УДК 004.056.53

Палагін В.В., д.т.н., професор,
Яковлєв Б.В., магістрант,
Гуржій І.В., магістрант
Черкаський державний технологічний університет

ІНТЕГРАЦІЯ SIEM-СИСТЕМИ WAZUH В ДЕРЖАВНИХ ФІНАНСОВИХ УСТАНОВАХ

Актуальність теми зумовлена стрімкою цифровізацією державного сектору та одночасним зростанням кількості кіберзагроз. Державні фінансові установи, що оперують критичними бюджетними даними та персональною інформацією, є пріоритетними цілями для зловмисників. Впровадження ефективних систем моніторингу подій та управління інформаційною безпекою (SIEM) є нагальною потребою. Проте, обмеженість бюджетів державних установ вимагає пошуку гнучких та економічно ефективних рішень, яким є open-source платформа Wazuh.

Метою роботи є аналіз особливостей впровадження SIEM-системи Wazuh в інформаційну інфраструктуру державних фінансових установ для підвищення загального рівня їх кіберзахисту.

Для досягнення мети було проаналізовано типову архітектуру IT-систем в державних установах та запропоновано модель інтеграції Wazuh. Вона базується на трьох основних компонентах:

1. **Wazuh Server:** центральний компонент, що відповідає за аналіз отриманих логів, кореляцію подій та генерацію сповіщень;
2. **Wazuh Indexer:** кластер на базі OpenSearch, що забезпечує зберігання, індексацію та швидкий пошук великих обсягів даних про події безпеки;
3. **Wazuh Agents:** легковагі клієнти, що встановлюються на кінцеві точки (сервери, робочі станції) для збору системних журналів, моніторингу файлів та виявлення аномалій.

Процес інтеграції передбачає налаштування агентів для збору специфічних для фінансових установ подій, зокрема логів банківського ПЗ, систем електронного документообігу та баз даних.

Основними результатами впровадження запропонованої моделі є:

- **централізований моніторинг:** забезпечення єдиної точки збору та аналізу журналів подій з усієї інфраструктури, що є ключовим для розслідування інцидентів;
- **виявлення загроз в реальному часі:** автоматичне спрацювання правил кореляції на відомі техніки атак (напр., спроби підбору паролів, підвищення привілеїв, несанкціоноване ПЗ);

- **моніторинг цілісності файлів (FIM):** контроль за змінами у критичних системних файлах та конфігураціях фінансових додатків, що запобігає несанкціонованому втручанню;
- **аудит вразливостей:** автоматизоване сканування активів на наявність відомих вразливостей (CVE), що дозволяє встановити пріоритети оновлення.

Окрему увагу приділено тонкому налаштуванню правил кореляції (ruleset). Реалізовано моніторинг специфічних загроз (доступ до БД, UBA) та інтеграцію з каталогом MITRE ATT&CK для класифікації інцидентів.

В ході підготовки було протестовано ключові функції моніторингу. Зокрема, модуль **моніторингу цілісності файлів (FIM)** був налаштований на відстеження критичних системних файлів. Під час тестування система коректно ідентифікувала **всі** тестові спроби зміни цих файлів, генеруючи відповідні сповіщення. Це підтверджує готовність системи до захисту важливих даних та конфігурацій.

Перспективи подальшого розвитку системи полягають у її інтеграції з платформами класу SOAR (Security Orchestration, Automation and Response) для автоматизації типових сценаріїв реагування, а також у поглибленому використанні модулів машинного навчання для проактивного виявлення загроз.

Висновки. Інтеграція SIEM-системи Wazuh є ефективним та економічно обґрунтованим рішенням для державних фінансових установ. Вона дозволяє не лише швидко реагувати на інциденти, але й виявляти слабкі місця в захисті, забезпечуючи належний рівень інформаційної безпеки в умовах обмежених ресурсів. Впровадження даного рішення також сприяє виконанню вимог національних стандартів у сфері кібербезпеки та захисту інформації.

Список використаних джерел:

1. Wazuh: The Open Source Security Platform. [Електронний ресурс]. URL: https://wazuh.com (дата звернення: 12.11.2025).

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-viii (дата звернення: 12.11.2025).