АНАЛІЗ СУЧАСНИХ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ІНЦИДЕНТАМИ БЕЗПЕКИ

Овчаренко М.Ю., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В умовах постійного збільшення об'ємів інформації, що обробляються в різних інформаційно-комунікаційних системах, на перше місце вийшло питання наявності інструмента, за допомогою якого можливо було аналізувати події, що відбуваються, у реальному часі. Одним з рішень є використання системи управління інформаційною безпекою та інцидентами безпеки (SIEM, Security information and event management) [1]. Основа SIEM системи полягає в тому, що данні про інциденти безпеки збираються з різних джерел та результат їх обробки подається у єдиному звіті, що полегшує обробку результатів інцидентів та прийняття рішень по зменшенню залишкового ризику та збитків. Система SIEM складається з двох сегментів - сегменту управління інформаційною безпекою (SIM), що відповідає за аналіз даних з метою покращення ефективності системи, та сегменту управління інцидентами безпеки (SEM), що з загального обсягу інформації вибирає ту, за допомогою якої інциденти можуть бути виявлені негайно.

Метою доповіді є аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки та обґрунтування необхідності їх використання для захисту критичної інформації в інформаційно-телекомунікаційних системах.

В доповіді розглянуті результати досліджень SIEM систем компанією Gartner [2]. Проводиться аналіз найбільш відомих сучасних SIEM систем LogRhythm SIEM, Splunk та Tivoli Security Information and Event Manager (TSIEM) [3, 4] з визначенням їхніх основних відмінностей та переваг, що значно впливають на сфери та масштабність їхнього використання. Розробка методів та засобів збору, зберігання, структуризації та аналізу даних про інциденти безпеки, що змогли би реалізувати всі вимоги, які встановлені до SIEM систем нового покоління, має надзвичайно велике значення не лише для захисту інформації, що циркулює в окремих інформаційно-телекомунікаційних системах, але й для забезпечення державної безпеки.

Список літератури

1. H. Karlzen, «An Analysis of Security Information and Event Management Systems: The Use of SIEMs for Log Collection, Management, and Analysis.» January 2009

2. K. Kavanagh, T. Bussa, G. Sadowski. «Magic Quadrant for Security Information and Event Management». Gartner, 3 December 2018

3. Mozhaev O. Multiservise network security metric / O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, M. Lohvynenco // IEEE Advanced information and communication technologies-2017. Proc. of the 2th Int. Conf. – Lviv, 2017. – P. 133-136.

4. Buecker A., Amado J., Druker D., Lorenz C., Muehlenbrock F.,Tan R. «IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager». IBM Redbooks. 2010.