теоретичних дисциплін, таких як математичне програмування, теорія ігор та інше [3].

В умовах воєнного стану збереження інформації та можливість її використання, а також не допущення несанкціонованого доступу до певної інформації має особливе значення. Це пов'язане з певними технічними негараздами (наприклад, відключення енергопостачання, перебування студентів в зоні військових дій, вплив міграційних факторів), також можливістю атак за допомогою певного програмного забезпечення, спрямованих на викрадення, знищення, пошкодження даних.

Список використаних джерел:

1. Закон України "Про національну програму інформатизації". URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 19.03.2025).

2. Онопрієнко М. В. Інформаційні технології в науці: методологічний вплив і проблеми. *Наука та наукознавство.* 2011. № 3. С. 48–58.

3. Шишкіна М. П. 10 Інститут інформаційних технологій і засобів навчання НАПН України, Київ, Україна / Моделі організації доступу до програмного забезпечення у хмаро орієнтованому освітньому середовищі. DOI: 10.14308/ite000525

DOI https://doi.org/10.36059/978-966-397-502-3-62

Черемнов М. В.,
аспірант кафедри комп'ютерної інженерії та інноваційних технологій
Міжнародного гуманітарного університету
м. Одеса, Україна

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Упровадження кіберзахисту як важливої частини об'єктів критичної інфраструктури (далі ОКІ) вимагає використання відповідних методів для розуміння поточних і потенційних проблем кіберзахисту та відповідного їх усунення.

Управління ризиками інформаційної та кібербезпеки, аудит системи управління інформаційних систем, реагування на інциденти кібербезпеки, управління вразливостями в інформаційно-комунікаційних систем і розвідка загроз належать до таких основних методів.

Незважаючи на те, що методи, зазначені вище, є важливими, проблеми кібербезпеки та управління вразливостями є більш поширеними для ОКІ.

Розробка та впровадження процесу управління вразливостями є необхідним для виявлення вразливостей, їх усунення та контролю. Однак існує ряд проблем, які потребують негайного вирішення:

– процес управління вразливостями не регулюється;
– пошук і усунення вразливостей проводиться безсистемно;
– контроль відповідності політикам безпеки не проводиться регулярно;
– результати пошуку вразливостей зазвичай не аналізуються, а процедури не працюють досить добре [2].

Наприклад, список Top 10 Open Web Application Security Project (OWASP) є загальноприйнятим списком найбільш важливих загроз безпеці веб-додатків. Він явно не надає комплексної основи для етапів керування вразливістю, незважаючи на те, що його основна мета полягає у виявленні та усуненні вразливостей. Тим не менш, можна виділити загальну стратегію управління вразливістю, яка включає десять найкращих принципів OWASP:

– постійний моніторинг;
– перевірка та тестування;
– сканування вразливостей;
– оцінка ризиків;
– реагування на інциденти;
– навчання та підвищення обізнаності;
– документація та звітність [1].

Ідентифікація вразливостей, встановлення пріоритетів, виправлення та постійний моніторинг – це принципи, які є основою цієї методики, які є ключовими для ефективного керування вразливістю.

Книжка «Управління вразливостями для новачків» містить загальні вказівки щодо управління вразливостями, а також поради щодо вибору інструментів для їх реалізації.

Відповідно до цього джерела, основними кроками управління вразливостями є:

1. Прийняття заходів щодо управління вразливостями відповідно до політики безпеки організації.
2. Інвентаризація та категоризація активів.
3. Використання методів сканування вразливостей.
4. Перевірка невідповідностей відповідно до активів.
5. Розподіл і ранжування ризиків.
6. Підготовка та застосування патчів і виправлень для усунення вразливостей.
7. Перевірка ефективності використаних засобів [3].

SANS Institute пропонує альтернативну стратегію управління вразливостями [2]. Ця стратегія полягає в виконанні наступні кроків:

1. Підготовка до сканування включає визначення масштабу, типу сканування та планування.
2. Тестування вразливостей.
3. Визначення методів усунення вразливостей.
4. Вживати заходів щодо усунення вразливостей.
5. Додаткове сканування.

NIST 800-40v4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology містить інформацію про стандартизовані методи управління вразливостями. У цьому стандарті запропоновано підхід, який включає наступні кроки:

1. Визначення внутрішніх і зовнішніх ресурсів інфраструктури.
2. Визначення вразливих активів, якими ми хочемо керувати, і визначте, наскільки вони важливі для бізнес-процесів компанії.
3. Пряме сканування вразливостей.
4. На основі правил управління вразливостями ОКІ отримують завдання з усунення вразливостей.
5. Повторне сканування, щоб забезпечити оновлення інформації щодо вразливостей, виявлених і усунених фахівцями, а також розподіл нових завдань для усунення нових вразливостей, якщо вони виявляються.
6. Отримання звітів від керівництва щодо роботи відділів, працівників і змін у ризиках компанії [3].

За результатами аналізу зазначених вище методів управління вразливостями можна зробити висновок, що вони залежать від кількості та актуальності використовуваних даних. Одним із недоліків зазначених методів є відсутність регламентованих процедур збору та обробки даних. Крім того, відсутні процедури накопичення даних, які дозволяють проводити ретроспективний аналіз під час розслідування кіберінцидентів. Таким чином, немає належного контролю над процедурами управління вразливостями, що може мати значний вплив на рівень кібербезпеки ОКІ. З цієї причини розробка методів і ресурсів, спрямованих на отримання та оброблення повної актуальної інформації, є необхідною для цього процесу.

Список використаних джерел:

1. OWASP Top Ten | OWASP Foundation. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: https://owasp.org/www-project-top-ten/ (date of access: 24.03.2025).

2. Palmaers T. Implementing a vulnerability management process. *Egnyte*. URL: https://www.giac.org/paper/gsec/32851/implementing-vulnerability-management-process/112555 (date of access: 31.07.2023)

3. Souppaya M., Scarfone K. Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. *National Institute of Standards and Technology*. 2022. URL: https://doi.org/10.6028/NIST.SP.800-40r4 (дата звернення: 24.03.2025).