АНАЛІЗ ПРОБЛЕМ ВИКОРИСТАННЯ SIEM СИСТЕМ

Сєвєрінов О. В., Чубенко О. В.
Харківський національний університет радіоелектроніки, Харків, Україна

Одним з найбільш ефективних методів протидії інцидентам інформаційної безпеки є впровадження систем управління інформаційною безпекою та подіями безпеки - SIEM (Security information and event management) [1,2]. Проведений аналіз показав, що SIEM системи не тільки забезпечують управління інцидентами, а також контролюють помилки і збої в операційних системах, мережевому обладнанні, програмному забезпеченні. Але ці системи мають і низку суттєвих недоліків.

Метою доповіді є аналіз проблем використання SIEM систем в системах захисту інформації.

Проведений аналіз показав, що одним з основних недоліків систем управління інформаційною безпекою та подіями безпеки (SIEM), що заважає широкому використанню їх в малих і середніх підприємствах, є висока вартість [3].

Другим проблемним питанням є відсутність детального планування перед покупкою SIEM системи. Без попереднього планування ймовірність успішної реалізації SIEM-проекту майже нульова, а витрати часу, ресурсів і фінансів будуть набагато переважувати передбачувані вигоди. Тому через складність і високі вимоги системи безпеки SIEM часто не виправдовують очікування керівництва і користувачів, мета їх використання не досягається.

Крім того, однією з найпоширеніші причини невдалих SIEM-проектів є брак кваліфікованих ресурсів і навичок обслуговуючого персоналу (фахівців з досвідом з розслідування інцидентів, аудиту і тестів на проникнення). SIEM система потребує постійної настройки і обслуговування для адекватного реагування на зміни середовища, погроз, вимог регуляторів або даних.

Існує також низька проблем, пов‘язаних з технічними питаннями застосування систем управління інформаційною безпекою та подіями безпеки. Низька ефективність використання SIEM-систем пов’язана з необхідністю постійно змінювати налаштування системи.

Але, незважаючи на достатню кількість проблемних питань при використанні SIEM-систем, вони остаються ефективним засобом протидії інцидентам інформаційної безпеки. Тому ведеться активна робота по їх модернізації, покращенню їх параметрів та можливостей.

Список літератури

1. Miller D. et al. Security information and event management (SIEM) implementation. – McGraw-Hill, 2011.

2. Johansen G. Digital forensics and incident response: an intelligent way to respond to attacks. – 2017.

3. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. – Харків: ХНУРЕ, 2019. - С. 104–105.