**УДК 004.7:8**
**А. Бучко; М. Стадник, к.т.н, доцент**
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

# РОЗРОБКА СТРАТЕГІЙ РЕАГУВАННЯ НА ІНЦИДЕНТИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

**UDC 004.7:8**
**A. Buchko, student of gr. СБм-62; M. Stadnyk, Ph.D.**

# DEVELOPMENT OF INCIDENT RESPONSE STRATEGIES IN INFORMATION SYSTEMS

Зважаючи на постійне зростання кількості кіберзагроз, розробка стратегій реагування є критично важливою для забезпечення та підтримання безпеки інформаційних систем. Особливу увагу варто приділяти швидкості виявлення інцидентів та мінімізації їх наслідків. Згідно з звітом IBM (2023 рік), вчасне реагування на інциденти дозволяє зменшити фінансові втрати компанії до 30%. У 2023 році середня вартість витоку даних досягла рекордного рівня в 4,88 мільйона доларів США, що на 10% більше порівняно з 2022 роком (4,45 мільйона доларів США). Це свідчить про зростання фінансових втрат, пов'язаних із кіберінцидентами, та підкреслює необхідність ефективних стратегій реагування для мінімізації їх наслідків [1].

Інциденти поділяються на мережеві атаки, компрометацію даних, відмову обладнання та збої програмного забезпечення. Така класифікація дозволяє більш ефективно розробляти стратегії для кожного типу інциденту [2].

Стратегія реагування на інциденти включає шість основних етапів: підготовку, виявлення, аналіз, стримування, ліквідацію та відновлення. Кожен з етапів супроводжується набором інструментів для автоматизації, таких як SIEM (Security Information and Event Management) – системи та SOAR (Security Orchestration, Automation and Response) – платформи [3].

| Етап | Опис |
|---|---|
| Підготовка | Розробка політик, навчання персоналу, планування реагування на інциденти. |
| Виявлення | Виявлення загроз та аномальної активності за допомогою SIEM-систем. |
| Аналіз | Збір та аналіз даних для визначення джерела та масштабів загрози. |
| Стримування | Ізоляція уражених систем для запобігання подальшого поширення загрози. |
| Ліквідація | Видалення шкідливого програмного забезпечення та відновлення систем. |
| Відновлення | Повернення до нормальної роботи, оцінка ефективності реагування. |

**Рисунок 1.** Етапи реагування на кіберзагрози

Використання SOAR(Security Orchestration, Automation and Response) платформ – дозволяє значно скоротити час реагування на інциденти, підвищити точність аналізу загроз і мінімізувати людський фактор. Згідно з Gartner (2023), автоматизація процесів знижує час усунення інцидентів у середньому на 40% [4].

Таким чином, запропонована стратегія реагування на інциденти довела свою ефективність під час тестування на прикладі моделювання реальних кіберзагроз. Вона дозволяє зменшити час простою систем, мінімізувати втрати даних та підвищити загальну стійкість інформаційних систем до інцидентів. Це підтверджує доцільність її впровадження в організаціях.

**Література**

1. IBM Security. Cost of a Data Breach Report 2023 // IBM Security Reports, 2023, URL: https://www.ibm.com.
2. NIST. Computer Security Incident Handling Guide (SP 800-61 Rev. 2) // NIST Special Publications, 2022, URL: https://csrc.nist.gov.
3. ENISA. Cybersecurity Incident Response Guidelines // ENISA Publications, 2023, URL: https://www.enisa.europa.eu. (https://www.enisa.europa.eu/)
4. Gartner. SOAR Market Guide // Gartner Reports, 2023, URL: https://www.gartner.com.