УДК 004.5 + 004.89

Д.П. Урлапова

АРХІТЕКТУРА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ПОВЕДІНКОВОГО ТА СЕМАНТИЧНОГО АНАЛІЗУ ДІЙ КОРИСТУВАЧІВ ДЛЯ ЗАХИСТУ ВЕБПЛАТФОРМ

Вінницький національний технічний університет

Анотація

У роботі запропоновано архітектурну модель інтелектуальної системи виявлення аномальної активності користувачів вебплатформ, що поєднує поведінковий аналіз із семантичною оцінкою змін контенту. [1] Актуальність дослідження зумовлена зростанням кількості інцидентів, пов'язаних із несанкціонованим редагуванням матеріалів, зловживанням правами доступу та використанням скомпрометованих облікових записів. [2]

Ключові слова: *штучний інтелект; поведінковий аналіз; аномалії; кібербезпека; вебплатформи; журналювання подій; семантичний аналіз; автоматичне реагування; інформаційна безпека.*

Abstract

This paper proposes an architectural model of an intelligent system for detecting anomalous activity of web platform users that combines behavioral analysis with semantic evaluation of content changes. [1] The relevance of the study is due to the growing number of incidents involving unauthorized editing of materials, abuse of access rights, and the use of compromised accounts. [2]

Keywords: *artificial intelligence; behavioral analysis; anomalies; cybersecurity; web platforms; event logging; semantic analysis; automatic response; information security.*

Вступ

Сучасні вебплатформи, зокрема освітні та корпоративні ресурси, функціонують в умовах постійного зростання кіберзагроз [2]. Навіть за наявності систем автентифікації та розмежування прав доступу ризик несанкціонованих змін контенту залишається актуальним [3]. Особливо небезпечними є ситуації, коли зловмисник використовує скомпрометований обліковий запис або здійснює дії, що формально відповідають правам користувача, але відхиляються від його типової поведінки; такі аномалії можуть бути виявлені за допомогою аналізу поведінки користувачів [1].

Запропонована модель орієнтована на вебплатформи з клієнт-серверною архітектурою типу frontend–backend, де frontend реалізується у вигляді вебінтерфейсу (SPA або класичний клієнт), а backend – у вигляді серверного застосунку (REST API, CMS, Node.js, PHP), який обробляє запити користувачів та приймає системні рішення.

У більшості типових вебсистем журналювання подій або відсутнє, або використовується лише для технічного аудиту без подальшого інтелектуального аналізу та автоматичного прийняття рішень backend.Традиційні підходи до забезпечення безпеки вебсистем здебільшого орієнтовані на пошук відомих вразливостей або обмеження доступу до окремих функцій [2]. Проте такі методи не враховують контексту змін та індивідуальних поведінкових характеристик користувачів [3]. У зв'язку з цим актуальним є розроблення інтелектуальної системи, здатної здійснювати комплексний аналіз усіх дій користувачів, що впливають на структуру, зміст або налаштування вебресурсу (вхід у систему, редагування контенту, завантаження файлів, зміна ролей, масові операції), у режимі реального часу [4].

Метою роботи є розроблення архітектурної моделі системи, що поєднує поведінковий аналіз та семантичну оцінку змін для автоматичного виявлення аномальної активності та формування рішень backend.

Результати дослідження

У ході дослідження запропоновано архітектуру інтелектуальної системи моніторингу та аналізу дій користувачів, що інтегрується з вебплатформою через програмний інтерфейс (API) та функціонує як окремий модуль безпеки [4].

На рисунку 1 подано архітектуру інтелектуальної системи поведінкового та семантичного аналізу дій користувачів.

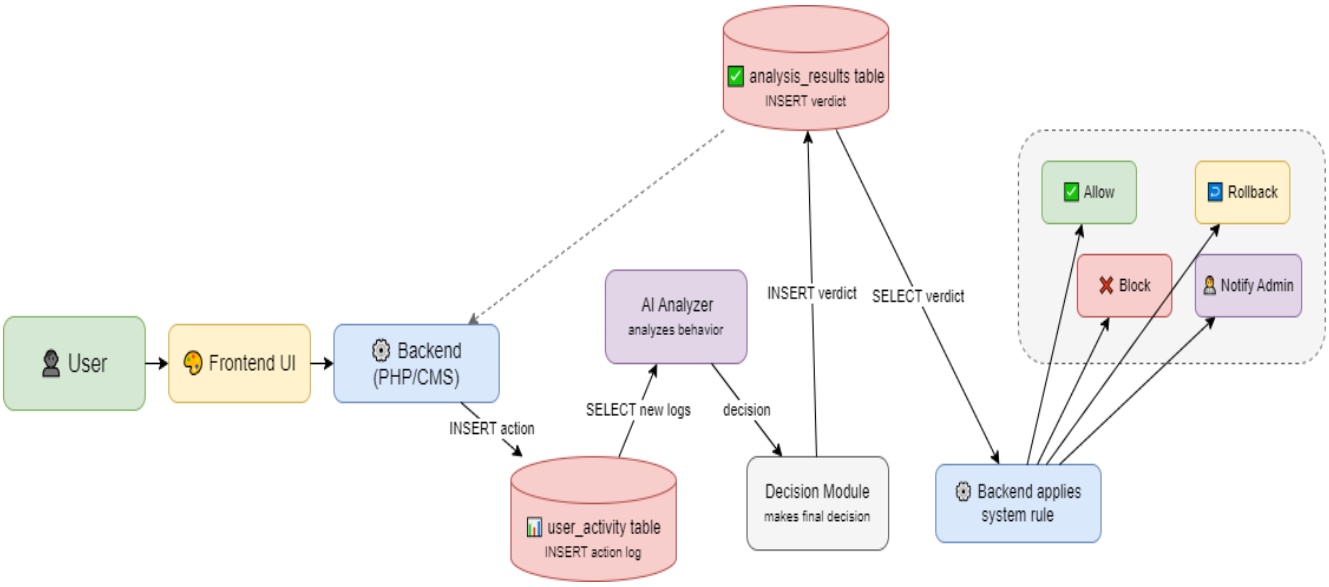

Рис. 1 – Архітектура інтелектуальної системи поведінкового та семантичного аналізу дій користувачів.

Основою запропонованої моделі є механізм журналювання подій, відповідно до якого кожна дія користувача (вхід у систему, редагування або створення контенту, додавання коментарів, завантаження файлів, зміна ролей тощо) автоматично фіксується у таблиці активності. Після реєстрації подія передається до модуля інтелектуального аналізу.

Модуль аналізу здійснює оцінювання події за двома основними напрямами:

1. поведінкові характеристики (частота дій, нетиповий час активності, відхилення від звичного сценарію користувача, аномальна послідовність операцій) [1];
2. семантичні характеристики зміненого контенту, що визначаються за допомогою моделей машинного навчання (відповідність тематиці ресурсу, збереження змістового профілю сайту, відсутність різкої тематичної зміни, виявлення підозрілих фрагментів коду, нецензурної або спам-лексики) [4].

Семантичний аналіз реалізується за допомогою NLP-моделі, яка визначає ступінь тематичної подібності нового контенту до профілю вебресурсу. Зокрема, якщо система виявляє, що змінений матеріал не відповідає загальній тематиці ресурсу (наприклад, освітній текст замінено на нерелевантний рекламний або сторонній контент), така подія класифікується як аномальна незалежно від формальної коректності тексту.

Для формалізації прийняття рішення введено набір параметрів моніторингу. У таблиці 1 наведено основні параметри аналізу подій користувачів, типи їх обробки та критерії формування реакції системи. Деякі параметри мають бути критичними тригерами, які у разі спрацювання одразу запускають реакцію системи (наприклад, виявлення ін’єкцій або різка зміна тематики контенту). Інші параметри використовуються для формування інтегрального ризик-показника, що обчислюється на основі агрегованої оцінки параметрів з урахуванням їх вагової значущості.

№	Параметр моніторингу	Тип аналізу	Критерій	Тип реакції

1	Частота подій	поведінковий	перевищення порогу	формує ризик
2	Нетиповий час активності	поведінковий	відхилення від профілю	формує ризик
3	Семантична невідповідність тематиці	MI-аналіз	низька тематична подібність	критичний тригер
4	Виявлення ін'єкцій/скриптів	rule-based	SQL або script патерни	критичний тригер
5	Токсичність або спам	MI-аналіз	перевищення порогу моделі	формує ризик

Таблиця 1 – Параметри моніторингу подій користувачів

Особливістю запропонованої моделі є відокремлення модуля інтелектуального аналізу від основної логіки вебсайту, що забезпечує універсальність рішення та можливість його інтеграції з різними платформами незалежно від їх внутрішньої структури [5]. Параметри моніторингу, наведені у таблиці 1, використовуються модулем інтелектуального аналізу для оцінювання подій користувачів та формування відповідної реакції системи. Такий підхід дозволяє реалізувати централізований моніторинг подій та масштабувати систему для одночасного захисту кількох вебресурсів.

Отримані результати підтверджують доцільність поєднання поведінкового аналізу з оцінкою змісту змін як ефективного інструмента раннього виявлення аномальної активності та підвищення рівня інформаційної безпеки вебплатформ [6].

Висновок

У роботі запропоновано архітектурну модель інтелектуальної системи моніторингу дій користувачів вебплатформ, що поєднує поведінковий та семантичний аналіз змін контенту. Система передбачає журналювання подій, оцінку ризику кожної дії та автоматичне формування рішення щодо її дозволу, обмеження або блокування.

Особливістю запропонованого підходу є відокремлення модуля інтелектуального аналізу від основної логіки вебсайту та інтеграція через API, що забезпечує універсальність і можливість масштабування рішення. Запропонована модель може бути використана як додатковий рівень захисту для підвищення цілісності та безпеки вебресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Predictive modeling and anomaly detection in large-scale web portals through the CAWAL framework*, Ozkan Canay, Umit Kocabicak, 2025. URL: https://arxiv.org/abs/2502.00413
2. *A survey of streaming data anomaly detection in network security*, P. Zhou. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12453818/
3. *Multi-Granularity User Anomalous Behavior Detection*, W. Feng et al., 2024. URL: https://www.mdpi.com/2076-3417/15/1/128
4. *Cybersecurity threat detection based on a UEBA framework using Deep Autoencoders*, Jose Fuentes et al., 2025. URL: https://arxiv.org/abs/2505.11542
5. *User and entity behavior analytics for enterprise security*, Madhu Shashanka et al., 2016. URL: https://www.researchgate.net/publication/313456188_User_and_entity_behavior_analytics_for_enterprise_security
6. *A New Generation of Perspective API: Efficient Multilingual Character-level Transformer Models for Toxicity Detection*, Lees A., Borkan D., et al., 2022. URL: https://arxiv.org/abs/2202.11176

Урлапова Дар'я Павлівна – студентка групи 1ІСТ-23б, факультет автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, Вінниця, e-mail: dashaurlapova@gmail.com

Науковий керівник: **Паламарчук Євген Анатолійович** — кандидат технічних наук, професор кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, Вінниця,

Urlapova Daria P. – student of the Faculty for Intelligent information technologies and automation, Vinnytsia National Technical University, Vinnytsia, e-mail: dashaurlapova@gmail.com

Scientific advisor: **Palamarchuk Yevhen Anatoliyovych** — Candidate of Technical Sciences, Professor of the Department of Automation and Intelligent Information Technologies, Vinnytsia National Technical University, Vinnytsia,