Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004.056.5:004.4:005.934
DOI: 10.32447/20784643.31.2025.13

В. І. Ящук, А. І. Івануса, Н. О. Маслова, Р. Л. Ткачук, Т. Б. Брич
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
ORCID: https://orcid.org/0000-0003-2651-4918 – В. І. Ящук
https://orcid.org/0000-0001-9141-8039 – А. І. Івануса
https://orcid.org/0000-0002-9078-0973 – Н. О. Маслова
https://orcid.org/0000-0001-9137-1891 – Р. Л. Ткачук
https://orcid.org/0000-0001-6853-1981 – Т. Б. Брич
valentina.lender@gmail.com

КОНЦЕПТУАЛІЗАЦІЯ ІНТЕГРАТИВНОГО ВИКОРИСТАННЯ БАЗ ДАНИХ ВРАЗЛИВОСТЕЙ У КОНТЕКСТІ СИСТЕМНОГО МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. У статті розглянуто концептуальні засади інтегративного використання баз даних вразливостей у межах системного менеджменту інформаційної безпеки. В умовах стрімкого зростання кількості кіберзагроз та розширення цифрових поверхонь атаки для державних і корпоративних структур, особливої актуальності набуває потреба у систематичному, автоматизованому та контекстно-орієнтованому використанні у процесах забезпечення інформаційної безпеки.

Проблемою об'єкта дослідження є недостатня скоординованість між різними джерелами вразливостей, розрізненість форматів подання даних (наприклад, CVE, CWE, CVSS), відсутність механізмів пріоритезації у реальному часі, а також обмежена інтеграція баз даних вразливостей у діючі системи управління інформаційною безпекою, відповідно до вимог стандартів ISO/IEC 27001, NIST CSF та інших нормативних документів.

Методологічну основу дослідження становить логіко-структурне моделювання процесів збору, нормалізації, обробки, контекстуалізації та пріоритезації даних про вразливості з метою інтеграції їх у системи інформаційної безпеки. Запропоновано концептуальну модель, що включає джерела зовнішніх баз даних вразливостей (NVD, CVE, CISA KEV, Microsoft SUG тощо), модулі агрегації та нормалізації, блок контекстного аналізу з урахуванням загроз (Threat Intelligence), а також механізми пріоритезації з використанням метрик CVSS, EPSS, доступності експлойтів і зв'язку з критичними активами. Особливу увагу приділено інтеграції отриманих результатів в інфраструктуру інформаційної безпеки, включаючи SIEM, SOAR, CMDB, ITSM та інші компоненти.

Результати дослідження дозволяють здійснювати ефективну підтримку процесів прийняття рішень у сфері інформаційної безпеки, зменшити час реагування на критичні вразливості та підвищити загальний рівень кіберстійкості організацій. Здійснено порівняльний аналіз актуальних баз даних вразливостей за низкою критеріїв (наявність CVE-ідентифікаторів, підтримка CVSS, наявність калькуляторів ризику, інтеграційні можливості тощо), що дозволяє обґрунтувати вибір джерел для автоматизованого моніторингу та оцінювання ризиків.

Наукова новизна полягає у формалізації інтегративного підходу до використання баз даних вразливостей у системному менеджменті інформаційної безпеки, визначенні критичних вимог до таких баз з погляду автоматизації процесів інформаційної безпеки, а також у запропонованій логіко-структурній моделі, яка охоплює повний життєвий цикл управління вразливостями — від виявлення до реагування. Представлені результати можуть бути використані як основа для розроблення інформаційно-аналітичних платформ з моніторингу кіберризиків, побудови ризик-калькуляторів та засобів аудиту безпеки.

Ключові слова: інформаційна безпека, бази даних вразливостей, менеджмент інформаційної безпеки, оцінювання ризиків, інтеграція даних.

V. I. Yashchuk, A. I. Ivanusa, N. O. Maslova, R. L. Tkachuk, T. B. Brych
Lviv State University of Life Safety, Lviv, Ukraine

CONCEPTUALIZATION OF INTEGRATIVE USE OF VULNERABILITY DATABASES IN THE CONTEXT OF SYSTEM MANAGEMENT OF INFORMATION SECURITY

Abstract. The article discusses the conceptual principles of the integrative use of vulnerability databases within the framework of information security system management. In the context of the rapid growth of the number of cyber threats and the expansion of digital attack surfaces for state and corporate structures, the need for systematic, automated and context-oriented use in information security processes is becoming particularly relevant.

The research addresses the problem of the lack of coordination between different sources of vulnerabilities, the diversity of data submission formats (for example, CVE, CWE, CVSS), the lack of real-time prioritization mechanisms, as well as the limited integration of vulnerability databases into existing information security management systems in accordance with the requirements of ISO/IEC 27001, NIST CSF and other regulatory documents.

The central issue addressed by this research is the lack of coordination between different vulnerability sources, the diversity of data submission formats (e.g., CVE, CWE, CVSS), the absence of real-time prioritization mechanisms, and the limited integration of vulnerability databases into existing information security management systems, despite the requirements of ISO/IEC 27001, NIST CSF, and other regulatory documents.

The methodological basis of the study is the logical-structural modeling of the processes of collecting, normalizing, processing, contextualizing and prioritizing vulnerability data in order to integrate them into information security systems. A conceptual model is proposed that includes sources of external vulnerability databases (NVD, CVE, CISA KEV, Microsoft SUG, etc.), aggregation and normalization modules, a contextual analysis block taking into account threats (Threat Intelligence), as well as prioritization mechanisms using CVSS, EPSS metrics, exploit availability, and connection to critical assets. Particular attention is paid to integrating the obtained results into the existing information security infrastructure, including SIEM, SOAR, CMDB, ITSM, and other components.

The research results enable effective support of decision-making processes in the field of information security, reduce response time to critical vulnerabilities, and increase the overall level of cyber resilience of organizations. The research results enable effective support of decision-making processes in the field of information security, reduce response time to critical vulnerabilities, and increase the overall level of cyber resilience of organizations. A comparative analysis of current vulnerability databases was carried out according to a number of criteria (availability of CVE identifiers, CVSS support, availability of risk calculators, integration capabilities, etc.), which allows justifying the choice of sources for automated monitoring and risk assessment.

The scientific novelty lies in the formalization of an integrative approach to the use of vulnerability databases in information security system management, the identification of critical requirements for such databases in terms of automation of information security processes, as well as in the proposed logical-structural model that covers the full vulnerability management life cycle - from detection to response. The presented results can be used as a basis for the development of information and analytical platforms for monitoring cyber risks, building risk calculators and security audit tools.

Keywords: information security, vulnerability databases, information security management, risk assessment, data integration.

Вступ. У сучасних умовах зростаючої складності інформаційних систем та стрімкого розвитку кіберзагроз особливої актуальності набуває питання забезпечення системного менеджменту інформаційної безпеки (ІБ) на всіх рівнях функціонування організацій. Ключовою складовою цього процесу є своєчасне виявлення, оцінювання та нейтралізація вразливостей, які можуть бути використані порушниками для реалізації атак. У зв'язку з цим бази даних вразливостей (БДВ) – vulnerability database (VDB) виступають не лише інструментами технічного аналізу, а й критично важливими елементами стратегічного планування та управління ризиками в рамках функціонування систем менеджменту інформаційної безпеки (ІБ).

Метою дослідження є концептуалізація механізмів інтеграції баз даних вразливостей у практики системного менеджменту інформаційної безпеки з урахуванням чинних нормативно-методичних положень, сучасних технологічних підходів і практик ризик-орієнтованого управління.

Методи дослідження. Системний підхід застосовано для аналізу інформаційної безпеки як цілісної керованої системи з взаємопов'язаними компонентами — включаючи бази даних вразливостей, засоби виявлення загроз, системи реагування, політики тощо; функціонально-структурний аналіз використано для ідентифікації основних функціональних елементів баз даних вразливостей (БДВ) та їх місця в архітектурі системи менеджменту ІБ; порівняльний аналіз дав змогу порівняти найпопулярніші БДВ за критеріями повноти, актуальності, стандартизованості, інтегро-ваності тощо; метод експертного оцінювання використано для оцінки ефективності застосування БДВ у реальних умовах функціонування систем управління ІБ. Метод концептуального моделю-вання використовується для побудови логіко-структурної моделі інтеграції

БДВ у систему менеджменту ІБ, що враховує обмін даними, пріоритезацію вразливостей, контекст загроз і реагування.

Наукова новизна роботи. У межах дослідження обґрунтовано новий підхід до інтегративного використання баз даних вразливостей у системному менеджменті інформаційної безпеки. Наукова новизна полягає в розробленні логіко-структурної моделі, що забезпечує повний цикл обробки інформації про вразливості — від агрегації та нормалізації даних до контекстної оцінки загроз, пріоритезації та автоматизованого реагування. Запропонована модель передбачає інтеграцію з ключовими компонентами СУІБ, такими як SIEM, SOAR, CMDB та ITSM, з урахуванням сучасних стандартів ISO/IEC 27001 і NIST CSF. Результати роботи можуть бути використані для вдосконалення процесів управління вразливостями та підвищення рівня кіберстійкості організацій. Результати дослідження закладають методологічну основу для створення більш адаптивних та аналітично підтримуваних систем управління вразливостями в умовах динамічного кіберсередовища.

Результати досліджень. У сучасних умовах швидкого розвитку інформаційних технологій та зростання кіберзагроз, питання забезпечення безпеки інформаційних систем набувають особливої актуальності. Одним із важливих інструментів для підтримки інформаційної безпеки є бази даних вразливостей (БДВ), які дозволяють систематизувати інформацію про виявлені вразливості та давати рекомендації з їх усунення.

Наукові дослідження, присвячені оглядам баз даних вразливостей [1-11], фокусуються на різних аспектах їх розробки, оновлення та використання. Основні напрями включають методи класифікації та категоризації вразливостей, де важливим етапом є створення стандартів і класифікацій, що дають змогу систематизувати інформацію про вразливості за різними критеріями (тип вразливості, методи атаки, рівень ризику); інструменти автоматизованого виявлення вразливостей з розробленням програмного забезпечення для автоматичної перевірки наявності вразливостей у програмному забезпеченні, що інтегрується з базами даних вразливостей; аналіз ефективності захисту враховуючи оцінку ефективності заходів безпеки, рекомендованих у базах даних вразливостей, та їх вплив на рівень загрози для інформаційних систем.

Використання БДВ регулюється низкою міжнародних та національних стандартів та нормативних документів. Найважливішими з них є [12]:

– CVE (Common Vulnerabilities and Exposures). Міжнародний стандарт для ідентифікації вразливостей, що забезпечує уніфіковане найменування та опис кожної вразливості;

– NIST (Національний інститут стандартів і технологій, США). Розробляє нормативні документи щодо управління вразливостями та забезпечення кібербезпеки, зокрема стандарт NIST SP 800-53, що містить рекомендації для оцінки та зменшення ризиків вразливостей;

– ISO/IEC 27001 та ISO/IEC 27002. Міжнародні стандарти для управління інформаційною безпекою, що включають вимоги до ідентифікації, аналізу та управління вразливостями в інформаційних системах;

– GDPR (Загальний регламент захисту даних). Європейський нормативний акт, який регулює захист персональних даних та потребує регулярного оновлення безпеки інформаційних систем, включаючи виявлення та усунення вразливостей.

Системний менеджмент інформаційної безпеки (ІБ) являє собою комплексну діяльність, що охоплює процеси планування, організації, реалізації, контролю та постійного вдосконалення заходів захисту інформаційних ресурсів. У сучасних умовах стрімкого розвитку цифрових технологій, постійного зростання кількості загроз та складності інформаційних систем (ІС), виникає необхідність застосування методологічно обґрунтованих підходів до управління інформаційною безпекою. Такий підхід дозволяє забезпечити цілісність, конфіденційність, доступність та достовірність інформації, а також стале функціонування організаційних і технологічних компонентів ІС.

Одним із базових методологічних підходів до системного менеджменту ІБ є процесний підхід, який полягає в поділі управління безпекою на окремі взаємопов’язані процеси: аналіз ризиків, оцінювання вразливостей, планування заходів безпеки, їх реалізацію та моніторинг результативності. Цей підхід формалізований у низці міжнародних стандартів, зокрема, ISO/IEC 27001, ISO/IEC 27005, які визначають вимоги до побудови та підтримання системи менеджменту інформаційної безпеки (СМІБ) на основі циклу PDCA (Plan–Do–Check–Act).

Другим важливим напрямом є ризик-орієнтований підхід, у якому пріоритети в управлінні ІБ встановлюються на основі оцінки ризиків. Це дозволяє обґрунтовано розподіляти ресурси, орієнтуючись на найбільш критичні активи та загрози. Методики аналізу ризиків включають як якісні, так і кількісні моделі, наприклад, методика OCTAVE, методи оцінки за ISO/IEC 27005 або методології NIST SP 800-30.

Системний підхід передбачає розгляд ІБ як складної динамічної системи, що включає сукупність технічних, організаційних, правових,

людських та процедурних компонентів. У цьому контексті управління ІБ є міждисциплінарною задачею, яка потребує узгодженості на всіх рівнях управління організації: від стратегічного до оперативного. Системний підхід передбачає також інтеграцію ІБ в загальну систему корпоративного управління.

Стандартизований підхід ґрунтується на застосуванні нормативно-регламентуючих документів та міжнародних стандартів. Крім ISO/IEC 27000-серії, важливими є стандарти COBIT (Control Objectives for Information and Related Technologies), ITIL (Information Technology Infrastructure Library), а також NIST Framework for Improving Critical Infrastructure Cybersecurity. Ці підходи забезпечують уніфікованість термінології, методів оцінки, процедур впровадження та моніторингу систем захисту.

Комплексний підхід до управління ІБ базується на інтеграції технічних, організаційних та правових заходів у єдину узгоджену систему. Це передбачає не лише реалізацію технічних засобів захисту (наприклад, міжмережевих екранів, засобів шифрування), але й розробку політик безпеки, навчання персоналу, аудит безпеки, реагування на інциденти та забезпечення юридичної відповідальності за порушення політик ІБ.

Значущим є також адаптивний підхід, що дозволяє системі управління ІБ адаптуватися до змін зовнішнього середовища, нових загроз, технологічних оновлень і змін у законодавстві. Адаптивність досягається шляхом регулярного перегляду політик, процедур, технічних рішень, а також гнучкого управління ризиками на основі актуальної аналітичної інформації.

Таким чином, ефективне управління інформаційною безпекою потребує поєднання різних методологічних підходів, адаптованих до специфіки конкретної організації. Комбінація процесного, ризик-орієнтованого, системного, стандартизованого та адаптивного підходів дозволяє створити стійку, гнучку та ефективну систему менеджменту ІБ, здатну протистояти сучасним кіберзагрозам і забезпечити безперервність діяльності організації.

Відтак, при розробленні систем забезпечення інформаційної безпеки (ЗІ), зокрема систем моніторингу і управління безпекою інформаційних баз (СМІБ), постає необхідність оцінювання стану інформаційної безпеки (ІБ) з урахуванням відомих вразливостей у програмно-інформаційних системах (ПІС). Постає важливе питання ефективності використання відповідних баз даних вразливостей (БДВ), що відповідають певним критеріям [7], таким як наявність ідентифікаторів CVE, оцінки за шкалою CVSS, категорій за стандартом CWE, наявність CVSS-калькуляторів, ризик-калькуляторів тощо. Застосування цих критеріїв дозволить здійснити раціональний вибір серед БДВ. У зв'язку з цим, актуальним є завдання дослідження відомих баз даних вразливостей з метою визначення набору критеріїв, які дозволять ефективно використовувати ці БДВ для оцінювання стану ІБ.

Сучасні бази даних вразливостей — це централізовані платформи, які збирають, систематизують та публікують відомості про знайдені вразливості в програмному забезпеченні, апаратному забезпеченні та мережах. Вони критично важливі для фахівців з кібербезпеки, адже дозволяють швидко реагувати на нові загрози, оцінювати ризики для своїх систем; пріоритезувати оновлення і заходи з усунення вразливостей.

Автори у своєму дослідженні [1] пропонують глибокий аналіз існуючих наборів даних для виявлення вразливостей у програмному забезпеченні, обговорюючи тенденції, виклики та майбутні напрями розвитку. Підкреслюється важливість якості даних для ефективності моделей штучного інтелекту у виявленні вразливостей. Дослідження [2] зосереджене на створенні та аналізі баз даних вразливостей, специфічних для Інтернету речей (IoT), зокрема VARIoT. Автори обговорюють виклики та можливості, пов'язані з управлінням вразливостями в контексті IoT. У наукових працях [3,4] розглядаються проблеми якості даних у наборах даних для виявлення вразливостей, такі як дисбаланс даних, низьке покриття вразливостей та упереджений розподіл. Автори також пропонують практики для покращення якості даних у майбутніх дослідженнях.

На сьогодні існує широкий спектр загальнодоступних баз даних вразливостей, які піддавалися аналізу в численних наукових дослідженнях. Наприклад, у роботі [4] досліджено відкриті бази даних вразливостей, де були визначені основні поля записів вразливостей, а також переваги та недоліки розглянутих баз. Однак автори не виокремили узагальнені критерії, що дозволяють систематизувати аналіз таких баз. Інші роботи, зокрема [6-7], розглядають БДВ з точки зору наявності посилань на інші бази, можливості отримання даних у форматі XML, а також у форматах представлення вразливостей у базах. Однак, і в цих роботах не визначені чіткі критерії для порівняння та вибору БДВ.

Автори роботи [8,9] при обґрунтуванні вибору бази даних для оцінки вразливостей використовували такі критерії: повнота (ємність) — кількість виявлених вразливостей; доступність даних — наявність безкоштовного доступу до бази; зручність отримання даних — наявність інтерфейсів для доступу до даних; підтримка оцінки вразливостей за системою CVSS, при

цьому акцент робився на вразливостях, що впливають на доступність інформаційних систем.

Проте у роботах [10-12] не було чітко визначено критерії, за якими можна порівнювати різні БДВ та здійснювати їх вибір для побудови ефективних систем оцінки вразливостей у сфері ІБ, таких як системи автоматизованого оцінювання ризиків (АОР). Зважаючи на це, доцільно провести дослідження відомих баз даних вразливостей для визначення критеріїв, що дозволяють здійснити порівняльний аналіз таких баз і використовувати їх для створення систем автоматизованого оцінювання ризиків в інформаційній безпеці.

Для проведення дослідження проаналізуємо загальнодоступні БД вразливостей, серед яких:

– National Vulnerability Database;
– Open Source Vulnerabilities (OSV);
– IBM X-Force;
– US-CERT;
– CVE® List – MITRE;
– VulnDB (Risk Based Security);
– CERT Vulnerability Notes Database;
– CISA Known Exploited Vulnerabilities Catalog;
– Microsoft Security Update Guide.

Оцінювання проведемо за такими критеріями:

– Оцінка ризику / Ризик-калькулятор. Бази даних, які надають інструменти для оцінки ризику або надають оцінки ризику для кожної вразливості.

– Версії CVSS v2.0 v3.0. Підтримка обох версій стандарту CVSS для оцінки серйозності вразливості.

– Калькулятор CVSS v2.0 v3.0. Наявність калькулятора для обчислення CVSS оцінки.

– CVE Ідентифікатор. Відповідність кожній вразливості CVE-ідентифікатора.

– CWE категорія. Наявність категорії CWE, що визначає тип вразливості.

– Можливість розширення. Наявність API або інших засобів для експорту або інтеграції даних.

– Вивід критичних загроз/вразливостей. Можливість виділення чи фільтрації критичних вразливостей.

– Можливість інтеграції. Спрощена інтеграція даних з іншими системами через API або інші методи.

База National Vulnerability Database розроблена National Institute of Standards and Technology (NIST) Computer Security Division, Information Technology Laboratory за підтримки Department of Homeland Security's National Cyber Security Division. Вона є державним сховищем даних США, яке засноване на стандартах управління вразливостями. Такі дані дозволяють автоматизувати процеси управління вразливостями, вимірювати стан ІБ і визначати його відповідність. База NVD включає в себе БД контрольних списків безпеки, недоліків PIC, неправильних конфігурацій, PIC і показників впливу.

БД є репозитарієм основних стандартів управління даними вразливостей, розробленим на основі протоколу автоматизації контенту безпеки – Security Content Automation Protocol (SCAP) [13]. Існують такі компоненти SCAP: БД вразливостей безпеки – Common Vulnerabilities and Exposures (CVE); БД вразливих конфігурацій PIC – Common Configuration Enumeration (CCE); стандартна номенклатура та база імен PIC – Common Platform Enumeration (CPE); БД слабких місць – Common Weakness Enumeration (CWE); стандарт оцінки впливу вразливостей – Common Vulnerability Scoring System (CVSS); стандарт XML-специфікації контрольних листів – Extensible Configuration Checklist Description Format (XCCDF); стандарт XML-специфікації контролю станів процесів – Open Vulnerability and Assessment Language (OVAL) [13].

Крім цього застосовується такий набір інших протоколів:

– Threat Analysis Automation Protocol (TAAP) – протокол документування та спільного використання структурної інформації про загрози. Він містить такі компоненти: БД атрибутів шкідливого ПЗ – Malware Attribute Enumeration & Characterization (MAEC); БД шаблонів атак – Common Attack Pattern Enumeration & Classification (CAPEC); CPE; CWE; OVAL; CCE; CVE.

– Event Management Automation Protocol (EMAP) – протокол для звітів про події безпеки. Він має такі складові: БД записів подій – Event Expression (CEE); MAEC; CAPEC.

– Incident Tracking and Assessment Protocol (ITAP) – протокол для відстеження, документування, управління та спільного використання інформації про інциденти. Він містить такі компоненти: OVAL; CPE; CCE; CVE; CVSS; MAEC; CAPEC; CWE; CEE; формат обміну описом інциденту – Incident Object Description Exchange Format (IODEF); національна модель обміну інформацією – National Information Exchange Model (NIEM); формат обміну інформацією з кібербезпеки – Cybersecurity Information Exchange Format (CYBEX) [13].

Розглянуті протоколи, стандарти і БД NVD на практиці, наприклад, можна використовувати в таких цілях: CPE – визначення ІС підприємства; CVE – ідентифікація вразливостей; CVSS – визначення критичних вразливостей; CCE – формування найбільш захищеної конфігурації ІС; XCCDF – визначення політики захищеної

конфігурації; OVAL – оцінка відповідності системи політиці захищеної конфігурації; CWE – визначення слабких місць PIC; CAPEC – визначення атак відносно слабких місць PIC; CEE – визначення подій для реєстрації та параметрів реєстрації; ARF – об'єднання результатів оцінки; MAEC – визначення шкідливого ПЗ.

На сайті NVD доступний повний список вразливостей, які містяться в базі та упорядковані за роками та місяцями [9]. Кожна вразливість, яка вноситься в БД, описується такими параметрами [13]: унікальний CVE-ідентифікатор; дата внесення в БД; дата останньої редакції; джерело вразливості (інформації); короткий опис (огляд); результати оцінок з кожної метричної групи (МГ) CVSS.

База даних Open Source Vulnerabilities (OSV) [14] — це сучасна ініціатива, підтримувана Google і спільнотою OpenSSF (Open Source Security Foundation), яка зосереджена на виявленні, описі та розповсюдженні інформації про вразливості у відкритому програмному забезпеченні. OSV автоматизує обробку та публікацію вразливостей для багатьох популярних екосистем, зокрема npm, PyPI, Go, Maven, RubyGems, Rust тощо. В табл. 1 наведено опис характеристик бази даних OSV за визначеними критеріями.

Таблиця 1

Опис характеристик бази даних OSV

Критерій	Опис у Open Source Vulnerabilities (OSV)
Оцінка ризику / ризик-калькулятор	Безпосередній калькулятор ризику не реалізований, але в деяких записах вказані CVSS-оцінки. Оцінка здійснюється на основі версій, у яких присутня/усунута вразливість.
Версії CVSS: v2.0 / v3.0	Частково підтримуються, особливо для вразливостей, які дублюються з CVE-баз. Оцінки CVSS можуть бути присутні, але не є основним стандартом у структурі OSV.
Калькулятор CVSS v2.0 / v3.0	Власного CVSS-калькулятора OSV не надає. Для розрахунків можна скористатися зовнішніми інструментами.
CVE-ідентифікатор	OSV підтримує зв'язок з CVE — багато записів містять відповідний CVE-ID (наприклад, CVE-2022-12345), однак також існують унікальні OSV-ідентифікатори для кожного проєкту.
CWE категорія	Прямої підтримки класифікації за CWE немає. Основна увага зосереджена на даних про діапазон версій, де вразливість є/усунена, без детальної типізації причин.
Можливість розширення	Дані доступні у форматах JSON та через REST API. Підтримується інтеграція з CI/CD, менеджерами залежностей та безпековими сканерами.
Вивід критичних вразливостей	Інформація про рівень критичності часто присутня через інтеграцію з CVE або вручну задану в проєкті. Деякі записи мають CVSS-бали для пріоритезації.
Можливість інтеграції	Висока інтеграційна здатність: офіційне API, підтримка менеджерів пакетів, CI/CD інструментів. Є підтримка командного рядка (osv-scanner).

База даних дозволяє шукати вразливості за ім’ям пакета, мовою програмування, CVE-ID або переглядати вразливості для певної екосистеми.

База БД вразливостей IBM ISS (Internet Security Services) XForce [15], створена фахівцями підрозділу IBM Internet Security Systems X-Force, є однією з найбільших та авторитетних БД в галузі. Вона містить понад 30000 записів і детальний аналіз кожної відомої вразливості, виявленої з 1994 року.

Фахівці підрозділу X-Force співпрацюють з тисячами найбільших в світі компаній та державних установ, центрами аналізу і вертикального обміну інформацією (ISAC), глобальними координаційними центрами та іншими постачальниками рішень. Для доступу до БД вразливостей необхідно пройти реєстрацію на сайті IBM X-Force Exchange. Після реєстрації в рядку пошуку необхідно задати потрібну інформацію про вразливість.

IBM X-Force Exchange Vulnerability Database — це велика аналітична платформа компанії IBM, яка збирає, аналізує та поширює дані про кіберзагрози, включаючи вразливості, експлойти, шкідливе ПЗ, домени, IP-адреси та інші індикатори компрометації. Вона є однією з найавторитетніших баз даних у галузі кібер-безпеки, широко використовується фахівцями з ІБ для аналізу ризиків, формування захисних стратегій та інтеграції з SIEM і інструментами моніторингу [15]. В табл. 2 наведено опис характеристик бази даних IBM X-Force за визначеними критеріями.

Таблиця 2

Опис характеристик бази даних IBM X-Force

Критерій	IBM X-Force Exchange
Оцінка ризику / ризик-калькулятор	Платформа надає оцінку ризику для кожної вразливості у вигляді CVSS-балів та рейтингу ризику від IBM. Є власна аналітика ризику.
Версії CVSS: v2.0 / v3.0	Підтримуються обидві версії CVSS: v2.0 і v3.0, часто одночасно.
Калькулятор CVSS v2.0 / v3.0	Власного інтерактивного калькулятора не передбачено, однак CVSS-оцінки вказані. Для розрахунків рекомендується використовувати зовнішній CVSS-калькулятор.
CVE-ідентифікатор	Присутній: усі вразливості мають відповідний CVE-ID.
CWE категорія	Вказується, якщо доступно. IBM часто класифікує тип вразливості (наприклад, buffer overflow, SQLi), хоча іноді без прямого зазначення CWE.
Можливість розширення	API доступне для інтеграції, дані можуть бути експортовані. Можлива розширюваність через REST API.
Вивід критичних загроз/вразливостей	Є можливість фільтрації за рівнем критичності (Critical, High, Medium, Low).
Можливість інтеграції	Висока: платформа інтегрується з SIEM, SOAR, сторонніми сканерами, інструментами аналізу загроз. Підтримується IBM QRadar.

На сайті можна шукати вразливості за CVE, продуктом, типом загрози, вендором або ключовими словами.

US-CERT Vulnerability Notes Database — це база даних, яку підтримує United States Computer Emergency Readiness Team (US-CERT), що є частиною CISA (Cybersecurity and Infrastructure Security Agency). Цей ресурс містить опис вразливостей, їх вплив на продукти, потенційні наслідки, методи усунення, а також рекомендації щодо пом'якшення ризиків. Особливістю бази є акцент не лише на технічних деталях, але й на практичних рекомендаціях щодо реагування [16]. База даних VND записів вразливостей US-CERT належить United States Computer Emergency Readiness Team (USCERT). Вона розроблена спільно з Office of Cybersecurity and Communications (Управління кібербезпеки і комунікацій), Department of Homeland Security (Департамент внутрішньої безпеки), Software Engineering Institute (інженерний інститут ПЗ) та Carnegie Mellon University (інститут Карнегі-Мелоуна).

За аналогією з розглянутими вище БД, в VND наявні такі основні пункти опису вразливості: огляд; короткий опис; вплив; рекомендації про усунення; оцінки CVSS; в додатковій інформації вказується (якщо є) ідентифікатор CVE; дата першої публікації та оновлення. На відміну від інших БД, вразливості фіксуються із зазначенням постраждалої сторони та інформації про продавця. Також на сайті БД VND присутня можливість отримання зведених даних оцінок CVSS вразливостей. В табл. 3 наведено опис характеристик бази даних **US-CERT (Vulnerability Notes Database)** за визначеними критеріями.

Таблиця 3

Опис характеристик бази даних US-CERT (Vulnerability Notes Database)

Критерій	US-CERT Vulnerability Notes Database
Оцінка ризику / ризик-калькулятор	Вразливості описуються якісно, з поясненням впливу та серйозності, але формального ризик-калькулятора немає.
Версії CVSS: v2.0 / v3.0	Частково: іноді зазначено оцінку CVSS, однак не для всіх вразливостей. Версії CVSS не завжди вказуються.
Калькулятор CVSS v2.0 / v3.0	Не надається. Для розрахунку оцінки потрібно користуватись сторонніми інструментами, такими як калькулятор від NVD.
CVE-ідентифікатор	Так, зазначаються CVE-ідентифікатори у відповідних записах.
CWE категорія	Зазвичай не вказується. Натомість фокус робиться на описі вразливості та способах її усунення.
Можливість розширення	Дані публікуються у відкритому доступі, але API або спеціалізованих форматів для інтеграції/розширення немає.
Вивід критичних загроз/вразливостей	Вразливості позначаються якісними характеристиками (наприклад, "високий рівень ризику"), але фільтрації за CVSS чи категоріями критичності немає.
Можливість інтеграції	Обмежена. API або інтерфейси інтеграції відсутні. Дані доступні лише для ручного аналізу або парсингу веб-сторінок.

Цей ресурс дозволяє здійснювати пошук за номерами CVE, назвами продуктів або ключовими словами, а також переглядати щотижневі огляди нових вразливостей.

База даних CVE® (Common Vulnerabilities and Exposures), яка підтримується організацією MITRE, є одним із найвідоміших міжнародних стандартів для ідентифікації та класифікації публічно відомих вразливостей у програмному забезпеченні. Вона використовується у багатьох системах керування безпекою для уніфікації даних про вразливості [13]. В табл. 4 наведено опис характеристик бази даних CVE® List – MITRE за визначеними критеріями.

Таблиця 4

Опис характеристик бази даних CVE® List – MITRE

Критерій	**Опис у CVE® List – MITRE**
Оцінка ризику / ризик-калькулятор	Безпосередньо не реалізована. Оцінка ризику здійснюється через інтеграцію з NVD, що використовує CVSS.
Версії CVSS	Підтримуються CVSS v2.0 та v3.x через посилання на NVD.
Калькулятор CVSS	Надаються зовнішні посилання на калькулятори: CVSS v2, CVSS v3.
CVE-ідентифікатор	Кожна вразливість має унікальний ID формату CVE-YYYY-NNNNN.
CWE категорія	Частково присутня: вказується в записах, особливо через інтеграцію з іншими базами (напр. NVD).
Можливість розширення	Відкрита структура (JSON, XML); можна розширювати та інтегрувати в сторонні системи.
Вивід критичних вразливостей	Критичність не зазначається напряму. Використовується CVSS-бал через NVD для визначення рівня небезпеки.
Можливість інтеграції	Широка підтримка API, JSON, XML. Активно інтегрується в SIEM, сканери вразливостей, CMDB, системи керування.

База даних VulnDB, розроблена компанією Risk Based Security (нині частина Flashpoint), є однією з найповніших комерційних платформ з аналізу вразливостей. Вона охоплює понад 300 000 записів, включаючи понад 100 000 вразливостей, які не представлені в публічних базах, таких як CVE/NVD. VulnDB надає детальну технічну інформацію, оцінки ризиків, дані про експлойти, рекомендації з усунення вразливостей та підтримує інтеграцію через API [18]. В табл. 5 наведено опис характеристик бази даних VulnDB (від Risk Based Security) за визначеними критеріями.

Таблиця 5

Опис характеристик бази даних VulnDB (від Risk Based Security)

Критерій	**VulnDB (Risk Based Security / Flashpoint)**
Оцінка ризику / ризик-калькулятор	Так. VulnDB використовує власні метрики VTEM (Vulnerability Timeline and Exposure Metrics) для оцінки ризику, а також надає CVSS-бали для кожної вразливості, що дозволяє оцінити вплив та пріоритетність усунення.
Версії CVSS: v2.0 / v3.0	Підтримуються обидві версії CVSS, з акцентом на CVSS v3.x.
Калькулятор CVSS v2.0 / v3.0	VulnDB надає готові CVSS-бали для кожної вразливості, але інтерактивного калькулятора в межах платформи не передбачено. Для розрахунків рекомендується використовувати зовнішні інструменти.
CVE-ідентифікатор	Так. VulnDB відповідно мапує вразливості до CVE, а також включає додаткові вразливості, які не мають CVE-ідентифікаторів.
CWE категорія	Так. VulnDB класифікує вразливості за CWE (Common Weakness Enumeration), що дозволяє ідентифікувати типи вразливостей.
Можливість розширення	Так. VulnDB пропонує RESTful API для інтеграції з іншими системами, такими як SIEM, SOAR, та інші інструменти безпеки.
Вивід критичних загроз/ вразливостей	Так. Платформа дозволяє фільтрувати вразливості за рівнем критичності, включаючи критичні, високі, середні та низькі рівні ризику.
Можливість інтеграції	Висока. VulnDB підтримує інтеграцію з різними платформами, включаючи Splunk, Device42, та інші через API.

На сайті є можливість ознайомитися з можливостями VulnDB, отримати демонстрацію та дізнатися більше про інтеграційні можливості платформи.

База даних CERT Vulnerability Notes Database (CERT/CC VND), яку підтримує CERT Coordination Center при Carnegie Mellon University, надає детальну інформацію про вразливості програмного

забезпечення. Записи включають технічні деталі, рекомендації з усунення, списки постраждалих постачальників та іншу релевантну інформацію. Більшість нотаток є результатом приватної координації та розкриття вразливостей [19]. В табл. 6 наведено опис характеристик бази даних CERT Vulnerability Notes Database за визначеними критеріями.

Таблиця 6

Опис характеристик бази даних CERT Vulnerability Notes Database

Критерій	Опис
Оцінка ризику / ризик-калькулятор	Деякі записи містять оцінку ризику, але **формального калькулятора ризику** не надається.
Версії CVSS: v2.0 / v3.0	Інформація про **CVSS-бали** може бути присутня в окремих записах, але **не є обов'язковою** для всіх вразливостей.
Калькулятор CVSS v2.0 / v3.0	**Не надається** інтерактивний калькулятор CVSS; для розрахунків рекомендується використовувати зовнішні інструменти, такі як калькулятор від NVD.
CVE-ідентифікатор	Так, **CVE-ідентифікатори** вказуються у відповідних записах, що дозволяє легко ідентифікувати вразливості.
CWE категорія	**Не вказується**; база фокусується на описі вразливостей та рекомендаціях щодо їх усунення.
Можливість розширення	**Обмежена**; **API або спеціалізованих форматів для інтеграції/розширення** не надається.
Вивід критичних загроз/вразливостей	**Можливість фільтрації** за рівнем критичності обмежена; **фокус** робиться на якісному описі впливу та рекомендаціях.
Можливість інтеграції	**Обмежена**; **API або інтерфейси інтеграції** відсутні.

Цей ресурс дозволяє здійснювати пошук за номерами CVE, назвами продуктів або ключовими словами, а також переглядати щотижневі огляди нових вразливостей.

CISA Known Exploited Vulnerabilities Catalog (KEV) — це база даних, яку веде Агентство з кібербезпеки та безпеки інфраструктури США (CISA), і яка містить перелік відомих активно експлуатованих вразливостей (vulnerabilities). Основна мета KEV — надати організаціям список вразливостей, які потребують першочергового усунення [20]. В табл. 7 наведено опис характеристик бази даних CISA Known Exploited Vulnerabilities Catalog за визначеними критеріями.

Таблиця 7

Опис характеристик бази даних CISA Known Exploited Vulnerabilities Catalog

Критерій	Опис
Оцінка ризику / Ризик-калькулятор	KEV не дає власної оцінки ризику чи калькулятора, однак використовує дані з NVD та CVSS.
Версії CVSS	Підтримуються CVSS v2.0 та v3.0 через зв'язок з NVD (National Vulnerability Database).
Калькулятор CVSS	Не вбудований у KEV. Для оцінювання використовується офіційний калькулятор CVSS.
CVE ідентифікатор	Так. Усі вразливості мають CVE-ідентифікатори (напр. CVE-2021-34527).
CWE категорія	Не прямо вказана, але може бути визначена через CVE-дані з NVD.
Можливість розширення	Так. KEV надається у форматі CSV, JSON — легко інтегрується в SIEM, SOC, сканери.
Вивід критичних вразливостей	Так. KEV містить тільки вразливості, які **вже експлуатуються**, тобто є пріоритетними.
Можливість інтеграції	Так. API немає напряму, але можливо автоматично імпортувати CSV/JSON-файл, доступний на сайті.

Microsoft Security Update Guide (SUG) — це база даних вразливостей, яку Microsoft веде для своїх продуктів, і яка надає вичерпну інформацію про вразливості, виправлення та оновлення безпеки для продуктів Microsoft. Вона включає дані про різноманітні вразливості, які були виправлені через безпекові оновлення [21, 22]. В табл. 8 наведено опис характеристик бази даних Microsoft Security Update Guide за визначеними критеріями.

Таблиця 8

Опис характеристик бази даних Microsoft Security Update Guide

Критерій	Опис
Оцінка ризику / Ризик-калькулятор	Безпосередньо калькулятор ризику не надається, але використовуються дані з CVSS для оцінки ризику.
Версії CVSS	Підтримуються CVSS v2.0 та v3.0. Усі вразливості в базі мають оцінки CVSS, що допомагають в оцінці серйозності загрози.
Калькулятор CVSS	Для оцінювання використовуються офіційні калькулятори CVSS.
CVE ідентифікатор	Так, у кожній вразливості є CVE-ідентифікатор (наприклад, CVE-2021-34527).
CWE категорія	Надаються категорії CWE, які описують тип вразливості (наприклад, CWE-79 для XSS).
Можливість розширення	Так. Вивантаження вражливостей доступне у форматах JSON, XML, CSV — що дозволяє інтегрувати дані в інші системи.
Вивід критичних вразливостей	Так. База містить фільтри для сортування вразливостей за рівнем серйозності та за критичністю (Critical, Important тощо).
Можливість інтеграції	Так. Дані можна експортувати та інтегрувати у різноманітні системи через API або за допомогою експорту в форматах (CSV, XML, JSON).

База даних дозволяє також здійснювати фільтрацію за продуктами, типами загроз та виправленнями для певних вразливостей. Це робить її корисною для організацій, які управляють інфраструктурами Microsoft та потребують оперативного реагування на вразливості.

В табл. 9 проведено порівняльний аналіз баз даних вразливостей відповідно до визначених критеріїв.

Таблиця 9

Зведені дані дослідження баз даних вразливостей

База даних	Оцінка ризику / Ризик-калькулятор	Версії CVSS v2.0 v3.0	Калькулятор CVSS v2.0 v3.0	CVE Ідентифікатор	CWE категорія	Можливість розширення	Вивід критичних загроз / вразливостей	Можливість інтеграції
National Vulnerability Database (NVD)	-	+	+	+	+	+	-	+
Open Source Vulnerabilities (OSV)	-	+ -	-	+	-	+	+	+
IBM X-Force	+	+	-	+	+	+	+	+
US-CERT	-	+ -	-	+	-	+	+	-
CVE® List – MITRE	-	+	-	+	+ -	+	-	+
VulnDB (Risk Based Security)	+	+	+	+	+	+	+	+
CERT Vulnerability Notes Database	-	+ -	-	+	-	-	-	-
CISA Known Exploited Vulnerabilities Catalog	-	+	-	+	+ -	+	+	+
Microsoft Security Update Guide	-	+	+	+	+	+	+	+

Проведене порівняння баз даних вразливостей за формалізованими критеріями дозволило визначити функціональні можливості кожної з них та здійснити обґрунтований вибір найбільш придатних джерел для використання у системах забезпечення інформаційної безпеки. Зокрема встановлено, що хоча більшість баз підтримують стандартні атрибути безпеки — такі як CVE-ідентифікатори, CVSS-оцінки, категоризацію CWE та механізми інтеграції, — жодна з них не забезпечує повноцінної реалізації механізму оцінювання ризику у власному складі.

З урахуванням цього сформовано набір порівняльних критеріїв, за якими можна

здійснювати структуровану оцінку потенціалу баз даних у контексті їх інтеграції до систем моніторингу, аналізу та оцінювання ІБ. Отримані результати є цінними для розробників засобів управління вразливостями, зокрема систем оцінювання ризиків або ризик-калькуляторів, що потребують надійного, актуального та формалізованого джерела вхідних даних. Таким чином, дослідження закладає методичну основу для вибору та впровадження відповідних баз даних у рамках ризик-орієнтованих моделей управління кібербезпекою.

Побудуємо логіко-структурну модель інтеграції баз даних вразливостей (БДВ) у систему менеджменту інформаційної безпеки (СУІБ), яка б охоплювала обмін даними, пріоритезацію, контекст загроз та реагування, відповідно до сучасних підходів ISO/IEC 27001 та NIST CSF (рис.1). Логіко-структурна модель такої інтеграції включає кілька взаємопов'язаних компонентів. На першому рівні розташовані зовнішні джерела — провідні бази даних вразливостей, зокрема NVD, CVE (MITRE), CISA KEV, Microsoft Security Update Guide, VulnDB, IBM X-Force, CERT Vulnerability Notes тощо. Ці ресурси забезпечують доступ до даних через стандартизовані формати (API, JSON, XML, CSV) і містять ключові елементи — CVE-ідентифікатори, рейтинги CVSS, категорії CWE, відомості про експлойти та контекст використання вразливостей.

Далі інформація з різних джерел надходить до модуля агрегації та нормалізації, де здійснюється уніфікація даних, синхронізація форматів, фільтрація дублікатів і формування єдиного представлення вразливостей. На наступному етапі — в модулі контекстного аналізу — здійснюється порівняння виявлених вразливостей із внутрішніми активами організації. Тут враховується контекст загроз, актуальність експлуатації, наявність відомих методів атак, відповідність сценаріям MITRE ATT&CK та іншим джерелам threat intelligence.

Пріоритезація вразливостей виконується на основі багатофакторного підходу, що враховує оцінки CVSS (v2.0 та v3.0), ймовірність експлуатації (EPSS), доступність експлойтів, а також критичність активів, до яких прив'язана вразливість. Це дозволяє сформувати обґрунтований рейтинг ризиків і визначити першочерговість заходів реагування. Отримані результати передаються до компонентів СМІБ, таких як системи управління активами (CMDB), SIEM-платформи, SOAR-рішення та ITSM-системи. На цьому етапі можуть генеруватися автоматизовані сценарії реагування, створюватися інциденти або тікети на усунення вразливостей. Завершальний блок моделі забезпечує формування звітності, моніторинг виконання заходів та надання інформації для аудиту відповідно до вимог стандартів ISO/IEC 27001, NIST CSF та внутрішніх політик безпеки.

Загалом запропонована модель дозволяє інтегрувати різні джерела інформації про вразливості у єдиний управлінський контур, забезпечуючи безперервний моніторинг, пріоритезацію та ефективне реагування на загрози інформаційній безпеці організації.

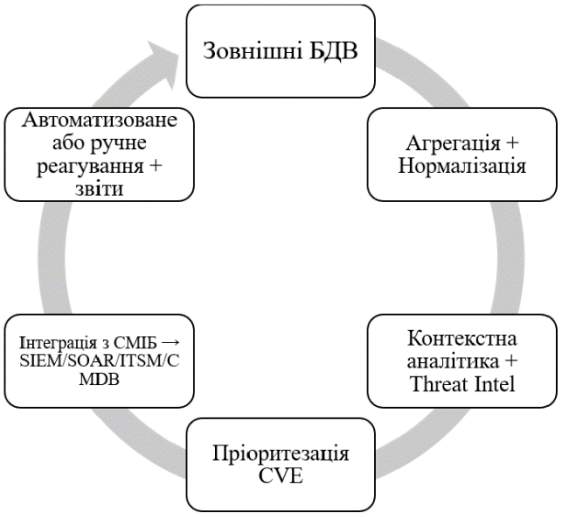

Рисунок 1 - Логіко-структурна модель інтеграції баз даних вразливостей (БДВ) у систему менеджменту інформаційної безпеки (СУІБ)

Перевагами запропонованої моделі є пріоритезація на основі реального ризику, а не лише CVSS; інтеграція з наявними процесами безпеки; підвищення швидкості реагування; повна відповідність ISO/IEC 27001 (розділ A.12/A.16) та NIST CSF (Detect → Respond → Recover). Отже,

запропонована нами модель забезпечує цілісну інтеграцію даних з баз вразливостей у процеси управління інформаційною безпекою, сприяючи підвищенню обґрунтованості прийняття рішень, оптимізації процесів реагування та дотриманню нормативно-правових вимог.

Висновки. Здійснено комплексний аналіз провідних баз даних вразливостей за низкою релевантних критеріїв, що дозволило визначити їхні функціональні можливості та обґрунтувати вибір оптимальних джерел для інтеграції в автомати-зовані процеси оцінювання ризиків інформаційної безпеки. Результати аналізу засвідчили, що жодна з розглянутих БД не забезпечує повного спектра механізмів для оцінювання ризику, однак сукупне використання кількох джерел дозволяє компенсувати їхні індивідуальні обмеження. У результаті проведеного аналізу баз даних вразливостей (HVD, CVE® List – MITRE, CISA KEV, Microsoft SUG, VulnDB, OSV, IBM X-Force, US-CERT, CERT Vulnerability Notes тощо) встановлено, що вони відіграють ключову роль у забезпеченні ефективного управління вразливостями в системах інформаційної безпеки. Більшість досліджених джерел підтримують стандартизовані механізми класифікації вразливостей (CVSS v2.0/v3.0, CWE), надають уніфіковані іденти-фікатори (CVE), а також підтримують засоби інтеграції через API або інші формати даних (CSV, JSON, XML). З огляду на зростаючі загрози в кіберпросторі, розвиток баз даних вразливостей має значний потенціал для подальшого удосконалення. Напрямом подальших досліджень є дослідження можливостей розширення інтеграції БДВ з іншими системами управління безпекою; покращення алгоритмів автоматизованого виявлення вразливостей за допомогою штучного інтелекту та машинного навчання; поглиблення співпраці між державними та приватними організаціями в сфері обміну інформацією про вразливості.

На основі проведеного аналізу запропоновано логіко-структурну модель інтеграції БДВ у систему менеджменту інформаційної безпеки, яка охоплює весь цикл обробки інформації — від збору, уніфікації та контекстуалізації даних до їхньої пріоритезації та автоматизованого реагування. Запропонований підхід сприяє підвищенню ефективності управління вразливостями, забезпечує адаптивність до динамічних загроз і відповідає вимогам сучасних стандартів у сфері інформаційної безпеки. Інтеграція таких баз даних у систему менеджменту інформаційної безпеки (СМІБ) дозволяє автоматизувати процес виявлення, оціню-вання та реагування на вразливості, що значно підвищує рівень захищеності IT-інфраструктури та відповідає вимогам сучасних стандартів (ISO/IEC 27001, NIST CSF). Таким чином, використання комплексної системи моніторингу та пріоритезації вразливостей із залученням зовнішніх БДВ є необхідною складовою ефективного управління кіберризиками на рівні організації.

Список літератури:

1. Alkinoon, M., Althebeiti, H., Alkinoon, A., Mohaisen, M., Salem, S., Mohaisen, D. (2025). Industry-Specific Vulnerability Assessment. In: Barhamgi, M., Wang, H., Wang, X. (eds) Web Information Systems Engineering – WISE 2024. WISE 2024. Lecture Notes in Computer Science, vol 15440. Springer, Singapore. doi.org/10.1007/978-981-96-0576-7_10

2. Felkner, A., Adamski, J., Koman, J., Rytel, M., Janiszewski, M., Lewandowski, P., Pachnia, R., & Nowakowski, W. (2024). Vulnerability and Attack Repository for IoT: Addressing Challenges and Opportunities in Internet of Things Vulnerability Databases. *Applied Sciences*, *14*(22), 10513. doi.org/10.3390/app142210513

3. Croft, R., Babar, M. A., & Kholoosi, M. M. (2023, May). Data quality for software vulnerability datasets. In 2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE) (pp. 121-133). IEEE.

4. KEKÜL, H., ERGEN, B., & ARSLAN, H. (2022). Comparison and analysis of software vulnerability databases. International Journal of Engineering and Manufacturing, 12(4), 1.

5. Kekül H., Ergen B., Arslan H. A new vulnerability reporting framework for software vulnerability databases // *International Journal of Education and Management Engineering*. – 2021. – Vol. 11, No. 3. – P. 11–19. – DOI: 10.5815/ijeme.2021.03.02.

6. Kobek L.P. The state of cybersecurity in Mexico: an overview. – Washington: *Wilson Centre's Mexico Institute*, 2017. – Jan.

7. Ruohonen J. A look at the time delays in CVSS vulnerability scoring // *Applied Computing and Informatics*. – 2019. – Vol. 15, No. 2. – P. 129–135. – DOI: 10.1016/j.aci.2017.12.002.

8. Kekül H., Ergen B., Arslan H. Comparison and analysis of software vulnerability databases // *International Journal of Engineering and Manufacturing (IJEM)*. – 2022. – Vol. 12, No. 4. – P. 1–14. – DOI: 10.5815/ijem.2022.04.01.

9. Kekül H., Ergen B., Arslan H. A multiclass hybrid approach to estimating software vulnerability vectors and severity score // *Journal of Information*

Security and Applications. – 2021. – Vol. 63. – Article ID 103028. – DOI: 10.1016/j.jisa.2021. 103028.

10. Moore T.W., Probst C.W., Rannenberg K., van Eeten M. Assessing ICT security risks in socio-technical systems (Dagstuhl Seminar 16461) // *Dagstuhl Reports*. – 2017. – Vol. 6, No. 11. – P. 63–89. – DOI: 10.4230/DagRep.6.11.63.

11. Theisen C., Williams L. Better together: comparing vulnerability prediction models // *Information and Software Technology*. – 2020. – Vol. 119. – Article ID 106204. – DOI: 10.1016/j.infsof. 2019.106204.

12. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT): ДСТУ ISO/IEC 27001:2015. – Київ: ДП «УкрНДНЦ», 2016. – 28 с.

13. National Vulnerability Database [Електронний ресурс] // National Institute of Standards and Technology, Gaithersburg, 2016. – Режим доступу: https://nvd.nist.gov/home.cfm.

14. OSV (Open Source Vulnerabilities) [Електронний ресурс]. – Режим доступу: https://osv.dev.

15. IBM X-Force Exchange [Електронний ресурс]. – Режим доступу: exchange.xforce.ibmcloud.com.

16. US-CERT (Vulnerability Notes Database) [Електронний ресурс]. – Режим доступу: https://www.kb.cert.org/vuls.

17. CVE® List – MITRE [Електронний ресурс]. – Bedford: MITRE, 2016. – Режим доступу: http://cwe.mitre.org/index.html.

18. VulnDB [Електронний ресурс]. – Режим доступу: flashpoint.io/ignite/vulnerability-intelligence/.

19. CERT Vulnerability Notes Database [Електронний ресурс]. – Режим доступу: https://www.kb.cert.org/vuls.

20. CISA Known Exploited Vulnerabilities Catalog [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.csv.

21. Microsoft Security Update Guide [Електронний ресурс]. – Режим доступу: https://msrc.microsoft.com/update-guide/.

22. Доступ до вразливостей та оновлень Microsoft Security [Електронний ресурс]. – Режим доступу: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory.

References:

1. Alkinoon, M., Althebeiti, H., Alkinoon, A., Mohaisen, M., Salem, S., Mohaisen, D. (2025). Industry-Specific Vulnerability Assessment. In: Barhamgi, M., Wang, H., Wang, X. (eds) Web Information Systems Engineering – WISE 2024. WISE 2024. Lecture Notes in Computer Science, vol 15440. Springer, Singapore. https://doi.org/10.1007/978-981-96-0576-7_10

2. Felkner, A., Adamski, J., Koman, J., Rytel, M., Janiszewski, M., Lewandowski, P., Pachnia, R., & Nowakowski, W. (2024). Vulnerability and Attack Repository for IoT: Addressing Challenges and Opportunities in Internet of Things Vulnerability Databases. *Applied Sciences*, *14*(22), 10513. https://doi.org/10.3390/app142210513

3. Croft, R., Babar, M. A., & Kholoosi, M. M. (2023, May). Data quality for software vulnerability datasets. In 2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE) (pp. 121-133). IEEE.

4. KEKÜL, H., ERGEN, B., & ARSLAN, H. (2022). Comparison and analysis of software vulnerability databases. International Journal of Engineering and Manufacturing, 12(4), 1.

5. Kekül, H., Ergen, B., & Arslan, H. (2021). A new vulnerability reporting framework for software vulnerability databases. *International Journal of Education and Management Engineering*, *11*(3), 11–19. https://doi.org/10.5815/ijeme.2021.03.02

6. Kobek, L. P. (2017, January). *The state of cybersecurity in Mexico: An overview*. Wilson Centre's Mexico Institute.

7. Ruohonen, J. (2019). A look at the time delays in CVSS vulnerability scoring. *Applied Computing and Informatics*, *15*(2), 129–135. https://doi.org/10.1016/j.aci.2017.12.002

8. Kekül, H., Ergen, B., & Arslan, H. (2022). Comparison and analysis of software vulnerability databases. *International Journal of Engineering and Manufacturing (IJEM)*, *12*(4), 1–14. doi.org/10.5815/ijem.2022.04.01

9. Ergen, B., Kekül, H., & Arslan, H. (2021). A multiclass hybrid approach to estimating software vulnerability vectors and severity score. *Journal of Information Security and Applications*, *63*, 103028. https://doi.org/10.1016/j.jisa.2021.103028

10. Moore, T. W., Probst, C. W., Rannenberg, K., & van Eeten, M. (2017). Assessing ICT security risks in socio-technical systems (Dagstuhl Seminar 16461). *Dagstuhl Reports*, *6*(11), 63–89. https://doi.org/10.4230/DagRep.6.11.63

11. Theisen, C., & Williams, L. (2020). Better together: Comparing vulnerability prediction models. *Information and Software Technology*, *119*, 106204. https://doi.org/10.1016/j.infsof.2019.106204

12. Metody zakhystu systemy upravlinnia informatsiinoiu bezpekoiu. Vymohy (ISO/IEC 27001:2013; Cor 1:2014, IDT): DSTU ISO/IEC 27001:2015. (2016). Kyiv: DP "UkrNDNTs".National Institute of Standards and Technology. (2016).

13. *National Vulnerability Database* [Online]. https://nvd.nist.gov/home.cfm

14. Open Source Vulnerabilities. (n.d.). *OSV database* [Online]. https://osv.dev

15. IBM. (n.d.). *IBM X-Force Exchange* [Online]. https://exchange.xforce.ibmcloud.com

16. CERT Coordination Center. (n.d.). *US-CERT Vulnerability Notes Database* [Online]. kb.cert.org/vuls

17. MITRE. (2016). *CVE® List* [Online]. http://cwe.mitre.org/index.html

18. Flashpoint. (n.d.). *VulnDB* [Online]. https://flashpoint.io/ignite/vulnerability-intelligence/

19. CERT Coordination Center. (n.d.). *CERT Vulnerability Notes Database* [Online]. https://www.kb.cert.org/vuls

20. Cybersecurity and Infrastructure Security Agency. (n.d.). *Known Exploited Vulnerabilities Catalog* [CSV file]. www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.csv

21. Microsoft. (n.d.). *Microsoft Security Update Guide* [Online]. microsoft.com/ update-guide/

22. Microsoft. (n.d.). *Security guidance and updates portal* [Online]. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory

Оглядова стаття.
Надійшла до редакції 07.05.2025.
Прийнято до публікації 04.06.2025.