International Science Group

ISG-KONF.COM

II

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE "YOUNG SCIENTISTS AND METHODS OF IMPROVING MODERN THEORIES"

Milan, Italy

September 26 - 29, 2023

ISBN 979-8-89074-566-8

DOI 10.46299/ISG.2023.2.2

YOUNG SCIENTISTS AND METHODS OF IMPROVING MODERN THEORIES

Proceedings of the II International Scientific and Practical Conference

Milan, Italy
September 26 – 29, 2023

26.	Мартинюк М.Т., Підгорний О.В. ПРО МОДЕЛЬ ПЕДАГОГІЧНОЇ СИСТЕМИ ФОРМУВАННЯ У ЗДОБУВАЧІВ ВИЩОЇ ПЕДАГОГІЧНОЇ ОСВІТИ СУЧАСНОЇ ПРИРОДНИЧО-НАУКОВОЇ КАРТИНИ СВІТУ (ТА ВІДПОВІДНОГО ЇЙ ОБРАЗУ СВІТУ) ЯК ОСНОВИ ЙОГО ОСОБИСТІСНОГО ТА ПРОФЕСІЙНОГО СТАНОВЛЕННЯ	143
	PHILOLOGY	
27.	Mashakova A.K. LOUIS ARAGON AND CENTRAL ASIAN LITERATURE	147
28.	Miroshnyk S. ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ВЖИВАННЯ ЧАСІВ В ІСПАНСЬКІЙ ТА УКРАЇНСЬКІЙ МОВАХ	151
29.	Вовченко Г.І. ПОГЛЯДИ НА ФЕМІНІЗАЦІЮ Й НЕОФЕМІНІЗАЦІЮ В СУЧАСНОМУ УКРАЇНСЬКОМУ МОВОЗНАВСТВІ	155
	TECHNICAL SCIENCES	
30.	Andriievskyi V. RESEARCH ON THE EFFECTIVENESS OF SOLVING THERMOVISCOELASTOPLASTICITY PROBLEMS OF PRISMATIC BODIES USING THE SEMI-ANALYTICAL FINITE ELEMENT METHOD	158
31.	Presniakov M., Skrypnyk N. ACTIVE CAR SAFETY SYSTEM	160
32.	Toitanov Y. THE FUTURE OF 3D PRINTING TECHNOLOGY FOR ROCKET MANUFACTURING	163
33.	Безрук Д.О. ВИКОРИСТАННЯ ДРОНІВ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТРАНСПОРТНО-ЕКСПЕДИТОРСЬКОЇ ДІЯЛЬНОСТІ ТА ЛОГІСТИКИ	169
34.	Білобородов О. ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ	173

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Білобородов Олександр,
магістрант кафедри інформатики
Харківський національний університет радіоелектроніки

Проблеми інформаційної безпеки є важливими та актуальними для сучасного суспільства. Повальна інформатизація, технологізація охоплює все більше сфер суспільства, від використання розумних помічників у побуті до інформатизації цілих галузей держави.

У цьому є вагомі переваги: в побуті – це економія часу на повсякденних рутинних справах, для бізнесу – це можливість економії на ресурсах (наприклад, реалізація концепції «банк без відділень»), для держави перенесення послуг в онлайн – це спрощення взаємодії формальних процедур та ефективний механізм боротьби з корупцією.

Роблячи таку цифрову трансформацію, вирішуємо одні проблеми, але тепер стикаємося і з новими. Перехід сервісу, бізнесу, або цілої галузі в онлайн означає появлення нових викликів, пов’язаних з необхідністю підтримки таких характеристик інформаційної безпеки [1] як:

– доступність (availability);
– цілісність (integrity);
– конфіденційність (confidentiality).

Тобто, говорячи простими словами, інформаційна система повинна справлятися з загрозами, що можуть викликати непрацездатність системи, що призводять до несанкціонованої зміни даних та з загрозами, що викликані розкриттям конфіденційної інформації особам, що не мають на це спеціальних повноважень.

Розглядаючи побудову сучасних клієнт-серверних застосунків та SaaS-рішень, можна виділити типовий стек для таких рішень, який включає [2]:

– вебзастосунок;
– вебсервер та сервер застосунків;
– сховище даних (сервер баз даних);
– операційну систему.

Кожен з цих компонентів може містити вразливості. При цьому, слід зауважити, що якщо розробник може впливати на безпеку вебзастосунків як йому доступні усі вихідні коди застосунку, то операційна система, сховище баз даних, вебсервер та сервер застосунків він використовує як готові рішення, що прийнято називати Component Of The Shelf (COTS), тобто такий, що розробляється сторонніми розробниками та надається «як є». Звісно, розробники операційних систем також піклуються про безпеку свого продукту та приділяють неабияку увагу цьому, але сучасні системи надто складні, що призводить до того, що виявити абсолютно усі вразливості в програмному забезпечені до випуску релізу є неможливою задачею. Розробляють систему люди, та люди можуть

помилятися та додавати дефекти в програмне забезпечення, що можуть впливати на інформаційну безпеку. Саме тому питання вивчення вразливостей є дуже важливим на сьогоднішній день.

Нині існує значна кількість урядових, міжнародних і комерційних організацій, що займаються збором інформації про вразливості програмних засобів. Інформація про ці вразливості зберігається в спеціальних, як правило, загальнодоступних базах даних і може бути використана для оцінки рівня безпеки вебсистем [3]. Приклади та коротка характеристика деяких баз даних вразливостей наведені в таблиці 1. Порівняння даних, що містяться в базах даних вразливостей, розглянуто в [4].

Таблиця 1.
Бази даних вразливостей

№ з/п	Інформаційний ресурс	Коротка характеристика	Спосіб надання інформації
1	National Vulnerability Database (NVD) http://nvd.nist.gov/	Національна база вразливостей, один із найпередовіших ресурсів вразливостей, який інтегрує всі бази вразливостей, доступні в США, та надається для безкоштовного доступу. NVD базується на інформації CVE і синхронізує всі свої поповнення зі словником CVE. Рейтинг серйозності вразливостей виставляється згідно зі стандартом CVSS.	Вебінтерфейс, XML-дампи, JSON-дампи, API
2	Common Vulnerabilities and Exposures (CVE) http://cve.mitre.org/	Підтримується корпорацією Mitre. Надається в режимі вільного доступу і фінансується урядом США. Головна мета CVE – стандартизувати імена всіх відкритих і публічно відомих вразливостей у програмних продуктах. Основне завдання – полегшити обмін даними між окремими базами вразливостей та інструментами із забезпечення інформаційної безпеки. Більшість наявних баз і ресурсів вразливостей програмних продуктів використовують CVE індекси і синхронізуються з інформацією, доступною в CVE.	Вебінтерфейс, XML-дампи
3	Open Vulnerability and Assessment Language (OVAL). http://oval.mitre.org/	Є міжнародним громадським стандартом інформаційної безпеки. OVAL містить мову, що використовується для кодування подробиць системи та перелік вмісту сховища, прийняту спільнотою. Мова стандартизує три головні оцінки процесу: подання конфігурації системи,	Вебінтерфейс

№ з/п	Інформаційний ресурс	Коротка характеристика	Спосіб надання інформації
		що тестується, аналіз системи на наявність певних станів (вразливість, конфігурація, стан «патча») і створення звіту про результати оцінки. Сховище містить загальнодоступну відкриту інформацію про використовувану мову.	
4	Computer Emergency Response Team (CERT) http://www.cert.org/	Використовувані назви: Команда комп'ютерної безпеки з реагування на інциденти (Computer Security Incident Response Team, CSIRT), або Комп'ютерна команда екстреної готовності (Computer Emergency Readiness Team) – назви експертних груп, що займаються інцидентами в комп'ютерній та інтернет-безпеці. У США групи CERT найчастіше співпрацюють з оригінальним CERT з університету Карнегі-Меллон, який служить як загальнонаціональний координаційний центр.	Вебінтерфейс
5	Secunia http://secunia.com/	Данська комерційна організація, яка надає сервіси із забезпечення інформаційної безпеки та пропонує програмні продукти для пошуку комп'ютерних вірусів і вразливостей програмних продуктів. Secunia утримує штат фахівців з безпеки, які тестують, перевіряють, контролюють та оцінюють публічні повідомлення про дефекти та вразливості. Водночас фахівці Secunia проводять і власну роботу з пошуку дефектів і прогалин у безпеці.	Вебінтерфейс

Алгоритм агрегації даних про вразливості з баз даних CVE, NVD наведено на рисунку 1.

Дане дослідження фокусується на вивченні вразливостей серверних операційних систем [5-13].

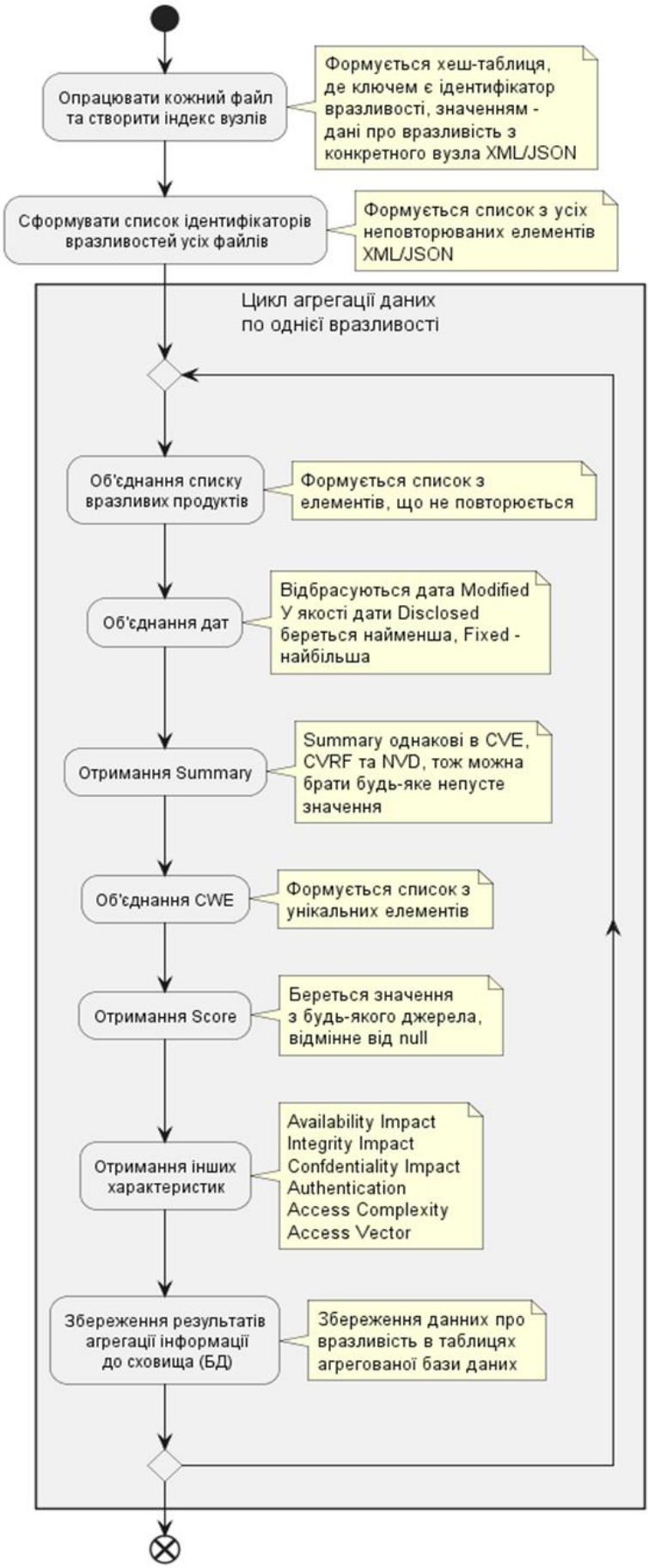

Рисунок 1 – Алгоритм агрегації даних про вразливості з різних джерел

Список літератури:

1. Баранов, О. А. (2014). Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*, 2(42), С. 54-62.

2. Gorbenko, A., Kharchenko, V., Tarasyuk, O., & Furmanov, A. (2006). F (I) MEA-technique of web services analysis and dependability ensuring. *Rigorous Development of Complex Fault-Tolerant Systems*, pp. 153-167.

3. Garcia, M., Bessani, A., Gashi, I., Neves, N., & Obelheiro, R. (2011, June). OS diversity for intrusion tolerance: Myth or reality? In 2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN) (pp. 383-394). IEEE.

4. Gorbenko, A., Romanovsky, A., Tarasyuk, O., & Biloborodov, O. (2019). From analyzing operating system vulnerabilities to designing multiversion intrusion-tolerant architectures. *IEEE Transactions on Reliability*, 69(1), pp. 22-39.

5. Гороховатський В., Творошенко І., Сидоренко Д. (2021) Класифікація зображень із використанням кластерного подання, Міжнародний науковий симпозіум «Інтелектуальні рішення-С». Обчислювальний інтелект (результати, проблеми, перспективи). Теорія прийняття рішень: праці міжн. наук. симпозіуму (Вересень 29, 2021). Київ – Ужгород, С. 44-45.

6. Кучеренко, Е. И., & Творошенко, И. С. (2010). Прикладные аспекты моделирования нечетких процессов в сложных системах. *Збірник наукових праць Харківського університету Повітряних сил*, (1), С. 127-131.

7. Кучеренко, Е. И., Филатов, В. А., Творошенко, И. С., & Байдан, Р. Н. (2005). Интеллектуальные технологии в задачах принятия решений технологических комплексов на основе нечеткой интервальной логики. *Восточно-Европейский журнал передовых технологий*, (2), С. 92-96.

8. Гороховатський В.О., Творошенко І.С. (2021) Методи інтелектуального аналізу та оброблення даних: навч. посібник. Харків: ХНУРЕ, 92 с.

9. Творошенко, І.С. (2018). Особливості застосування сучасних принципів штучного інтелекту до розробки ефективних механізмів моделювання складних систем. Science and Technology of the Present Time: Priority Development Directions of Ukraine and Poland, 118-121.

10. Daradkeh Y.I., Gorokhovatskyi V., Tvoroshenko I., & Zeghid M. (2022). Tools for fast metric data search in structural methods for image classification, IEEE Access, 10, pp. 124738-124746.

11. Gorokhovatskyi, V., Tvoroshenko, I., Kobylin, O., & Vlasenko, N. (2023). Search for visual objects by request in the form of a cluster representation for the structural image description, Advances in Electrical and Electronic Engineering, 21(1), pp. 19-27.

12. Pomazan, V., Tvoroshenko, I., & Gorokhovatskyi, V. (2023). Development of an application for recognizing emotions using convolutional neural networks, International Journal of Academic Information Systems Research, 7(7), pp. 25-36.

13. Gorokhovatskyi, V., Peredrii, O., Tvoroshenko, I., & Markov, T. (2023). Матриця відстаней для множини компонентів структурного опису як інструмент для створення класифікатора зображень, Advanced Information Systems, 7(1), С. 5-13.