УДК 004.056

В. С. Бугаєць
Л. М. Куперштейн

СИСТЕМА АВТОМАТИЗАЦІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

В ході проведеного дослідження було проаналізовано процес реагування на інциденти як систематичний набір дій. Запропоновано та розроблено автоматизовану систему для реагування на інциденти. Розроблено тестові сценарії реагування та успішно впроваджено їх у систему, що зменшило час реагування на інциденти в два рази.

Ключові слова: інцидент безпеки, загроза, кібербезпека, автоматизація, система реагування.

Abstract

In the conducted study, the incident response process was analyzed as a systematic set of actions. An automated incident response system was proposed and developed. Test response scenarios were created and successfully implemented into the system, reducing the incident response time by half.

Keywords: security incident, threat, cybersecurity, automation, response system

Вступ

У сучасному цифровому світі кібербезпека стає все більш критичною для організацій різних галузей. Зростання кількості та складності кіберзагроз вимагає ефективних механізмів реагування на інциденти, які можуть мінімізувати потенційні збитки та забезпечити безпеку інформаційних ресурсів [1]. Метою даного дослідження є аналіз процесу реагування на інциденти в сфері кібербезпеки та визначення ролі автоматизації у підвищенні ефективності цього процесу.

Основна частина

Процес реагування на інциденти – це систематичний набір дій, спрямованих на ідентифікацію, аналіз, стримування, усунення та відновлення після кіберзагроз або порушень інформаційної безпеки. Основна мета цього процесу – мінімізувати вплив інциденту на організацію, захистити її критичні активи та забезпечити безперервність бізнес-процесів [2, 3]. Основні етапи даного процесу наведено на рисунку 1.

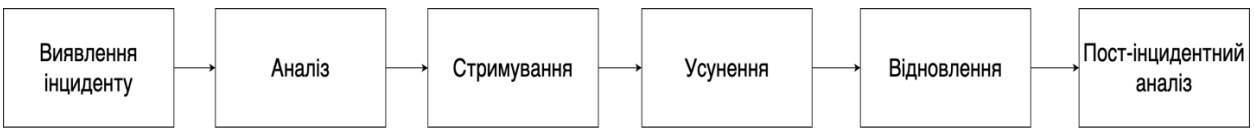

Рисунок 1 – Схема етапів реагування на інциденти

Процес реагування на інциденти складається з шести ключових етапів: виявлення інциденту, аналізу, стримування, усунення загрози, відновлення систем та пост-інцидентного аналізу. На кожному з цих етапів виконуються відповідні дії, спрямовані на ідентифікацію загрози, її нейтралізацію та відновлення нормальної роботи систем.

Ручна обробка інциденту на кожному з етапів займає значний час, що може дозволити загрозі поширитися глибше в системі. Крім того, людський фактор може призвести до помилок.

Архітектура системи автоматичного реагування на інциденти включає кілька ключових компонентів, таких як шари інтеграції, автоматизації, плейбуків, оркестрації, моніторингу та пост-інцидентного аналізу (рис 2.)

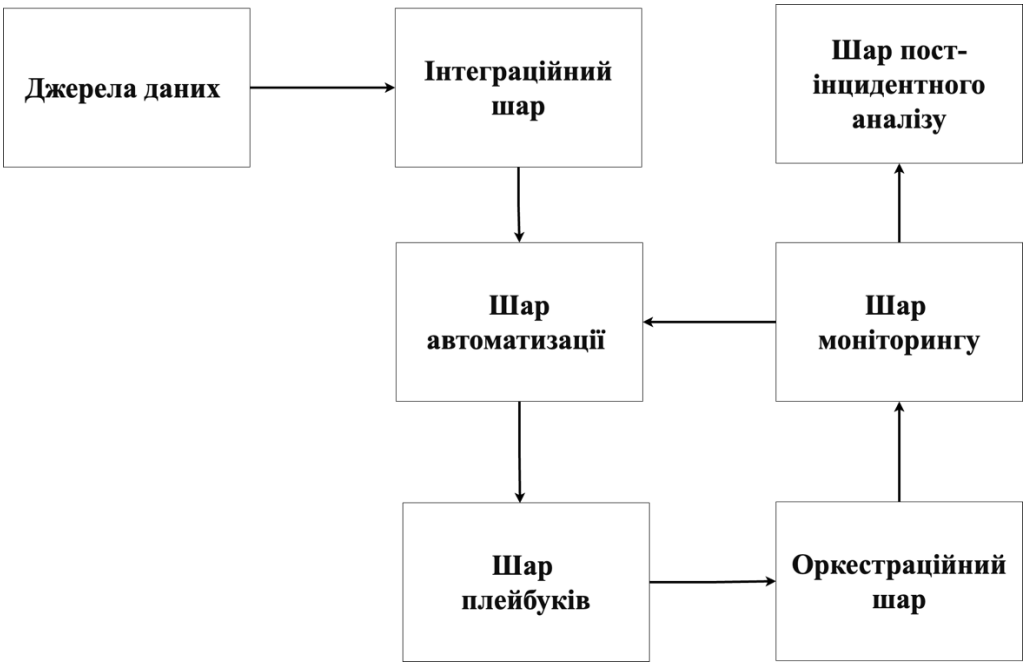

Рисунок 2 – Архітектура системи

Ці компоненти забезпечують швидке виявлення, аналіз і нейтралізацію загроз у режимі реального часу. Основна мета рішення – зменшення часу реагування на інциденти, автоматизація рутинних завдань і мінімізація людського фактору, що забезпечує підвищення рівня захищеності інформаційних систем.

Для тестового впровадження було реалізовано кілька сценаріїв реагування, включаючи управління доступом, безпеку електронної пошти, мережеву безпеку, захист хмарних середовищ та виявлення шкідливого програмного забезпечення. Їх було протестовано в умовах приближених до справжніх. Результати тестування показали, що час реагування на інциденти скоротився у два рази.

Висновок

У результаті тестового впровадження запропонованої системи автоматизації процесу реагування на інциденти було досягнуто зменшення часу реагування на інциденти в 2 рази.

Автоматизація рутинних завдань знизила ризик людських помилок, підвищивши точність та надійність реагування.

Таким чином, реалізація автоматизованої системи реагування на інциденти сприяє підвищенню безпеки, забезпеченню безперервності бізнес-процесів та зміцненню довіри до інформаційних систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Crowdstrike GlobalThreatReport2024 URL: https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf
2. National Institute of Standards and Technology (NIST). “Computer Security Incident Handling Guide” (SP 800-61) URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
3. ENISA (European Union Agency for Cybersecurity). “Incident Response and Management.” URL: https://www.enisa.europa.eu/topics/incident-response

Науковий керівник: **Куперштейн Леонід Михайлович** – канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця,
e-mail: kupershtein@vntu.edu.ua

Бугаєць Владислав Сергійович – студент групи 1БС-23М, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця,
e-mail: vladbugaets@gmail.com

Supervisor: **Kupershtein Leonid Mykhailovych** — Cand. Sc., Associate Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia,
e-mail: kupershtein@vntu.edu.ua

Buhaiets Vladislav S. – student of group 1BS-23M, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia,
e-mail: vladbugaets@gmail.com