УДК 681.3.06

ПОБУДОВА СИСТЕМИ ЛОГУВАННЯ ТА МОНІТОРИНГУ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Яна Пилипчук

CONSTRUCTION OF A SYSTEM FOR LOGGING AND MONITORING INFORMATION SECURITY EVENTS

Yana Pylypchuk

Волинський національний університет імені Лесі Українки, просп.. Волі, 13, Луцьк 43025, Україна

Abstract. *The abstracts consider the importance of building logging and event monitoring systems as one of the key areas of ensuring information security. Logging allows you to record user actions, system events, and network activity, which is the basis for detecting violations and responding to incidents. Monitoring systems, in particular SIEM platforms, provide real-time event analysis and automated threat notification. Special attention is paid to the stages of building a system, selecting tools, and organizing log storage. The role of personnel and the need for continuous improvement of cyber protection procedures are also taken into account. It is emphasized that an effective logging system is not only a technical solution, but also an element of a risk management strategy. The materials presented will be useful to cybersecurity specialists, IT managers, and students of relevant specialties.*

У сучасну цифрову епоху інформаційна безпека стає пріоритетом для всіх – від державних установ до бізнесу і приватних користувачів. Активне використання хмарних технологій, мобільних пристроїв та віддаленого доступу створює нові ризики, які використовують кіберзлочинці для отримання доступу до конфіденційної інформації. У зв’язку з цим особливо важливими стають системи, що забезпечують збір і контроль подій у цифровому середовищі – логування та моніторинг [2].

Системи логування призначені для запису дій користувачів, змін налаштувань, спроб несанкціонованого доступу та інших критичних подій. Це дає змогу ефективно розслідувати інциденти і виявляти загрози.

Системи моніторингу, у свою чергу, забезпечують постійне спостереження за станом інформаційної інфраструктури, дозволяючи вчасно реагувати на порушення та знижувати можливі наслідки [4].

Захист інформації сьогодні передбачає не лише використання технічних засобів безпеки, але й постійний контроль над тим, що відбувається всередині IT-систем. Саме тому створення ефективних систем логування та моніторингу є необхідною умовою для своєчасного виявлення загроз і підтримки безпеки.

Першим кроком у впровадженні таких систем є визначення важливих подій, які потрібно реєструвати. До них можуть належати спроби входу в систему, зміна конфігурацій, збої в роботі програм, доступ до важливої інформації тощо. Це дозволяє уникати надмірного навантаження системи та зосередитися на ключових аспектах безпеки [3].

Наступним етапом є виявлення основних джерел логів – серверів, комп’ютерів, мережевого обладнання, антивірусного ПЗ, хмарних сервісів тощо. Кожен з цих компонентів створює журнали, які дозволяють оцінити стан системи та її слабкі місця. Для ефективного аналізу бажано централізувати всі дані.

У цьому допомагають спеціалізовані платформи, зокрема SIEM-системи (Security Information and Event Management), які забезпечують збір, зберігання, аналіз, звітування та візуалізацію подій.

Нормалізація логів – це перетворення інформації в єдиний формат для спрощення аналізу. Важливою функцією є також кореляція подій – встановлення зв'язку між різними сигналами, що дає змогу виявляти складні атаки чи приховані загрози всередині організації. Автоматичне інформування відповідальних фахівців дозволяє швидко реагувати і зменшувати шкоду від кіберінцидентів. Журнали подій мають зберігатися відповідно до чинного законодавства та внутрішніх норм – у захищеному вигляді, з обмеженим доступом і під постійним контролем.

Отже, структуровані механізми реєстрації та спостереження за безпековими інцидентами складають не просто технічну необхідність, а формують стратегічний актив у системі кіберзахисту організації.

В умовах постійної трансформації загроз ці інструменти забезпечують організаціям критично важливу здатність до раннього виявлення та протидії шкідливим втручанням. Інвестування у розвиток цих інфраструктурних компонентів створює міцний фундамент для збереження цілісності інформаційних систем та захисту конфіденційних даних.

Водночас, максимальна ефективність досягається лише за умови постійного вдосконалення методів аналізу, регулярного оновлення правил моніторингу та підвищення кваліфікації персоналу.

Підсумовуючи, можна стверджувати, що комплексний підхід до відстеження безпекових подій виходить далеко за межі суто технічного рішення – це інтегральний елемент загальної стратегії безпеки, який потребує належної уваги на всіх організаційних рівнях [2]. Належне впровадження таких систем суттєво підвищує стійкість цифрової інфраструктури та створює сприятливі умови для надійного функціонування організації в сучасному інформаційному просторі.

Бібліографія

1. Бровко О. М. Штучний інтелект як інструмент забезпечення кібербезпеки: сучасні виклики та перспективи розвитку // Інформаційна безпека України. 2023. № 1. С. 45–53.
2. Гладкий С. П. Кібербезпека в умовах цифрової трансформації: роль інтелектуальних технологій // Вісник Національного технічного університету України. 2022. Т. 18, № 2. С. 28–36.
3. Кириленко Л. А. Етичні та правові аспекти використання штучного інтелекту в системах захисту інформації // Правова держава. 2021. Вип. 32. С. 91–98.
4. Соловей І. В. Перспективи впровадження штучного інтелекту в інформаційну безпеку: міждисциплінарний підхід // Наукові праці НДІ інформатики і права. 2023. № 4. С. 60–68.