УДК 004.056
**Р. Маслій**
(Тернопільський національний технічний університет імені Івана Пулюя,Україна)

## СИСТЕМА БЕЗПЕКИ ДЛЯ ІОТ З ВИКОРИСТАННЯМ SIEM ТЕХНОЛОГІЙ

UDC 004.056
**R. Maslii**

# SECURITY SYSTEM FOR IOT USING SIEM TECHNOLOGIES

Вже зараз технологія IoT (Internet of Things) застосовується у широкому побутовому колі та сферах бізнесу, починаючи від розумних будинків, закінчуючи пристроями в космічній промисловості. Кожного разу, коли в систему додається можливість підключення нових пристроїв, збільшуються ризики. На сьогодні немає повністю прийнятної архітектури безпеки IoT систем. Виробники часто жертвують заходами безпеки заради того, щоб як найшвидше вийти на ринок, що може призвести до серйозних проблем у майбутньому для кожного окремого користувача.[1]

SIEM (Security Information and Event Management) є ключовим компонентом корпоративної інфраструктури. Термін SIEM комбінує в собі два управління: керування мережею та керування безпекою. SEM (управління подіями безпеки) здійснює аналіз журналів і кореляції подій (часто в режимі реального часу) для протидії загрозам безпеки та інцидентам. А SIM (управління інформацією про безпеку) – збір та керування журналами та звітність для внутрішніх аудитів або дотримання вимог.

Завдяки програмному забезпеченню SIEM можливо використовувати утиліти, які допомагають оцінити вразливості згідно стандартів. Перш ніж користувач обере той чи інший інструмент для роботи, він повинен розуміти основні принципи роботи моніторингу, наприклад, інструмент повинен відокремлювати нешкідливі невдалі спроби входу від цільових атак. Адже ключовими моментами є:

1. аналіз даних у реальному часі та автоматичне оповіщення користувача;
2. ведення журналу подій;
3. інтелектуальне виявлення загроз на основі архівних даних.

Всі ці дані повинні бути доступні для пошуку та фільтрації, щоб користувачі могли легко і швидко приймати рішення стосовно подальшої роботи. Графіки та лічильники наочно представляють те, що відбувається в системі, саме тому останнім часом більш популярною стає візуалізація даних.

Більшість хмарних постачальників, які надають рішення для IoT (MS Azure, Amazon Web Services, IBM Watson IoT і т.д.), надають надійний набір API та зовнішніх сховищ даних, що можуть бути легко інтегровані в кращі в своєму роді SIEM-рішення. [2] Тобто на етапі проектування в IoT систему можна легко інтегрувати існуючу архітектуру SIEM, що зрештою покращить і надасть додаткову цінність рішенню.

**Література**

1. Безпека IoT починається з ідентифікації. URL: https://iot-ssl.com.ua/iot_secure.html.
2. IoT and SIEM Integration. URL: https://medium.com/@dtembe/iot-and-siem-integration-pt-1-6645a012bdc.