу мережевого трафіку, LSTM для часових рядів
Оркестраційні (Response)	Автоматизоване реагування на інциденти, модифікація конфігурацій мережі, блокування підозрілих вузлів та ізоляція скомпрометованих компонентів інфраструктури.	SOAR-платформи, адаптивні правила SDN, playbooks, automated incident response

Джерело: систематизовано та узагальнено авторами за [2; 3]

На відміну від традиційних систем виявлення вторгнень, де обробка інформації відбувається переважно у лінійній послідовності модулів, у запропонованій архітектурі реалізовано механізм continual learning, що забезпечує періодичне оновлення моделей на основі нових даних. Тобто, результати роботи аналітичних модулів можуть повторно використовуватися для корекції параметрів попередніх етапів обробки даних. Зокрема, модулі виявлення аномалій здатні ідентифікувати приховані взаємозв'язки між окремими подіями безпеки, які на перший погляд не мають очевидного логічного зв'язку. Наприклад, одночасна поява таких факторів, як незначне зростання вихідного мережевого трафіку, нестандартний час входу адміністратора до системи та збільшення кількості запитів до бази даних, може сигналізувати про підготовчі етапи складних APT-атак (Advanced Persistent Threat).

Для оцінювання ефективності роботи когнітивного модуля системи та мінімізації помилок другого роду (тобто пропуску реальних атак) доцільно використовувати комплекс статистичних метрик, зокрема інтегральний показник точності (Accuracy) та збалансовану метрику *F*1-*score*, що враховує співвідношення між точністю і повнотою виявлення загроз:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}, \quad (1)$$

де, *Precision* (точність) характеризує частку правильно ідентифікованих інцидентів серед усіх спрацьовувань системи та дозволяє мінімізувати кількість хибнопозитивних спрацювань (False Positives), що особливо важливо для запобігання блокуванню легітимних бізнес-процесів організації;

Recall (повнота) відображає здатність системи виявляти максимальну кількість реальних загроз, що є критичним для ефективного протистояння складним та прихованим кіберінцидентам.

Практична реалізація описаної архітектури створює передумови для впровадження концепції Active Defense (активної оборони) у корпоративних інформаційних системах. У межах цієї концепції система кіберзахисту не обмежується пасивним спостереженням за мережевим середовищем, а активно формує динамічні профілі безпеки, які адаптуються до поточних умов функціонування інформаційної інфраструктури. Наприклад, у разі виявлення ознак підготовки до DDoS-атаки (зокрема, підвищеної інтенсивності розвідувальних запитів або сканування портів) виконавчі модулі системи можуть превентивно обмежити швидкість встановлення з'єднань для підозрілих сегментів мережі або тимчасово змінити правила маршрутизації трафіку. Такий підхід дозволяє локалізувати потенційну загрозу ще до моменту її переходу у фазу активної атаки.

У результаті впровадження інтелектуальних систем виявлення кіберзагроз значно скорочується середній час виявлення інциденту (Mean Time to Detect, MTTD) та середній час реагування (Mean Time to Respond, MTTR). Зменшення цих показників є критично важливим для сучасних організацій, оскільки швидкість реагування на кіберінциденти безпосередньо впливає на рівень збереження інформаційних активів, фінансових ресурсів та репутаційного капіталу підприємства. В умовах стрімкого розвитку кіберзагроз і загальної цифровізації економіки використання адаптивних ШІ-орієнтованих систем кіберзахисту стає ключовим елементом формування стійкої та безпечної інформаційної інфраструктури.

Висновки

Проведене дослідження підтверджує, що впровадження штучного інтелекту є критичним етапом еволюції систем кіберзахисту, що забезпечує перехід від реактивного до проактивного управління інцидентами. Запропонована архітектура, заснована на функціональній декомпозиції та використання механізму безперервного донавчання моделей (continual learning) підвищує точність виявлення атак, дозволяє суттєво мінімізувати час перебування зловмисника в мережі за рахунок безперервного аналізу поведінкових аномалій. Використання математичного апарату оцінки, зокрема *F*1-*score*, гарантує високу точність класифікації загроз при одночасному зниженні рівня хибнопозитивних спрацювань. Таким чином, інтеграція когнітивних модулів у контур інформаційної безпеки формує адаптивний механізм «активної оборони», здатний автономно протидіяти складним цілеспрямованим атакам і забезпечувати безперервність бізнесу в динамічному цифровому середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Лисецький Ю. М. Штучний інтелект у кібербезпеці. *Military strategy and technology*. 2025. № 3(3). С. 94–99. DOI: https://doi.org/10.63978/3083-6476.2025.3.3.08.
2. Wang Y.-C., Houng Y.-C., Chen H.-X., Tseng S.-M. Network Anomaly Intrusion Detection Based on Deep Learning Approach. *Sensors*. 2023. Vol. 23, no. 4. Art. 2171. DOI: https://doi.org/10.3390/s23042171.
3. Zhang Y., Muniyandi R., Qamar F. A Review of Deep Learning Applications in Intrusion Detection Systems. *Applied Sciences*. 2025. Vol. 15, no. 3. Art. 1552. DOI: https://doi.org/10.3390/app15031552.

Юрчук Наталія Петрівна – канд. екон. наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: urnata@vntu.edu.ua

Кириченко Катерина Дмитрівна – студентка групи 1ІСТ-24б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця

Yurchuk Nataliia P. – PhD in Economics, Associate Professor, Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: urnata@vntu.edu.ua

Kyrychenko Kateryna D. – Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia