УДК 004.77
Свирида А. В. – ст. гр. СІм-51
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ МЕТОДІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ ВЕБ-САЙТІВ ТА СПОСОБИ ЗАХИСТУ ВІД НИХ

Науковий керівник: к.т.н., доцент Луцків А. М.

Svyryda A. V.
Ternopil Ivan Pul'uj National Technical University

RESEARCH METHODS OF UNAUTHORIZED ACCESS TO WEBSITES INFORMATION AND HOW TO PROTECT YOURSELF

Supervisor: Lutskiv A. M.

Ключові слова: ризик, веб-сайт, захист
Keywords: risk, website, protection

Ненадійність програмного забезпечення негативно впливає на важливі об'єкти інфраструктури: фінанси, охорона здоров'я, оборона, енергетика та інші. Оскільки, програмне забезпечення є складним і розгалуженим, труднощі досягнення необхідного рівня безпеки додатків зростають в геометричній прогресії. Швидкі темпи сучасних процесів розробки програмного забезпечення вимагають виявляти ризики максимально швидко і точно.

Згідно з актуальними (2017) дослідженнями Інтернет ресурсу Open Web Application Security Project (OWASP) виділено 10 основних загроз інформаційній безпеці: Injection, Broken Authentication and Session Management, Cross-Site Scripting (XSS), Broken Access Control, Security Misconfiguration, Sensitive Data Exposure, Insufficient Attack Protection, Cross-Site Request Forgery (CSRF), Using Components with Known Vulnerabilities, Underprotected APIs. Вони не завжди є ізольованими, чи слідують обмеженій систематиці. Ці вразливості класифікуються за характером дій зловмисника, недоліком безпеки системи чи типом певних активів [1].

З метою підвищення стійкості веб-сайтів потрібно враховувати рекомендації (best practices) на всіх етапах життєвого циклу програмного забезпечення: формулювання вимог, проектування системи, кодування, тестування, документування, розгортання та супроводу. Варто відслідковувати ключові аспекти діяльності зловмисників в Україні, зокрема, актуальна інформація стосовно інцидентів відображена на ресурсі [2].

В ході магістерського дослідження проводиться аналіз можливих загроз та розробляються заходи по зменшенню кількості прогалин у безпеці програмного забезпечення.

Перелік посилань:
1. Команда реагування на комп'ютерні надзвичайні події України [Електронний ресурс]. – Режим доступу : URL : http://cert.gov.ua/. – CERT-UA.
2. Open Web Application Security Project [Electronic Resource]. – Mode of access : URL : https://www.owasp.org/. – OWASP.