УДК 004.056.5:004.056.54:005.8(045)

ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УПРАВЛІННІ СКЛАДНИМИ ТЕХНІЧНИМИ ОБ'ЄКТАМИ

Уляна Пановик[1,2], Назарій Єсик[1], Олександр Богоніс[2]
[1]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна
[2]Українська академія друкарства, м. Львів, Україна

Анотація. Розглянуто ключові аспекти оптимізації стратегій управління інформаційною безпекою в умовах складних технічних об'єктів. Проаналізовані основні компоненти центру операцій інформаційної безпеки (SOC), зокрема, системи управління інцидентами, та їхній вплив на прийняття рішень у реальному часі. Зокрема, досліджуються функції та роль SIEM-системи і NTA-системи в підтримці ефективної роботи SOC.
Ключові слова: інформаційна безпека, управління ризиками, SOC, прийняття рішень, технічні об'єкти.

Abstract. The key aspects of optimizing information security management strategies in the conditions of complex technical objects are considered. The main components of an information security operations center (SOC), including incident management systems, and their impact on real-time decision-making are analyzed. In particular, the functions and role of the SIEM system and the NTA system in supporting the effective operation of the SOC are investigated.
Keywords: information security, risk management, SOC, decision-making, technical objects.

У сучасному технічному середовищі, де складні технічні об'єкти стають неодмінною частиною промислових та корпоративних систем, питання інформаційної безпеки набувають великого значення. Масштабні інфраструктури, такі як енергетичні системи, транспортні мережі та виробничі комплекси, потребують ефективного управління, щоб забезпечити надійність та захист інформації. З метою покращення цього процесу, важливим є розроблення систем підтримки прийняття рішень щодо інформаційної безпеки. Такі системи можуть забезпечити необхідний інструментарій для аналізу, моніторингу та ефективного управління ризиками, пов'язаними з інформаційною безпекою складних технічних об'єктів.

Перший крок у вирішенні цього завдання – це розуміння конкретних викликів, які виникають при управлінні інформаційною безпекою в складних технічних системах [1]. Серед таких викликів можуть бути ідентифікація потенційних загроз, оцінка вразливостей системи, планування заходів забезпечення безпеки та реагування на інциденти. Далі, розробка інтегрованих систем підтримки прийняття рішень може охоплювати застосування аналітичних методів та технологій для обробки великих обсягів даних, зокрема, застосування штучного інтелекту та машинного навчання. Це дає можливість не лише виявляти потенційні загрози, а й передбачати їхні можливі виникнення, що полегшує прийняття рішень на ранніх стадіях [2]. Важливим компонентом системи підтримки прийняття рішень є також моніторинг та аналіз у реальному часі, що дає змогу оперативно реагувати на зміни в інформаційному середовищі та запобігати можливим інцидентам безпеки.

Для виявлення інцидентів на початкових етапах атак використовується центр моніторингу та реагування на інциденти інформаційної безпеки, відомий як *security operations center* (SOC). Основним завданням SOC є нагляд за активністю в IT-інфраструктурі, аналіз подій, виявлення загроз інформаційної безпеки та відповідь на них [3]. Виявлення потенційних загроз безпеці системи здійснюється під час збирання події з різних джерел, таких як ПК, сервери, бази даних, бізнес-системи та мережеве обладнання включно з мережевим трафіком. Для розв'язання цих завдань використовуються компоненти SOC, зокрема, системи класу *security information and event management* (SIEM), які автоматизують збір подій та виявлення інцидентів інформаційної безпеки.

SIEM-система діє як централізоване вікно для всіх подій від підключених джерел. Збір подій в SIEM-системі реалізується за допомогою спеціальних правил нормалізації, які дають можливість системі розпізнати, що отримується події з конкретного джерела, та структурувати дані за визначеними параметрами (час події, користувач, IP-адреса тощо). Це надає

інформаційній безпеці можливість отримувати події в єдиному форматі, що зручно, як для ручного аналізу, так і для автоматизованого порівняння подій.

Зазвичай, SIEM-системи використовують бази даних для проведення аналізу поведінки користувачів та облікових записів, відомі як *user and entity behavior analytics* (UEBA). Цей аналіз ґрунтується на виявленні відхилень від середньостатистичних даних, зібраних упродовж тривалого періоду. Наприклад, якщо співробітник увійшов у систему вперше за пів року в ночі, це може свідчити про потенційний інцидент. SIEM-системи, як правило, використовують стандартні журнали інших систем, таких, як операційні системи, мережеве обладнання, антивірусні засоби, міжмережеві екрани, Active Directory, DNS та DHCP-сервери. Рівень деталізації, з яким фахівці SOC можуть проаналізувати події, залежить від налаштувань журналювання на цільовій системі. Для виявлення подій на кінцевих точках користувачів та серверах в IT-інфраструктурі може бути використаний інструмент класу *endpoint detection and response* (EDR). Цей інструмент не лише має вбудовані механізми журналювання, але також детально аналізує події на рівні операційної системи.

Важливим джерелом для виявлення інцидентів може бути мережевий трафік в IT-інфраструктурі. Для автоматизації збору та аналізу подій, що відбуваються в трафіку, використовуються інструменти класу *network traffic analysis* (NTA). NTA-система може функціонувати, як самостійний засіб із власними двигунами нормалізації та кореляції, а також слугувати джерелом даних щодо інцидентів інформаційної безпеки для SIEM-системи. Основна відмінність від звичайних систем виявлення мережевих атак (IDS) полягає в тому, що NTA-система працює з великими обсягами трафіку. Це дає можливість виявляти повний цикл атак, а не обмежуватися окремою сигнатурою. Крім того, NTA-система зберігає копію трафіку для подальшого аналізу. На збереженій копії можна перевіряти нові індикатори компрометації (IOC). Додатково, збережений трафік сприяє проведенню докладного розслідування кіберінциденту та допомагає на основі аналізу виявляти невідомі загрози.

Також, для виявлення невідомих загроз, можна використовувати аналіз поведінки будь-якого програмного забезпечення, яке потрапило до IT-інфраструктури, незалежно від того, чи це знімний диск, Інтернет чи внутрішня мережа. Для цього аналізу використовуються інструменти класу *sandbox* (пісочниці). Пісочниця може вивчати поведінку об’єкта всередині спеціально створеного середовища та виносити рішення про те, наскільки об’єкт може бути небезпечним. Рекомендовано проводити перевірку всіх файлів всередині трафіку, якщо відправити потік файлів із трафіку від NTA до пісочниці. Знайдені рішення та індикатори файлів можна використовувати, як у NTA, так і в SIEM-системі. Коли не вистачає достатньої інформації, то тоді можуть бути використані засоби управління активами (AM) та управління вразливістю (VM). Такі системи можуть бути, наприклад, у ролі сканерів вразливостей, які за допомогою активного мережевого сканування допомагають складати списки активів в IT-інфраструктурі та фіксувати їх вразливості. Це дасть змогу належним чином оцінити загрози та інциденти з огляду на спроби злому, які зафіксовані у SIEM-системі, і визначити ступінь небезпеки цих спроб для конкретної атакованої системи.

У підсумку, підтримка прийняття рішень щодо інформаційної безпеки в управлінні складними технічними об’єктами є важливим напрямком розвитку в умовах зростаючих викликів у кіберпросторі. Впровадження інтегрованих та інтелектуальних систем допомагає підвищити рівень захисту інформації та забезпечити стабільність функціонування складних технічних об’єктів в умовах сучасного цифрового середовища.

Інформаційні джерела

1. Пановик У. П. Системний підхід до управління ризиками інформаційної безпеки. *Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України*: Тези доп. IX Всеукр. заоч. науково-практ. конф., м. Київ, 2023 р. с. 125–126. URL: https://kztdop.ipf.npu.edu.ua/science-conference/conferenc-bgd.
2. Reeves A., Ashenden D. (2023). Understanding decision making in security operations centers: building the case for cyber deception technology. *Frontiers in Psychology*. *Vol. 14*. https://doi.org/10.3389/fpsyg.2023.1165705
3. Happa J., Agrafiotis I., Helmhout M., Bashford-Rogers T., Goldsmith M., Creese S. (2021). Assessing a decision support tool for SOC analysts. *Digital Threats Res. Pract.* 2, 1–35. https://dl.acm.org/doi/10.1145/3430753