Анчис А. О., магістрант,
Головня О. С., к.пед.н., доцент,
Державний університет «Житомирська політехніка»

СТРУКТУРА ТА ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ СИСТЕМИ МОНІТОРИНГУ ZABBIX

В умовах сучасного світу, де інформаційні технології є основою функціонування бізнесу, державних структур і соціальних систем, питання кібербезпеки стає надзвичайно актуальним. Забезпечення безпеки IT-інфраструктури є ключовим завданням для збереження конфіденційності, цілісності та доступності даних [1]. У цьому контексті моніторинг IT-систем стає основним інструментом для своєчасного виявлення та реагування на інциденти безпеки.

Одним із найефективніших рішень для моніторингу є система Zabbix, яка забезпечує комплексний підхід до управління IT-інфраструктурою. Її функціонал дозволяє не лише виявляти технічні несправності, а й аналізувати дані з точки зору безпеки, виявляти аномалії та оперативно сповіщати про загрози. Відкритий код, масштабованість і активна спільнота роблять Zabbix оптимальним вибором для організацій будь-якого розміру.

Мета дослідження полягає у вивченні структури та функціональних можливостях системи Zabbix. Аналіз практичних аспектів використання Zabbix спрямований на демонстрацію її потенціалу в побудові ефективної системи моніторингу, яка відповідає сучасним викликам та загрозам у сфері кібербезпеки.

Система моніторингу Zabbix є потужним інструментом для забезпечення кібербезпекового функціоналу в IT-інфраструктурі завдяки своїй гнучкості, масштабованості та інтеграційним можливостям. Її архітектура включає кілька ключових компонентів, що забезпечують комплексний моніторинг і управління. Zabbix Server є центральним елементом системи, відповідальним за збір, обробку та зберігання даних, а також за управління всіма процесами моніторингу. Zabbix Agents працюють на кінцевих системах, збираючи інформацію про продуктивність і стан інфраструктури. Веб-інтерфейс Zabbix Frontend забезпечує зручність у налаштуванні та аналізі даних для користувачів [2].

Система дозволяє здійснювати моніторинг стану таких компонентів, як міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), а також антивірусне програмне забезпечення. Інтеграція з цими рішеннями забезпечує моніторинг в режимі реального часу, дозволяючи оперативно реагувати на інциденти. Завдяки використанню статистичних методів система здатна ідентифікувати потенційні загрози, такі як DDoS-атаки чи спроби несанкціонованого доступу.

Моніторинг журналів (логів) дозволяє централізовано збирати інформацію з різних джерел, таких як операційні системи чи бази даних, для виявлення інцидентів безпеки. Крім того, Zabbix відстежує стан оновлень програмного забезпечення, що мінімізує ризики експлуатації вразливостей. Контроль доступу до систем дозволяє фіксувати аутентифікаційні події та виявляти підозрілі дії, такі як повторні невдалі спроби входу. Звіти та аудити, які генерує Zabbix, сприяють оцінці поточного стану безпеки та розробці рекомендацій для її покращення [3].

Однією з ключових переваг Zabbix є її здатність працювати з великими обсягами даних у масштабованих середовищах. Завдяки використанню проксі-серверів система забезпечує стабільну роботу навіть у розподілених мережах із багатьма сегментами. Це дозволяє компаніям, які мають складну та географічно розподілену інфраструктуру, централізовано управляти моніторингом і знижувати навантаження на центральний сервер.

Таким чином, Zabbix поєднує в собі широкі функціональні можливості, доступність і масштабованість, що робить її однією з найкращих систем для моніторингу в контексті забезпечення кібербезпеки. Її впровадження дозволяє організаціям не лише підтримувати високу продуктивність IT-інфраструктури, а й створювати ефективний захист від сучасних кіберзагроз.

Список використаних джерел

1. Системи моніторингу та керування - IT-Solutions, Україна. IT-Solutions, Україна. URL: https://it-solutions.ua/servisi/sistemi-monitoringu-ta-keruvannya/ (дата звернення: 02.12.2024).

2. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. URL: https://www.zabbix.com/ (date of access: 02.12.2024).

3. Overview of Zabbix. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. URL: https://www.zabbix.com/documentation/1.8/en/manual/about/overview_of_zabbix (date of access: 24.12.2024).