УДК 004.056.5:004.891

# ОЦІНЮВАННЯ ЗАСТОСОВНОСТІ МЕТОДІВ ВИЯВЛЕННЯ ПОВЕДІНКОВИХ АНОМАЛІЙ У КОРПОРАТИВНИХ ВЕБСИСТЕМАХ

Новожилов О.Д.[1]; Гайда А.Ю., к.т.н., доц.[2]
[1,2] Національний університет кораблебудування ім. адмірала Макарова
[1,2] Україна, Миколаїв
[1] veewile@gmail.com; [2] cetus@ukr.net

***Анотація.*** *Досліджено умови застосування порогових правил, робастної статистики Median/MAD та алгоритму Isolation Forest для виявлення аномалій у діях користувачів корпоративних вебсистем. Порівняно якість виявлення аномалій на контрольованих наборах подій в умовах «холодного старту», неповноти спостережень, імпорту поведінкового профілю. Обґрунтовано необхідність поєднання декількох методів для визначення повноти спостережень та оцінки межі обсягу спостережень для відмови від оцінювання при нестачі спостережень.*
***Ключові слова:*** *поведінкові аномалії; корпоративна вебсистема; моніторинг безпеки; Median/MAD; Isolation Forest;*

**Вступна частина.** У сучасній кібербезпеці значна увага приділяється аналітиці поведінки користувачів і сутностей (User and Entity Behavior Analytics) та підсистемам виявлення нормальної та аномальної поведінки в автоматизованій інформаційній системі. Така аналітика є тим більше важливою для систем з вебінтерфейсом. Корпоративні веборієнтовані інформаційні системи фіксують автентифікацію, зміну даних, погодження операцій та керування доступом. Нетипові дії користувача, їх частота або послідовність цих дій може свідчити про порушення політик безпеки, проте статистичне відхилення саме по собі не є доведеним інцидентом. За класифікацією [1] аномалії можуть бути точковими, контекстними та колективними. Для їх виявлення важливі не тільки алгоритм, а й склад доступних подій, повнота інформації про події, достовірність ідентифікації користувачів та якість журналювання [2].

**Мета дослідження.** Визначити умови застосовності порогових правил, робастної статистики та машинного навчання без учителя для виявлення поведінкових аномалій користувачів корпоративних вебсистем за неоднорідних і неповних журналів подій та обґрунтувати відповідні рішення для підсистеми AIS Monitor.

**Основна частина.** У базовому експерименті події з різних вебзастосунків нормалізовано за часом, джерелом, категорією дії, результатом, ідентифікатором суб’єкта та ознаками якості. На їх основі сформовано поведінкові вектори у часових вікнах. Розглянуто три підходи: порогові правила для явно визначених порушень; робастне відхилення від медіанного профілю з використанням MAD [3]; багатовимірне виявлення ізольованих спостережень алгоритмом Isolation Forest [4].

Використано п’ять штучно згенерованих і незалежних наборів даних (початкові значення генератора 42–46) з часовим розділенням навчальної, калібрувальної та тестової вибірок. Сукупний тестовий набір містив 6000 вікон зі сценарними мітками. Порогові правила досягли $F_{1_av} = 0{,}792$ за відсутності хибних спрацювань у цьому наборі; Median/MAD — $F_{1_av} = 0{,}666$ та FPR = 4,53 %; Isolation Forest — $F_{1_av} = 0{,}680$ та FPR = 1,86 %. Ці результати характеризують лише задані контрольовані сценарії, а не універсальну перевагу окремих

правил. Також для кожного методу важливо окремо встановлювати мінімально необхідні ознаки та достатність історичних даних.

Під час перевірки холодного старту в 130 конфігураціях варіювали обсяг навчальної історії, ширина часових вікон і частка пропущених даних. За збільшення кількості навчальних вікон із 200 до 2880 показник $F_{1_av}$ алгоритму Isolation Forest зріс із 0,319 до 0,644, хоча залежність від кількості вікон не була монотонною. Для Median/MAD значення залишалися приблизно в межах 0,68–0,67. Отже, статистичну придатність не можна ототожнювати лише з кількістю зібраних записів.

Істотним виявився вплив перенесення згенерованого профілю користувача між середовищами. За чотириразової зміни типової частоти операцій використання попереднього профілю призводило до FPR близько 17,74 % для правил, 100 % для Median/MAD та 99,89 % для Isolation Forest. Це підтверджує потребу локальної перевірки профілю після зміни характеру навантаження, що узгоджується з проблематикою зміни розподілу даних (concept drift) [5].

На незалежному контрольованому вебзастосунку FastAPI зі сценаріями погодження заявок після локального налаштування отримано $F_{1_av}$ = 0,635 (правила), 0,730 (Median/MAD) та 0,499 (Isolation Forest). Відповідні FPR становили 0,19 %, 1,90 % та 1,71 %. Відмінність від базового експерименту показує залежність ефективності від предметної області, типів дій і доступних ознак.

Перевірено також комбінування рішень детекторів. На 8700 тестових вікнах контекстна стратегія дала $F_{1_all} \approx 0{,}240$ та FPR = 1,51 % за частки доступних оцінок 81,44 %. Об'єднання детекторів за логічним «АБО» збільшило $F_{1_all}$ до $\approx 0{,}495$, проте FPR зріс до $\approx 24{,}81$ %. Окрема перевірка достатності спостережень для кожного методу (method-specific observability) забезпечила приріст $F_{1_all}$ лише з 0,195 до 0,197; заздалегідь визначеного порога практичної значущості +0,02 не досягнуто. Тому сукупну гіпотезу про перевагу цієї політики не підтверджено.

На основі результатів дослідження в AIS Monitor передбачено збереження походження подій, відокремлення невідомого значення атрибута від справжнього нуля, незалежні рішення детекторів та фіксація причин неможливості оцінювання. Встановлено, що порогові правила доцільні за наявності достовірних ознак конкретного порушення; правила на основі Median/MAD потребують стійкого локального профілю, а правила на основі Isolation Forest — репрезентативної історії та узгодженого набору ознак. Все це разом не дозволяє на основі розглянутих методів або їх композиції автоматично генерувати достовірний сигнал про аномальну поведінку користувача вебсистеми, але дозволяє оперативно надати оператору системи повідомлення із обґрунтованим поясненням про можливий інцидент для подальшої перевірки.

**Висновки.** Порівняння трьох методів на контрольованих наборах даних підтвердило «золоте правило» систем машинного навчання: «дані перемагають алгоритми» («Data beats algorithms»). Якість виявлення аномалій істотно залежить від складу подій, обсягу історії, повноти журналів і відповідності поведінкового профілю поточним умовам. Експерименти не підтвердили безумовної переваги складніших стратегій на основі комбінування різних методів виявлення аномалій, але отримані на основі такого комбінування результати можна оцінити як обнадійливі і їх бажано додатково перевірити на реальних корпоративних наборах даних — у ситуації, коли профілі користувачів можуть істотно відрізнятись від штучно згенерованих. Практично обґрунтованим є необхідність застосування прозорих правил на основі статистичних і машинних методів визначення повноти даних для визначення необхідної міри

їх репрезентативності для використання у зазначених методах і отримання на їх основі достовірних результатів визначення аномалій.

**Використання інструментів ШІ.** Для мовного та стилістичного редагування тексту тез доповіді, зокрема анотацій, вступу, основної частини та висновків, використано ChatGPT (OpenAI, модель GPT-6).

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


[1] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), Article 15. https://doi.org/10.1145/1541880.1541882

[2] Kent, K., & Souppaya, M. (2006). *Guide to computer security log management* (NIST SP 800-92). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92

[3] Rousseeuw, P. J., & Croux, C. (1993). Alternatives to the median absolute deviation. *Journal of the American Statistical Association*, 88(424), 1273–1283. https://doi.org/10.1080/01621459.1993.9476408

[4] Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). *Isolation forest. In 2008 Eighth IEEE International Conference on Data Mining* (pp. 413–422). IEEE. https://doi.org/10.1109/ICDM.2008.17

[5] Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). *A survey on concept drift adaptation. ACM Computing Surveys*, 46(4), Article 44. https://doi.org/10.1145/2523813



Novozhylov O.D., Gaida A.Yu.


**ASSESSING THE APPLICABILITY OF BEHAVIORAL ANOMALY DETECTION METHODS IN CORPORATE WEB SYSTEMS**


***Abstract.*** *The applicability of Rules, Median/MAD, and Isolation Forest to behavioral anomaly detection in corporate web systems is investigated. Experiments demonstrate that detection quality depends on log completeness and changes in user behavior. The necessity of assessing observation completeness separately for each method and retaining the option to abstain from evaluation when observations are unreliable has been substantiated.*



***Keywords:*** *behavioral anomalies; corporate web systems; security monitoring; Median/MAD; Isolation Forest.*