INTEGRATION OF VULNERABILITY DATABASES INTO ISMS – A PATH TO ENHANCING CYBER RESILIENCE OF CRITICAL SYSTEMS

Valentina Yashchuk, Andriy Ivanusa, Nataliya Maslova, Rostyslav Tkachuk, Taras Brych

ІНТЕГРАЦІЯ БАЗ ДАНИХ ВРАЗЛИВОСТЕЙ У СУІБ – ШЛЯХ ДО ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНИХ СИСТЕМ

Ящук В.І., Івануса А.І., Маслова Н.О., Ткачук Р.Л., Брич Т.Б.
Львівський державний університет безпеки життєдіяльності
(Україна)

Анотація. У роботі запропоновано логіко-структурну модель інтеграції баз даних вразливостей (БДВ) у систему управління інформаційною безпекою (СУІБ) з метою підвищення кіберстійкості критичних інформаційно-технічних систем. Модель охоплює ключові етапи: агрегацію та нормалізацію даних, контекстуалізацію вразливостей, пріоритезацію ризиків, інтеграцію з системами реагування та адаптивний моніторинг. У межах дослідження конкретизовано вимоги до джерел вразливостей, визначено їх роль у підтримці процесів оцінки та зменшення ризиків, а також обґрунтовано практичну доцільність використання комбінованого підходу до інтеграції даних у критичних системах. Результати спрямовані на вдосконалення механізмів автоматизованого реагування в СУІБ та забезпечення стійкої роботи критичної IT-інфраструктури в умовах зростаючих кіберзагроз.

Вступ. У сучасному цифровому світі інформаційні технології є фундаментальним елементом функціонування державних, комерційних та соціальних структур. Проте їхнє широке впровадження супроводжується стрімким зростанням кіберзагроз, які можуть спричинити критичні наслідки для національної безпеки та економічної стабільності. Серед найуразливіших об’єктів – критична інфраструктура, що включає енергетичні комплекси, транспортні системи, комунікаційні мережі та державні інформаційні ресурси.

Кіберзагрози можуть не лише порушити роботу таких систем, але й призвести до масштабних аварій, втрати конфіденційних даних та порушення економічної рівноваги. Вразливості, які накопичуються в інформаційних системах, є основними точками доступу для зловмисників, ігнорування або несвоєчасна реакція на них підвищує ризик атак.

Зважаючи на це, питання інтеграції актуальних даних про вразливості у систему управління інформаційною безпекою критичних об'єктів набуває стратегічного значення. Це дозволяє забезпечити своєчасну ідентифікацію загроз, динамічну оцінку ризиків та автоматизоване реагування на потенційні атаки. Важливим аспектом є використання сучасних баз даних вразливостей, які містять стандартизовану інформацію про відомі загрози й можливі сценарії їх експлуатації.

Таким чином, ефективне управління інформаційною безпекою критичних систем має базуватися на комплексному підході, який включає аналіз, моніторинг і автоматизоване реагування на кіберзагрози. Запропонована концептуальна модель інтеграції даних з баз вразливостей у процеси оцінювання ризиків та управління загрозами покликана не лише

покращити захисні механізми, але й сприяти впровадженню адаптивних та стандартизованих рішень у сфері інформаційної безпеки.

Актуальність досліджень. У сучасних умовах цифровізації критичної інфраструктури головною проблемою є зростання кількості вразливостей, недостатній рівень автоматизації в їхньому виявленні та обмежена здатність оперативно оцінити рівень ризику. Стандарти ISO/IEC 27001 та NIST CSF регламентують підхід до управління вразливостями, проте не дають детального опису інтеграції із зовнішніми джерелами. Згідно з даними IBM X-Force чи ENISA, понад 60% успішних атак на критичну інфраструктуру реалізуються через невчасно виявлені відомі вразливості. Це створює потребу у концептуальних моделях, що дозволяють формалізувати процеси збору, нормалізації, пріоритезації й реагування на вразливості в межах критичних систем.

Постановка задачі. Метою роботи є розроблення структурної моделі для інтеграції даних баз вразливостей у процеси моделювання, діагностики та управління ризиками критичних систем. Основні завдання:

- визначити (уточнити) джерела релевантних даних про вразливості;
- побудувати модель, що охоплює етапи від збору даних до автоматизованого реагування;
- обґрунтувати застосування моделі в системах моніторингу та безпеки критичних об’єктів.

Методологія досліджень. Системне управління інформаційною безпекою охоплює весь життєвий цикл захисту інформаційних ресурсів організації – від планування і реалізації до постійного контролю та вдосконалення засобів захисту. Такий підхід базується на інтеграції кількох взаємодоповнюючих методологій.

Процесний підхід дозволяє структурувати управління інформаційною безпекою як набір взаємопов’язаних процедур: ідентифікацію ризиків, аналіз і класифікацію вразливостей, планування захисних заходів, їх впровадження та подальший моніторинг. Це забезпечує формалізацію рішень та послідовність дій у рамках системи.

Ризик-орієнтований підхід ставить у центр уваги оцінювання ризиків, дозволяючи пріоритезувати ресурси для захисту найбільш критичних активів і зосередитись на найнебезпечніших векторах атак. Така модель особливо важлива для критичних інформаційно-технічних систем, де навіть незначна вразливість може спричинити масштабні наслідки.

Стандартизований підхід забезпечує відповідність сучасним міжнародним нормам: ISO/IEC 27001, ISO/IEC 27005, NIST CSF, COBIT, ITIL. Ці стандарти надають уніфіковані вимоги до процесів виявлення, класифікації та обробки вразливостей, а також описують вимоги до політик, процедур і технічних рішень.

Адаптивний підхід дає змогу системі безпеки швидко реагувати на зміни – нові кіберзагрози, вразливості, оновлення нормативної бази чи зміну архітектури інформаційної системи. Така гнучкість забезпечується регулярним переглядом стратегій, процедур і технологій, а також впровадженням динамічного аналізу ризиків.

Таким чином, ефективне управління інформаційною безпекою вимагає 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.

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.

Наукові дослідження, присвячені оглядам баз даних вразливостей [1-6], 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 дозволяють 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.

На попередньому етапі дослідження [7] авторами було проведено детальний порівняльний аналіз провідних баз даних вразливостей з акцентом на їх функціональні характеристики, що мають значення для автоматизованої інтеграції в процеси оцінювання ризиків. Розглядалися джерела, зокрема NVD, CVE® (MITRE), CISA KEV, Microsoft SUG, VulnDB, OSV, IBM X-Force, CERT тощо. Аналіз охоплював такі ключові параметри, як підтримка стандартів CVE, CVSS, CWE, наявність відкритих інтерфейсів API, формати експорту (CSV, JSON, XML), а також потенціал для інтеграції з СУІБ.

Результати засвідчили, що жодна з окремих баз даних не є універсальною з погляду повного охоплення критично важливих функцій оцінки ризику. Проте комбіноване використання кількох джерел дає змогу компенсувати обмеження кожного окремо взятого ресурсу, підвищити точність і повноту діагностики та покращити ефективність реагування.

Ці напрацювання стали підґрунтям для формування структурної моделі інтегрованої системи, запропонованої в даних тезах. У ній реалізовано послідовну інтеграцію даних із зовнішніх БДВ на всіх етапах: від агрегації та нормалізації до пріоритезації ризиків та автоматизованого реагування. Таким чином, запропонована модель не лише продовжує попередню концепцію, а й формує практичний механізм реалізації управління вразливостями в критичних IT-системах.

Результати досліджень - побудова інтегрованої системи. Ключові компоненти інтегрованої системи, наведеною на рисунку 1 є:

- агрегація та нормалізація: об'єднання даних з кількох баз даних (CVE, CVSS, CWE) у єдиному форматі для подальшої обробки;
- контекстуалізація: зіставлення вразливостей з активами IT-інфраструктури організації (на основі CMDB, ITSM) з урахуванням їх критичності;
- пріоритизація ризиків: застосування систем оцінки - CVSS (v2.0/v3.0), EPSS, наявність експлойтів, тип вразливості тощо;
- інтеграція з СУІБ: передача даних на платформи SIEM, SOAR, IRP або ITSM для автоматичного реагування та створення інцидентів;
- моніторинг та адаптація: постійне оновлення моделей реагування, аналітики та політик захисту відповідно до змін у середовищі.

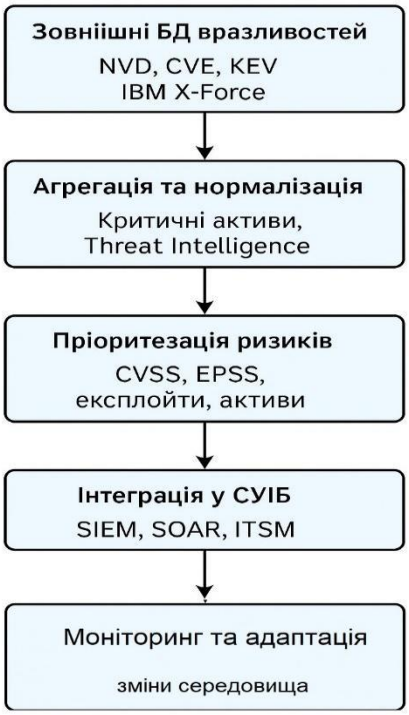

Рисунок 1 – Структура інтегрованої системи управління ризиками

В цьому дослідженні, на відміну від попередньої роботи авторів [7], в узагальненому переліку компонентів інтегрованої системи не застосовується база CERT. Причиною цього є те, що база CERT не має широких можливостей інтеграції через API чи у форматах JSON/XML, як інші (NVD, VulnDB, Microsoft SUG, OSV тощо). Її контент публікується у вигляді нотаток, орієнтованих переважно на читання людиною, а не на машинну обробку. Тобто, для автоматизованої, масштабованої побудови інтегрованої системи управління ризиками CERT має обмежене практичне застосування з точки зору моніторингу в режимі реального часу.

Особливістю моделі є її здатність адаптуватися до змін середовища загроз, підтримувати автоматизовану діагностику та скорочувати час реагування на критичні вразливості, що особливо важливо для безперервного функціонування критичних систем. Тож у структурі концептуальної моделі інтеграції, що описується в тезах, акцент зроблено на технічно зручних, стандартизованих джерелах, які дозволяють реалізувати повний цикл: виявлення – пріоритезація – реагування.

Використання сучасних баз даних вразливостей у рамках такої системи дозволяє:

- оперативно виявляти вразливості в цифровій інфраструктурі;
- скорочувати час реагування на критичні інциденти;
- оптимізувати витрати, зосереджуючись на найважливіших ризиках;
- автоматизувати аудити безпеки;
- дотримуватися міжнародних вимог та стандартів.

Тому поєднання процесних, ризик-орієнтованих, адаптивних та стандартизованих підходів є основою надійної, динамічної та масштабованої системи управління інформаційною безпекою, що особливо важливо для захисту об'єктів інфраструктури стратегічного значення.

Наукова новизна дослідження полягає у запропонованій структурній моделі інтеграції даних про вразливості з різних баз у систему управління інформаційною безпекою

критичних об’єктів, що забезпечує автоматизацію процесів оцінювання ризиків та реагування на загрози, адаптивність до змін кіберсередовища та відповідність сучасним міжнародним стандартам, що дозволяє оптимізувати кіберзахист стратегічних інформаційних систем.

Запропонована концептуальна модель інтеграції баз даних вразливостей може бути впроваджена у складі автоматизованих систем моніторингу й управління інформаційною безпекою критичних об’єктів інфраструктури, таких як енергетичні комплекси, транспортні вузли або державні інформаційні системи.

Практична реалізація моделі повинна включати етапи:

- підключення джерел вразливостей (наприклад, NVD, VulnDB, OSV) до системи збору подій через API або завантаження в уніфікованому форматі JSON/XML;
- агрегацію й обробку інформації засобами серверного модуля, який нормалізує дані, додає оцінки ризику (CVSS, EPSS) і позначає наявність експлойтів;
- контекстуалізацію отриманих вразливостей через співставлення їх із активами організації в CMDB, що дозволяє визначити критичність впливу кожної вразливості;
- передача результатів аналізу до систем SIEM або SOAR, які формують автоматизовані playbook’и реагування: блокування мережевої активності, створення інцидентів, сповіщення адміністратора;
- моніторинг виконання заходів та повторне оцінювання залишкового ризику, що дозволяє циклічно вдосконалювати політику захисту в реальному часі.

У рамках такої інтеграції модель не лише підтримує ухвалення рішень, а й дозволяє автоматизувати дії з нейтралізації загроз, що суттєво знижує час реагування та людський фактор. Завдяки використанню стандартизованих структур даних (CVE, CWE, CVSS) і відкритих протоколів, запропоноване рішення може бути легко адаптоване до різних архітектур IT-інфраструктури.

Висновки. У роботі розглянуто концептуальний підхід до побудови інтегрованої системи моделювання та управління ризиками в критичних інформаційно-технічних системах шляхом використання баз даних вразливостей. У межах дослідження було досягнуто такі результати:

- уточнено джерела релевантних даних про вразливості, зокрема NVD, CVE, CISA KEV, IBM X-Force, VulnDB, OSV, що містять стандартизовану інформацію, придатну для автоматизованого аналізу та інтеграції відмічено, що в узагальненому переліку компонентів інтегрованої системи не застосовується база CERT, як така, яка не має широких можливостей інтеграції через API чи у форматах JSON/XML;

- розроблено структурну модель, яка охоплює ключові етапи: агрегацію даних, їх нормалізацію, контекстуалізацію, пріоритезацію ризиків, інтеграцію у системи ISMS, SIEM, SOAR, а також адаптивне оновлення політик безпеки;

- обґрунтовано застосування моделі в системах моніторингу та захисту критичних об’єктів, зокрема в енергетичних, транспортних та державних IT-інфраструктурах, де необхідне своєчасне реагування на вразливості для забезпечення безперервності функціонування.

Запропонована система дозволяє підвищити ефективність управління ризиками, зменшити час реагування на загрози, оптимізувати ресурси та відповідати міжнародним стандартам безпеки. Модель забезпечує цілісний цикл обробки інформації: від збору до автоматизованого реагування, відповідає міжнародним стандартам та адаптована до

інтеграції в інфраструктуру об’єктів критичної інфраструктури. Її впровадження є актуальним кроком до забезпечення кіберстійкості критичних об'єктів інфраструктури.

ЛІТЕРАТУРА

1. 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.
2. 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
3. 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
4. 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.
5. KEKÜL, H., ERGEN, B., & ARSLAN, H. (2022). Comparison and analysis of software vulnerability databases. International Journal of Engineering and Manufacturing, 12(4), 1.
6. 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.
7. Ящук В.І., Івануса А.І., Маслова Н.О., Ткачук Р.Л., Брич Т.Б. Концептуалізація інтегративного використання баз даних вразливостей у контексті системного менеджменту інформаційної безпеки // *Вісник Львівського державного університету безпеки життєдіяльності*. – 2025. – Т. 31. – С. 59–61