УДК 004.056
О. Ярема; Н. Загородна, к. т. н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

КЛАСИФІКАЦІЇ ТИПІВ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО КОДУ

UDC 004.056
O. Yarema; N. Zagorodna PhD., Assoc. Prof.

CLASSIFICATION OF SOFTWARE CODE VULNERABILITY TYPES

Популярні класифікації вразливостей, що використовуються в наукових та навчальних джерелах, зазвичай не відповідають науковим критеріям класифікації. Вони можуть досить точно описувати дефект чи слабкість технології, через яку виникає вразливість, проте вразливості в таких випадках майже ніколи не відповідають одному класу, а можуть належати зразу до декількох.

Одним з найпоширеніших способів класифікувати вразливості є класифікація за фазою життєвого циклу розробки (SDLC). Вона намагається класифікувати вразливості за моментом їх появи в розробці, групуючи їх за фазами, наприклад дизайну, реалізації, обслуговування [1, 2]. Така класифікація сильно залежить від конкретної моделі розробки, що ускладнює уніфікацію і порівняння вразливостей між різними проєктами. Крім цього, вразливості програмного коду зазвичай рідше розрізняють за такими фазами, адже вони несуть мало корисного змісту безпосередньо для опису вразливості.

Серед інших популярних підходів існує класифікація за враженою технологією, наприклад «вразливість форматування рядка». Проте така класифікація не є універсальною, адже багато вразливостей не стосуються конкретно певної технології, а мають інший характер виникнення [2]. Іншим способом є класифікація вразливостей за сценарієм атаки, який її використовує, як от вразливість «cross-site scripting (XSS)». Така класифікація є описово точною і надає чітку спільну ознаку класу вразливостей. Але такий підхід не завжди є однаково ефективним. Термін «вразливості відмови в обслуговуванні» є прикладом менш корисного опису класу, адже відмова в обслуговуванні є лише наслідком атаки, а не сценарієм чи вказівником вразливості [2, 3]. Тому під такий клас можуть потрапити широкий спектр абсолютно різних вразливостей.

Одним з класифікаторів саме вразливостей для програмного коду є поділ на латентні, потенційні та експлуатовані вразливості [3]. Латентні це вразливості коду, який поки не експлуатується, через що вразливості ще не були виявлені чи використані. Потенційні вразливості зазвичай представляють погані практики написання коду, які не обов’язково є вразливістю, як такою, але мають потенціал стати нею після змін в коді. І експлуатовані вразливості це власне вразливості, які можна одразу виявити в коді та використати.

Головним осередком зусиль уніфікувати та подолати недоліки ненаукових класифікацій є MITRE Common Weakness Enumeration (CWE) [4, 5]. CWE це ініціатива зі створення словника вразливостей програмного забезпечення. Хоча CWE не є суворою таксономією вразливостей, він замінив попередню спробу MITRE – Preliminary List of Vulnerability Examples for Researchers (PLOVER) – що створювалася на основі фактичних проблем в порядку їх виникнення [5]. Серед подібних, але сфокусованих на атаках, є ініціатива Common Attack Pattern Enumeration and Classification (CAPEC), яка використовує шаблони атак як структуру для опису подібних типів атак [6]. Також непрямим інструментом для уніфікації є MITRE Common Vulnerabilities and Exposures (CVE), який надає унікальні ідентифікатори для вразливостей програмних артефактів.

Література

1. Security threat and vulnerability assessment and measurement in secure software development / M. Humayun та ін. Computers, materials & continua. 2022. Т. 71, № 3. С. 5039–5059. URL: https://doi.org/10.32604/cmc.2022.019289 (дата звернення: 06.12.2025).

2. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions / Ö. Aslan та ін. Electronics. 2023. Т. 12, № 6. С. 1333. URL: https://doi.org/10.3390/electronics12061333 (дата звернення: 06.12.2025).
3. Categorization of vulnerabilities in a software / N. Bhatt та ін. System reliability management. Boca Raton : Taylor & Francis, a CRC title, part of the Taylor &, 2018. С. 121–135. URL: https://doi.org/10.1201/9781351117661-9 (дата звернення: 06.12.2025).
4. Study on software vulnerability characteristics and its identification method / C. Luo et al. Mathematical problems in engineering. 2020. Vol. 2020. P. 1–6. URL: https://doi.org/10.1155/2020/ 1583132 (date of access: 06.12.2025).
5. Martin B. Common vulnerabilities enumeration (CVE), common weakness enumeration (CWE), and common quality enumeration (CQE). ACM SIGAda Ada Letters. 2019. Т. 38, № 2. С. 9–42. URL: https://doi.org/10.1145/3375408.3375410 (дата звернення: 06.12.2025).
6. Dimitrov V. CAPEC ontology. Annual of sofia university st. kliment ohridski. faculty of mathematics and informatics. 2023. Т. 110. С. 63–83. URL: https://doi.org/10.60063/gsu.fmi.110.63-83 (дата звернення: 06.12.2025).