Метод оцінювання стану інформаційної безпеки елементів кіберфізичних систем

Наталія Петляк[1], Артем Барабаш[1]

[1] *Хмельницький національний університет, вул. Інститутська 11, 29016 Хмельницький, Україна*

Анотація

У роботі розглянуто проблему забезпечення інформаційної безпеки кіберфізичних систем, які поєднують обчислювальні ресурси з фізичними процесами. З огляду на складність їхньої структури та високу інтегрованість у критичну інфраструктуру, виникає потреба у створенні методів комплексного оцінювання рівня захищеності. Запропоновано метод оцінювання стану інформаційної безпеки елементів кіберфізичних систем, який базується на формалізації параметрів захищеності, урахуванні їхніх вагових коефіцієнтів та багаторівневому аналізі ризиків. Проведені дослідження підтвердили ефективність застосування методу для виявлення критичних вразливостей, пріоритезації заходів безпеки та підтримки процесів управління кіберзахистом.

Ключові слова

інформаційна безпека, кіберфізичні системи, оцінювання ризиків, рівень захищеності, методи аналізу

1. Вступ

Кіберфізичні системи, що інтегрують апаратні пристрої, програмні комплекси, сенсорні мережі та засоби зв'язку, сьогодні стають ключовим компонентом у промисловості, енергетиці, транспорті та інших галузях. Вони функціонують у тісному зв'язку між цифровим і фізичним середовищем, що робить їх особливо вразливими до кіберзагроз. Атаки на елементи таких систем можуть спричинити серйозні наслідки не лише для інформаційної інфраструктури, а й для фізичної безпеки людей і технологічних процесів.

Проблема ускладнюється тим, що традиційні методи захисту інформаційних систем часто виявляються недостатньо ефективними у випадку кіберфізичних систем. Це пов'язано з їх розподіленим характером, високою гетерогенністю, а також взаємозалежністю окремих компонентів. У такому середовищі зростає роль методів оцінювання стану захищеності, які дозволяють не лише виявити наявність загроз, але й визначити рівень ризику для кожного елементу та всієї системи загалом.

2. Аналіз досліджень та публікацій

Актуальні дослідження свідчать, що основні підходи до оцінювання рівня інформаційної безпеки базуються на трьох групах методів: сигнатурному аналізі, поведінковому моніторингу та оцінюванні ризиків [1-2]. Сигнатурні методи дозволяють швидко виявляти відомі загрози, однак вони малоефективні проти нових або модифікованих атак [3-4]. Поведінковий аналіз орієнтується на пошук аномалій у функціонуванні системи, проте вимагає значних обчислювальних ресурсів і може призводити до помилкових спрацювань [5]. Методи оцінювання ризиків, у свою чергу, надають більш комплексний

[1] Corresponding authors

npetlyak@khmnu.edu.ua (Н. Петляк); abarabash@khmnu.edu.ua (А. Барабаш)

0000-0001-5971-4428 (Н. Петляк)

підхід, оскільки враховують можливість реалізації загроз, вразливості елементів системи та потенційний вплив на функціонування критичних процесів [6].

Останнім часом активно розробляються моделі оцінювання стану кіберфізичних систем на основі багатофакторного аналізу. У таких підходах використовуються формалізовані метрики, які характеризують ступінь захищеності кожного компонента. Це дозволяє визначати найбільш критичні елементи системи та концентрувати ресурси на їх захисті. Попри значні досягнення, залишається проблема уніфікації методів оцінювання, що мають враховувати специфіку кіберфізичних систем та їхню тісну інтеграцію з фізичними процесами.

3. Метод оцінювання стану інформаційної безпеки

Запропонований метод оцінювання стану інформаційної безпеки елементів кіберфізичних систем передбачає багаторівневу процедуру аналізу, що поєднує якісні та кількісні підходи. На першому рівні здійснюється ідентифікація ключових елементів системи, серед яких можуть бути контролери, сенсорні вузли, мережеві комутатори, сервери управління та інші компоненти. Для кожного елемента визначаються критичні параметри інформаційної безпеки, такі як цілісність даних, конфіденційність, доступність, автентичність і відмовостійкість. Далі вводиться система вагових коефіцієнтів, яка відображає відносну важливість кожного параметра для безперервного функціонування системи. Наприклад, для сенсорної мережі найважливішим може бути параметр цілісності даних, тоді як для серверів управління визначальним буде рівень доступності. Вагові коефіцієнти встановлюються експертним шляхом або на основі статистичних даних щодо ймовірності реалізації загроз і наслідків інцидентів. Після цього здійснюється збір фактичних даних про поточний стан елементів системи. Він може включати результати сканування вразливостей, журнали подій, дані систем моніторингу трафіку та інші джерела. Отримані показники зіставляються із заданими еталонними значеннями, що дозволяє обчислити рівень відповідності фактичного стану заданим критеріям. Для цього використовується нормалізована шкала, яка переводить усі параметри у єдиний діапазон від нуля до одиниці. Загальний рівень захищеності елемента визначається як зважена сума його параметрів з урахуванням вагових коефіцієнтів. Це дозволяє відобразити як відносну важливість кожного параметра, так і його поточний стан. Формально рівень захищеності можна подати як інтегральний показник, що є результатом агрегування окремих метрик.

На наступному етапі проводиться аналіз ризиків. Він передбачає визначення ймовірності реалізації конкретних загроз для кожного елемента та оцінку можливих наслідків їх впливу. Для цього використовується модель ризику, де підсумковий показник обчислюється як добуток імовірності загрози на рівень вразливості та значущість наслідків. Такий підхід дозволяє ранжувати елементи за рівнем ризику і виділяти найбільш критичні компоненти, які потребують першочергового захисту. Особливістю методу є можливість його застосування як у статичному, так і в динамічному режимі. У статичному режимі аналіз проводиться періодично на основі накопичених даних. У динамічному режимі метод інтегрується з системами моніторингу та забезпечує безперервне оновлення показників захищеності у реальному часі.

Ще одним важливим аспектом є адаптивність методу. Вагові коефіцієнти та порогові значення можуть змінюватися залежно від умов експлуатації системи та появи нових загроз. Завдяки цьому метод не є статичним, а може підлаштовуватися під актуальну ситуацію, що підвищує його практичну цінність.

У межах проведеного дослідження було розроблено та реалізовано програмний прототип інформаційної системи оцінювання, який забезпечує практичне застосування запропонованого методу. Даний прототип орієнтований на автоматизацію збору даних із різних джерел, зокрема систем моніторингу мережевого трафіку, журналів подій, засобів контролю доступу та результатів сканування вразливостей. Отримана інформація підлягає

попередній обробці, що передбачає нормалізацію параметрів, усунення шумів та приведення показників до єдиного формату, після чого здійснюється розрахунок інтегральних індексів стану інформаційної безпеки для окремих елементів системи. Розраховані значення дозволяють визначати ступінь відповідності кожного елемента заданим критеріям безпеки та формувати узагальнену оцінку, яка відображає загальний стан захищеності кіберфізичної системи.

Важливою особливістю прототипу є можливість наочного представлення результатів у вигляді звітів та графічних візуалізацій. Такий підхід не лише полегшує сприйняття отриманих даних, але й дає адміністраторам змогу швидко ідентифікувати вразливі компоненти, оцінити рівень ризиків і своєчасно прийняти рішення щодо реалізації захисних заходів. Використання інтегрального індексу дозволяє порівнювати між собою різні елементи системи, визначати найбільш критичні з них і здійснювати пріоритезацію у розподілі ресурсів для забезпечення захисту. Таким чином, запропонований метод функціонує як комплексний інструмент, що об'єднує кількісні розрахунки, експертні оцінки та інтегрований аналіз ризиків, забезпечуючи формування цілісної та багатовимірної картини стану інформаційної безпеки кіберфізичної системи. Його практичне застосування дозволяє виявляти потенційно небезпечні тенденції, прогнозувати розвиток загроз, а також реалізовувати адаптивне управління ресурсами захисту.

Наукова новизна розробленого підходу полягає у поєднанні вагового моделювання параметрів захищеності з інтегрованим ризик-орієнтованим аналізом та впровадженням механізму динамічного оновлення показників у режимі реального часу. Це забезпечує гнучкість і адаптивність системи, дозволяє формувати інтегральний індекс стану безпеки елементів кіберфізичної системи, що суттєво підвищує точність визначення найбільш критичних компонентів та ефективність пріоритезації захисних заходів. У результаті метод можна розглядати як універсальне рішення, здатне масштабуватися залежно від архітектури системи та рівня її інтегрованості у критичну інфраструктуру.

4. Висновки

Запропонований метод оцінювання стану інформаційної безпеки елементів кіберфізичних систем забезпечує комплексний підхід до аналізу рівня захищеності. Його особливістю є врахування вагових коефіцієнтів параметрів, інтеграція з аналізом ризиків та можливість застосування у динамічному режимі. Метод дозволяє визначати критичні елементи системи, пріоритезувати заходи кіберзахисту та формувати інтегральний індекс стану безпеки. Подальші дослідження планується спрямувати на оптимізацію програмної реалізації методу та його апробацію у реальних промислових кіберфізичних системах.

Література

[1] S. C. Phillips, S. Taylor, M. Boniface, S. Modafferi, M. Surridge, Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems, IEEE Access 12 (2024) 82482–82505. doi:10.1109/ACCESS.2024.3404264.

[2] A. Akbarzadeh, S. K. Katsikas, Dependency-based security risk assessment for cyber-physical systems, Int. J. Inf. Secur. 22 (2023) 563–578. doi:10.1007/s10207-022-00608-4.

[3] [3] D. A. Moskvin, Assessing the Security of a Cyber-Physical System Based on an Analysis of Malware Signatures, Aut. Control Comp. Sci. 57 (2023) 894–903. doi:10.3103/S0146411623080175.

[4] S. Y. Hilgurt, A. M. Davydenko, T. V. Matovka, M. P. Prygara, Tools for Analyzing Signature-Based Hardware Solutions for Cyber Security Systems, Journal of Cyber Security and Mobility 12 (3) (2023) 339–366. doi:10.13052/jcsm2245-1439.1235.

[5] H. Gong, R. Li, J. An, G. Xie, Reliability Modeling and Assessment for a Cyber-Physical System With a Complex Boundary Behavior, IEEE Transactions on Reliability 72 (1) (2023) 224–239. doi:10.1109/TR.2022.3160460.

[6] S. Deng, J. Zhang, D. Wu, Y. He, X. Xie, X. Wu, A Quantitative Risk Assessment Model for Distribution Cyber-Physical System Under Cyberattack, IEEE Transactions on Industrial Informatics 19 (3) (2023) 2899–2908. doi:10.1109/TII.2022.3169456.