УДК 681.5
DOI DOI DOI https://doi.org/10.32782/2663-5941/2026.2.1/26

Михалюк А.П.
https://orcid.org/0009-0004-7005-5864
Національний університет харчових технологій

Міркевич Р.М.
https://orcid.org/0009-0004-2796-9388
Національний університет харчових технологій

РОЗШИРЕНА КІЛЬКІСНА ОЦІНКА КІБЕРФІЗИЧНИХ РИЗИКІВ: ІНТЕГРАЦІЯ БЕЗПЕКИ, КОНТЕКСТУ ТА ОПЕРАЦІЙНИХ МОЖЛИВОСТЕЙ У СЕРЕДОВИЩАХ IIOT ТА АВТОМАТИАЦІЇ

У цій науковій статті представлено новий підхід до кількісного аналізу рівнів загроз для критичної інфраструктури, заснований на інтеграції екологічного контексту та можливостей компонентів промислового Інтернету речей (IIoT) та систем контролю та управління (I&C). Метою цього дослідження є вирішення «кризи метрик», що виникає через невід'ємний конфлікт між традиційною метрикою IT-безпеки. У той час як традиційні метрики IT-безпеки зосереджені на «тріаді ЦРУ» (Конфіденційність, Цілісність, Доступність) у певному порядку, у промислових системах управління (ICS) існує потреба змінити цей порядок, де безпека є головним пріоритетом, а потім доступність та цілісність. Автори цієї наукової статті проводять ретельний аналіз механіки нових екологічних метрик CVSS v3.1 та v4.0, включаючи модифікований вектор атаки (MAV), модифіковану складність атаки (MAC), модифіковані необхідні привілеї (MPR) та модифіковану область дії (MS). Одним з ключових внесків цього дослідження є розробка моделі «Оцінка кіберфізичних операційних ризиків» (CP-ORS). Модель CP-ORS – це математична конструкція, яка дозволяє проводити науковий розрахунок ризику шляхом перетворення статичних оцінок ризику в динамічні моделі, що синтезують фізичні пошкодження, цілісність процесу та експлуатаційну доцільність. Модель CP-ORS по суті перетворює показник «Безпека» (який є лише інформативним доповненням у системі CVSS v4.0) на основний критерій оцінювання. Модель CP-ORS враховує такі параметри, як «Час до відмови» (TtF) та «Час до усунення» (TtR), для вимірювання фізичної стійкості. Застосовність цього підходу доведена його здатністю коригувати бали серйозності відповідно до топології мережі, використовуючи модель Пердью. Це гарантує, що немає ні «втоми від оповіщення», ні критичних помилок у рішеннях щодо пріоритетів захисту, які розділяють вразливості, що є теоретично критичними, але операційно зменшені фізичними заходами пом'якшення. Отримані результати формують наукову основу для розробки нового покоління автоматизованих систем управління вразливостями, які можуть точно відображати реальний операційний ризик в Індустрії 4.0.

Ключові слова: *кіберфізичні системи, IIoT, системи управління процесами, оцінка ризиків, CVSS, метрики безпеки, критична інфраструктура.*

Постановка проблеми. Прискорена конвергенція операційних технологій (OT) та інформаційних технологій (IT) у рамках парадигми промислового Інтернету речей (IIoT) створила значну кризу в оцінці загроз кібербезпеці. Галузі критичної інфраструктури, починаючи від виробництва електроенергії, водоочищення, фармацевтичного виробництва та транспортної логістики, все більше покладаються на взаємопов'язані програмовані логічні контролери (ПЛК), системи керування процесами та збору даних (PCD) та розподілені датчики IIoT. Хоча така зв'язність забезпечує безпрецедентну продуктивність завдяки прогнозному обслуговуванню та оркестрації в режимі реального часу, вона також усуває «повітряний зазор», який історично відділяв ці системи від цифрових загроз. [1]

Аналіз останніх досліджень та публікацій. Рецензовані дослідження визнають необхідність адаптації стандартних систем оцінювання до специфіки CFS. Основна увага приділяється переходу від статичних показників до «контекстуального

ризику» [3]. Сучасні стандарти, такі як CVSS v4.0, намагаються врахувати специфіку промислових систем за допомогою нових векторів оцінювання [4], але їх практичне впровадження в автоматизованих середовищах залишається фрагментарним. Дослідники також пропонують спеціалізовані метрики, такі як RVSS для роботизованих комплексів [5] та модифіковані підходи CVSS для промислових систем управління [6].

Постановка завдання. Метою дослідження є теоретичне обґрунтування та формалізація методу числової оцінки операційних загроз для середовищ IIoT/ACSTP. Концепція базується на трансформації фіксованих оцінок через призму змінених показників навколишнього середовища та впровадження системи CP-ORS. Наукова актуалізація полягає у створенні математичної схеми, що враховує архітектурну ізоляцію, запобіжні заходи відеоспостереження та послідовний вплив на фізичні процеси. [7].

Виклад основного матеріалу. Центральним викликом, з яким стикаються фахівці з безпеки, дослідники та менеджери операційних ризиків у цій галузі, є кількісна оцінка ризику. Традиційні показники кібербезпеки, розроблені переважно для IT-середовищ, де конфіденційність даних є першочерговою, не враховують кінетичну реальність кіберфізичних систем (КФС).

У цій статті представлено комплексний аналіз поточного стану метрик кібербезпеки для середовищ IIoT та АСУТП. У ній критично розглядається механіка метрик CVSS «Екологічна» та «Модифікована» (MAV, MAC, MPR), які були розроблені для подолання розриву між теоретичною вразливістю та операційною реальністю.

Інтеграція застарілих систем контролю та управління із сучасними архітектурами IIoT створює гетерогенну поверхню для атак, яку важко просто класифікувати. Типове промислове середовище зараз складається з дедалі поширенішої архітектури «моделі Purdue». Пристрої рівня 0 (процеси) та рівня 1 (управління), раніше доступні лише через послідовні кабелі, тепер часто підключаються до рівня 4 (бізнес-логістика) через шлюзи IIoT для телеметрії та аналітики [1].

Цей структурний зсув робить статичну метрику вразливості непотрібною. Вразливість у певній реалізації стеку TCP/IP може бути оцінена як "критична" (CVSS 9.8) Національною базою даних вразливостей (NVD). У корпоративному IT-середовищі цей рейтинг є точним, оскільки сервер, ймовірно, підключений до Інтернету або глобальної інтрамережі. Однак, якщо той самий стек TCP/IP знаходиться на ПЛК, розташованому за однонаправленим шлюзом безпеки (діодом даних) глибоко всередині нафтопереробного заводу, фактичний ризик набагато нижчий[6]

Розбіжність виникає через інверсію «тріади ЦРУ» (CIA Triad Confidentiality, Integrity, Availability). Безпека IT надає пріоритет конфіденційності, цілісності та доступності, зазвичай у такому порядку. Безпека OT вимагає, щоб безпека була на першому місці, а доступність, цілісність та конфіденційність (SAIC або AIC) – на другому. [4] Традиційні метрики не враховують «безпеку» як основну змінну, що призводить до небезпечного перекосу пріоритетів, коли команди безпеки виявляють високо оцінені, але незначні помилки програмного забезпечення, ігноруючи проблеми з низьким рейтингом, які можуть призвести до фізичного знищення.

Щоб усунути ці розбіжності, дослідники та лідери галузі прагнули вдосконалити методології оцінювання. Впровадження «модифікованих базових рівнів» у CVSS v3.1 та v4.0 є спробою дозволити кінцевим користувачам адаптувати оцінювання до свого середовища. [9] Ми прагнемо створити сувору теоретичну основу для нового покоління кіберфізичних метрик.

Механіка модифікації: аналіз показників навколишнього середовища CVSS. Загальна система оцінювання вразливостей (CVSS) є фактичним стандартом для оцінки ступеня вразливості. Однак її ефективність у сфері IIoT/ACS майже повністю залежить від правильного використання набору показників середовища. Ці показники дозволяють аналітикам варіювати базовий бал залежно від конкретного розгортання вразливого компонента. Незважаючи на їхню важливість, їх часто неправильно розуміють або ігнорують в автоматизованій звітності.

Теоретичні основи модифікованих метрик. Команда CVSS Environmental працює, розраховуючи базовий бал, використовуючи «модифіковані» версії базових метрик. Основна концепція полягає в тому, що «базові» метрики (вектор атаки, складність атаки, необхідні привілеї тощо) відображають вразливість у вакуумі (або в найгіршому випадку), тоді як «модифіковані» метрики відображають вразливість in situ.

Для інженера з управління технологічними процесами найважливішими модифікованими показниками є:

Модифікований вектор атаки (MAV): Цей показник відображає фізичну або логічну доступність пристрою в мережі.

Модифікована складність атаки (MAC): Це враховує заходи щодо захисту навколишнього середовища, які збільшують складність експлуатації.

Необхідні змінені привілеї (MPR): Це враховує рівні автентифікації, додані середовищем розгортання (наприклад, шлюзи, VPN).

Змінений діапазон (MS): Це визначає, чи може вразливість впливати на системи, що виходять за межі дії вразливого компонента (наприклад, HMI порушує роботу ПЛК).

Модифіковані показники впливу (MC, MI, MA): Вони коригують показники впливу (конфіденційність, цілісність, доступність) залежно від критичності конкретного активу.

Математичний зв'язок між цими змінними визначає кінцевий бал впливу на навколишнє середовище. У CVSS версії 3.1 бал впливу на навколишнє середовище визначається шляхом підстановки модифікованого балу на базовий бал у стандартних рівняннях. Якщо модифікований бал встановлено на «Не визначено» (X), розрахунок за замовчуванням використовує базовий бал.[11]

Модифікований вектор атаки (MAV) у системах керування процесами.

Модифікований вектор атаки (MAV), мабуть, є найважливішою метрикою для оцінки ризику IIoT та автоматизації. NVD призначає базовий вектор атаки (AV) на основі властивостей вразливості.

Мережа (N): Можна використовувати віддалено через стек протоколів.

Сусіди (A): Можна використовувати лише з одного й того ж домену широкомовлення (наприклад, локальної мережі, Bluetooth).

Місцевий (Л): Потрібен доступ до оболонки або локальне виконання.

Фізичний (Ф): Вимагає фізичної взаємодії з пристроєм.

Якщо ПЛК має вразливість з AV:N (базовий), але розгорнутий у зоні Tier 1, яка має повітряний проміжок або доступна лише через однонаправлений шлюз, аналітик повинен встановити MAV:P (фізичний) або MAV:A (суміжний) залежно від ступеня ізоляції.

Зауважте, що MAV технічно може збільшити ризик, якщо середовище менш безпечне, ніж передбачав постачальник, хоча зазвичай це використовується для пом'якшення наслідків.

Модифікована складність атаки (MAC) слугує змінною для кількісної оцінки «компенсуючих елементів контролю». У середовищах АТ безпека часто досягається за рахунок різноманітності та невизначеності (наприклад, власницькі протоколи, нестандартні RTOS). Якщо вразливість залежить від стандартної поведінки фрагментації TCP/IP, але промисловий брандмауер суворо нормалізує всі пакети, перш ніж вони досягнуть ПЛК, складність успішної доставки корисного навантаження експлойту значно зростає. Аналітик повинен збільшити AC:L (низький) до MAC:H (високий).

Сценарій, у якому аналізується граф атаки з високим рівнем серйозності. Навіть за MAC: Високий, MPR: Високий та MUI: Жоден, загальний бал все одно можна збільшити, якщо всі показники впливу (конфіденційність, цілісність, доступність) високі. [12] Це підкреслює обмеження: збільшення складності зменшує ймовірнісний компонент балу, але не усуває впливовий компонент.

Потрібні змінені привілеї (MPR) релевантно для реалізацій RBAC. Багато застарілих протоколів ACS (наприклад, Modbus TCP) не мають автентифікації, тому PR:N є точним. Однак безпечні обгортки (наприклад, Secure Modbus або VPN-тунелі) встановлюють певний рівень автентифікації. Якщо зловмисник повинен спочатку скомпрометувати VPN-хаб, щоб дістатися до лінії

Таблиця 1

Вплив архітектури мережі на модифікований вектор атаки (MAV)

Контекст вразливості	Базовий антивірус	Реальність розгортання	Модифікований AV (MAV)	Вплив на оцінку (приблизно)
Веб-сервер ПЛК	Мережа (N)	Підключено до корпоративного шлюзу IIoT	Мережа (N)	Без змін (високий ризик)
Веб-сервер ПЛК	Мережа (N)	Поза межами брандмауера рівня [3] (доступ через VPN)	Мережа (N)	Без змін (високий ризик)
Веб-сервер ПЛК	Мережа (N)	Однонаправлений шлюз (інформаційний діод)	Фізичний (П)	Різке падіння (-60%)
Переповнення буфера HMI	Сусіди (A)	Ізольована локальна мережа диспетчерської (без зовнішнього доступу)	Сусіди (A)	Без змін
Переповнення буфера HMI	Сусіди (A)	Віддалений доступ через стільниковий модем (IIoT)	Мережа (N)	Різке зростання (+20%)

Джерело: [9].

Modbus, вразливість фактично змінюється з PR:N на MPR:H (що вимагає підвищених привілеїв на транспортному рівні мережі).[4]

Модифіковане опитування (MS) та ефект хвилі Концепція області дії (Scope, Scope) у CVSS версії 3.1 є складною, але життєво важливою для IIoT. Вона вимірює, чи впливає вразливість в одному компоненті на ресурси, якими керує інший орган безпеки.

Основна сфера застосування: S:U (Без змін) або S:C (Змінено).

Змінений діапазон (MS): Дозволяє аналітиці змінювати це залежно від підключення до системи.

У IIoT поширеним явищем є «ефект брижів». Вразливість у граничному шлюзі (компонент A) може дозволити зловмиснику надсилати неправильно сформовані команди до ПЛК (компонент B). Якщо базова лінія передбачає, що шлюз ізольований (S:U), але конкретне розгортання інтегрує шлюз безпосередньо в цикл керування, аналітик повинен встановити MS:C. [12] Ця «зміна обсягу» зазвичай діє як множник, збільшуючи оцінку, щоб відобразити каскадний ризик, типовий для кіберфізичних систем (CPS).

Науковий аналіз методології галузевого дослідження: контекстуальний ризик. Карміт Ядін, генеральний директор DeviceTotal, доктор філософії та визнаний експерт з кібербезпеки, конкуренції в бізнесі та управління технічними ризиками, сформулювала філософію оцінки ризиків, яка суттєво відрізняється від статичної моделі NVD/CVSS. [19] Хоча її робота поширюється переважно через високорівневі галузеві публікації, подкасти та операційну архітектуру платформи DeviceTotal, а не через традиційні рецензовані академічні журнали, вона являє собою сувору, емпірично обґрунтовану методологію для «контекстуального ризику» в епоху IIoT.

Її критика висвітлює три основні недоліки поточної ситуації:

1. Здатність проти серйозності: Галузь плутає серйозність (потенційну шкоду) з ризиком (ймовірністю). [8]

2. ДНК пристрою: Два пристрої з однаковою версією операційної системи можуть мати суттєво різні профілі ризику залежно від їхньої прошивки, активних служб та апаратних компонентів. [15]

3. «Сліпа зона» некерованих пристроїв: Традиційні сканери вразливостей вимагають агентів або активного сканування, що може призвести до збоїв чутливого обладнання OT. [16]

Структура «Контекстного ризику». Ця методологія, реалізована за допомогою DeviceTotal, пропонує контекстну оцінку ризику, яку можна аналізувати як багатовимірну функцію, що включає змінні, які зазвичай ігноруються стандартним CVSS.

Ключова змінна - Операційні можливості. Цей підхід поєднує дані з Каталогу відомих вразливостей, що можуть бути експлуатовані (KEV), CISA та інших джерел інформації про загрози.

Теоретично: Вразливість існує в коді.

Зброя: Існує код експлойту для підтвердження концепції (PoC).

Контекстуально шкідливий: Конфігурація пристрою виявляє вектор вразливості.

Ключова змінна: видимість поверхні атаки.

Методологія розраховує «оцінку поверхні атаки» для кожного пристрою.

Математично це відповідає модифікованому вектору атаки (MAV) CVSS, але визначається динамічно за допомогою «безагентного» відбитка пальців, а не вручну аналітиками.

Безагентний підхід до «науки про дані». Альтернатива Data Science передбачає створення універсального репозиторію безпеки пристроїв. [7] Попередньо аналізуючи характеристики прошивки та апаратного забезпечення тисяч типів пристроїв, система може визначити рівень ризику конкретного пристрою, просто визначивши його марку, модель та версію прошивки, без необхідності активного дослідження.

Наукове виведення алгоритму:

На основі описів, прогнозований алгоритм для цього контекстуального ризику можна змоделювати наступним чином:

$$R_{context} = f\left(V_{severity}, E_{probability}, C_{criticality}, S_{surface}\right)$$

де:

$V_{severity}$ – це внутрішній бал вразливості (базовий бал CVSS).

$E_{probability}$ – ймовірність експлуатації (отримана з CISA KEV, Exploit-DB).

$C_{criticality}$ важливість активу для організації (бізнес-контекст).

$S_{surface}$ – це рівень доступності пристрою (досяжність мережі).

Ця модель надає пріоритет «швидким перемогам» для зловмисників – вразливостям, які слугують основою – незалежно від їхнього загального рівня серйозності.[8]

Розрив у безпеці: фізичний вплив на оцінку ризику. Хоча CVSS версії 4.0 та ця контекстна модель ризику враховують ймовірність та цифровий вплив атак, вони історично мали труднощі з кількісною оцінкою фізичного впливу, властивого автоматизації та IIoT.

CVSS версії 4.0 та додатковий бал безпеки. Наприкінці 2023 року Форум команд реагування на інциденти та безпеки (FIRST) випустив CVSS версії 4.0, яка включає спеціальну метрику безпеки (S) як частину нової додаткової групи метрик.[15]

Категорія безпеки CVSS версії 4.0 (S):

Не вказано (X): Атрибут не було оцінено.

Незначна (N): Жодного впливу на безпеку.

Присутній (P): Наслідки відповідають визначенню IEC 61508 як «граничні», «критичні» або «катастрофічні». [10]

Критичний аналіз:

Хоча включення поняття «безпека» є важливою віхою, його впровадження як додаткової метрики є суттєвим обмеженням. Додаткові метрики у CVSS версії 4.0 не змінюють кінцевий числовий бал (0-10). Вони призначені виключно для надання додаткового контексту споживачеві.

Це означає, що вразливість в ICS може мати оцінку CVSS 5.0 (середній рівень), але бути позначеною як «Безпека: присутня». Автоматизовані системи, які фільтрують за шкалою «Оцінка > 7.0», пропустять цю потенційно небезпечну для життя вразливість. Такий підхід «маркування» не дозволяє математично інтегрувати безпеку в логіку пріоритезації ризиків, залишаючи небезпечну прогалину для автоматизованих систем виправлення.

Альтернативні структури: RVSS та IVSS. Щоб заповнити цю прогалину, у науковій літературі запропоновано варіанти адаптації CVSS до конкретних предметних галузей.

Система оцінки вразливостей роботів (RVSS):

Запропонований Вілчесом та ін., RVSS явно розширює CVSS для обробки роботизованої безпеки.[18] Він вводить метрику впливу на безпеку (S), яка впливає на кінцевий бал, на відміну від додаткової метрики в CVSS версії 4.0.

Ключова інновація: Це додає до вектора впливу (разом із ЦРУ) компонент «безпеки».

Модифікований захист (MS): Дозволяє враховувати вплив на безпеку з екологічної точки зору на основі фізичних бар'єрів (наприклад, робот у клітці має менший ризик для безпеки, ніж колаборативний робот).

Система оцінки промислової вразливості (IVSS):

IVSS розроблено як «індустріалізована альтернатива» CVSS.4

Фокус: Це знижує пріоритет конфіденційності (часто неактуальний в АО) та ставить більший акцент на доступність та цілісність.

Методологія: Він коригує вагу показників навколишнього середовища, щоб відобразити той факт, що «перезавантаження» пристрою I&K не є стандартним виправленням.

Кількісна оцінка фізичного впливу. Нещодавнє дослідження показників «фізичного впливу» для CPS пропонує змінні, які виходять за рамки простих позначок. Цей підхід наголошує на кількісному підході з використанням [16]:

Час до відмови (TtF): Тривалість часу від кібератаки до прояву небезпечних фізичних умов.

Час до вирішення проблеми (TtR): Час, необхідний операторам для виявлення порушення та виконання ручного втручання.

Умова стабільності:

$$Risk \propto \frac{1}{TtF - TtR}$$

Якщо система аварійно завершує роботу, перш ніж користувачі встигають її зберегти, це створює умову гонки, яку статичні метрики CVSS не можуть зафіксувати. $TtF < TtR$

Пропозиція: Оцінка кіберфізичних операційних ризиків (CP-ORS)

Враховуючи недоліки, виявлені у CVSS версії 4.0 (лише додаткова інформація щодо безпеки), та інтегруючи філософію «контекстуального ризику» галузевих досліджень (придатність пристроїв та ДНК), у цьому звіті пропонується єдина модель оцінки: Оцінка кіберфізичних операційних ризиків (CP-ORS).

Ця модель забезпечує сувору, математично визначену основу для розрахунку ризику в середовищах IIoT/ICS. Вона ефективно «модифікує» підхід CVSS, перетворюючи додаткову мітку безпеки на основний фактор оцінки та інтегруючи змінні фізичної стійкості.

Математична структура CP-ORS

CP-ORS надає оцінку за шкалою від 0 до 100, яка надає детальнішу інформацію, ніж шкала від 0 до 10.

$$CP - ORS = \min\left(100,[\left(V_{exploit} \times I_{physical} \times M_{resilience}\right) + \beta_{safety}]\right)$$

де:

Вектор контекстної експлуатаційної здатності (похідний від цієї логіки + CVSS MAV).

$I_{physical}$ **:**Фізичний коефіцієнт удару (отриманий з RVSS/IEC 61508).

$M_{resilience}$ **:**Пом'якшувальний коефіцієнт стабільності (отриманий з динаміки TtF/TtR).

β_{safety} **:**Зведення ключових показників безпеки.

Заголовки та визначення компонентів

Вектор контекстуальної експлуатації $V_{exploit}$

Ця змінна синтезує технічну серйозність вразливості з її контекстуальним охопленням та статусом зброї. Вона ефективно втілює критику галузевих досліджень на кшталт «серйозності проти можливості використання».

Значення розраховується наступним чином:

$$V_{exploit} = Base\,Severity \times Exploit\,Status \times MAV\,Coefficient$$

Таблиця 2

Коефіцієнти умов експлуатації E_{stat}

Статус	Визначення	Коефіцієнт	Логіка джерела
Озброєний	Експлойт існує в CISA KEV або Metasploit.	1.5	Високопріоритетна «Точка підтримки» [8]
Опубліковано PoC	Доступний код для підтвердження концепції (GitHub).	1.0	Стандартний ризик
Теоретичний	Публічний експлойт-код невідомий.	0,5	Низька терміновість

Таблиця 3

Коефіцієнти модифікованого вектора атаки (MAV)

Налаштування MAV	Визначення	Коефіцієнт	Логіка джерела
Ланцюг	Доступно через маршрутизовану мережу IIoT/ корпоративну мережу.	1.0	Повна експозиція
Сусіди	Доступно лише через OT VLAN/ зону.	0,6	Сегментований [9]
Фізичний	З повітряним зазором або вимагають локальної взаємодії.	0,1	Ізольований

Фізичний фактор впливу ($\boldsymbol{I_{physical}}$ *)*

Ця змінна кількісно визначає кінетичні наслідки на основі рівнів цілісності безпеки (SIL) стандарту IEC 61508 та визначень, що містяться в ньому. [18]

Таблиця 4

Рубрика фізичного впливу

Рівень	Значення	Визначення
Катастрофічно	10.0	Втрата життя, незворотна шкода навколишньому середовищу, повна втрата активів.
Критичний	7.5	Значна шкода (підлягає відновленню), значний викид у навколишнє середовище, значні виробничі втрати.
Маргінальний	4.0	Незначні травми, обмежені пошкодження, втрата ефективності виробництва.
Неповнолітні	1.0	Без фізичних пошкоджень; лише втрата даних або незначний простой.

Коефіцієнт стійкості до пом'якшення ($\boldsymbol{M_{resilience}}$ *)*

Це співвідношення винагороджує системи, розроблені з урахуванням принципів «безпеки за проектом», особливо ті, що відокремлюють функцію безпеки від кіберактиву. Це включає логіку проти [16]. *TtFTtR*

Таблиця 5

Рубрика сталого розвитку

Тип опору	Значення	Визначення
Пов'язано (немає)	1.0	Кіберактив безпосередньо контролює фізичний; незалежного захисту від збоїв немає. $TtF \to 0$
Людина в циклі	0,7	Сигналізація забезпечує достатньо часу для ручного втручання.. $TtR < TtF$
Механічна безпека	0,2	Фізичні блокування (наприклад, розрив мембран, падіння під дією сили тяжіння) запобігають катастрофі незалежно від стану ПЛК.

Суматор основних показників безпеки(β_{safety} *)*

Щоб гарантувати, що ризик вразливостей у критично важливих для безпеки пристроях ніколи не паде до «нуля» (ключове питання в цьому аналізі критичного ланцюга «низького рівня серйозності»), додається фіксоване значення в балах залежно від ролі пристрою. Пристрій SIL 3/4:+20 балів. Пристрій SIL 1/2:+10 балів. Незабезпечений актив: +0 балів.

Порівняння тематичного дослідження: ПЛК для дозування хлору

Щоб продемонструвати ефективність CP-ORS порівняно зі стандартними CVSS v3.1 та v4.0, розглянемо критичну вразливість віддаленого виконання коду (RCE) у ПЛК, який керує дозуванням хлору на водоочисній станції.

Сценарій: ПЛК має критичний RCE (базовий бал 9,8). Він підключений до захищеної OT-мережі (сусіда). Код експлойта є загальнодоступним.

Конфігурація A (Небезпечна): Немає механічних обмежувачів; програмне забезпечення ПЛК контролює максимальний потік.

Конфігурація B (стійка): Механічний обмежувач потоку фізично запобігає передозуванню.

Таблиця 6

Порівняльний аналіз оцінювання

Метрична модель	Конфігурація А (Небезпечна)	Конфігурація В (стійка)	Аналіз
Базовий рівень CVSS 3.1	9.8 (Критично)	9.8 (Критично)	Не розрізняє фізичний ризик.
Версія середовища CVSS 3.1	8.1 (Високий)(MAV:A)	8.1 (Високий)(MAV:A)	Враховує мережу, ігнорує сталий розвиток.
CVSS версії 4.0	8,5 (Високий)(Безпека :P)	8,5 (Високий)(Безпека :P)	Є мітка безпеки, але клас ідентичний.
Запропонований CP-ORS	95 (Критично)	31 (низький)	Правильно визначає операційний ризик.

Розрахунок CP-ORS (конфігурація А):

$V_{exploit}$:

$(Base 9.8 scaled) \times 1.5 (Weaponized) \times 0.6 (Adjacent) \approx 8.8$

$I_{physical}$: 10.0 (Катастрофічний)

$M_{resilience}$: 1.0 (Немає)

β_{safety} : +20

Рейтинг: $(8.8 \times 10.0 \times 1.0) + 20 = 108 \rightarrow 100$

Розрахунок CP-ORS (конфігурація В):

$V_{exploit}$: 8.8

$I_{physical}$: 10.0

$M_{resilience}$: 0,2 (механічна стійкість до пошкоджень)

β_{safety} :+20

Рейтинг: $(8.8 \times 10.0 \times 0.2) + 20 = 17.6 + 20 = 37.6$

Модель CP-ORS успішно деескалює ризик у конфігурації В, відображаючи той факт, що механічна негативна безпека робить кібератаку нездатною спричинити катастрофічні наслідки. Це запобігає «втомі від тривоги» та дозволяє зосередити ресурси на конфігурації А.

Операційні стратегії та їх реалізація. Впровадження моделі CP-ORS або навіть покращених модифікованих метрик CVSS вимагає переходу від пасивного сканування вразливостей до активного «управління кіберфізичними активами».

Вимоги до збору даних. Щоб автоматично розрахувати ці оцінки, екосистема безпеки повинна обробити три окремі потоки даних:

1. Розвідка кіберзагроз (CTI): Отримує дані про зрілість експлойту в режимі реального часу (наприклад, CISA KEV) для заповнення змінної. Це узгоджується з акцентом на "вплив".

2. Карта топології мережі: Динамічне відображення розташування активів (рівень 2 проти рівня 4) для заповнення коефіцієнта MAV.

3. Аналіз технологічних ризиків (TRA): Отримання інженерних даних (дослідження HAZOP) для визначення рівня цілісності безпеки (SIL), фізичного впливу () та стабільності (). Це найскладніші дані для оцифрування, але вони є важливими для справжньої безпеки $I_{physical} M_{resilience}$.

Безагентна оцінка та машинне навчання. З огляду на обмеження ПЛК, «безагентний» підхід, запропонований DeviceTotal, є єдиним життєздатним шляхом для широкого розгортання. Аналізуючи мережевий трафік (порти SPAN) та файли конфігурації (файли проекту), а не запитуючи операційну систему пристрою, система може отримати відбиток «ДНК» пристрою, щоб знайти його профіль безпеки в репозиторії.

Крім того, моделі машинного навчання (зокрема, багатошарові перцептрони) показали багатообіцяючі результати у виявленні атак та прогнозуванні їхнього впливу шляхом вивчення «фізики» системи автоматизації.[26] У майбутніх ітераціях CP-ORS машинне навчання (ML) може бути використане для динамічного коригування коефіцієнта на основі стабільності процесу в режимі реального часу – якщо система виявляє, що процес працює поблизу запасу безпеки, показник стабільності знижується, а показник кіберризику різко збільшується $M_{resilience}$.

Висновки. Метрики кібербезпеки, що зараз використовуються в середовищах IIoT та ICS, є пережитком епохи IT, небезпечно відірваними від фізичної реальності критичної інфраструктури. Хоча розробка CVSS версії 4.0 та «модифікованих» показників навколишнього середовища забезпечують інструменти для кращої оцінки, вони рідко використовуються на повну потужність через складність та брак контекстних даних.

Аналіз методології галузевих досліджень показує критично важливий шлях уперед: ризик має бути контекстуальним, орієнтованим на зручність використання та адаптованим до ДНК конкретного пристрою. Однак навіть цей підхід має бути доповнений ретельною кількісною оцінкою фізичної безпеки та стійкості.

Запропонована структура CP-ORS об'єднує ці області. Математично поєднуючи кіберймовірність (операційну ймовірність/MAV) з фізичними наслідками (вплив/стійкість), вона пропонує метрику, яка відображає справжній операційний ризик. В епоху конвергентної інфраструктури метрика, яка не враховує запобіжний клапан або систему безпеки, є не просто неточною, вона небезпечна. Перехід до кіберфізичної оцінки – це не просто академічна вправа; це операційний імператив для безпеки Індустрії 4.0.

Список літератури:

1. Barrere M., Hankin C., Nicolaou N., Eliades D., Parisini T. Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. *Journal of Information Security and Applications*. DOI: 10.1016/j.jisa.2020.102471.
2. Massaro V., Capacci L., Montanari R. Towards Context-Aware Risk Assessment Scoring System for IoT/IIoT Devices. *Матеріали семінару CEUR.* URL: https://ceur-ws.org/Vol-3488/paper25.pdf (дата звернення: 17.12.2025).
3. Aftabi N., Li D., Sharkey T. An Integrated Cyber-Physical Risk Assessment Framework for Worst-Case Attacks in Industrial Control Systems. URL: https://arxiv.org/html/2304.07363v5 (дата звернення: 17.12.2025).
4. Gori G., Rinieri L., Melis A., Al Sadi A., Callegati F., Prandini M. A Systematic Analysis of Security Metrics for Industrial Cyber–Physical Systems. DOI: 10.3390/electronics13071208.
5. Moraitis G., Nikolopoulos D., Bouziotas D., Lykou A., Karavokiros G., Makropoulos C. Quantifying Failure for Critical Water Infrastructures under Cyber-Physical Threats. *Journal of Environmental Engineering.* DOI: 10.1061/(ASCE)EE.1943-7870.00017.
6. Collier Z., Panwar M., Ganin A., Kott A., Linkov I. Security Metrics in Industrial Control Systems. URL: https://arxiv.org/pdf/1512.08515 (дата звернення: 17.12.2025).
7. Yoon S., Kim D., Kim K., Euom I. Vulnerability Exploitation Risk Assessment Based on Offensive Security Approach. DOI: 10.3390/app132212180.
8. Oser P., Heijden R., Luders S., Kargl F. Risk Prediction of IoT Devices Based on Vulnerability Analysis. *ACM Transactions on Internet Technology.* 2022. Vol.25, №14. P. 1-36. DOI: 10.1145/3510360.
9. Common Vulnerability Scoring System v4.0: Examples. URL: https://www.first.org/cvss/examples (дата звернення: 17.12.2025).
10. Common Vulnerability Scoring System version 4.0: Specification Document. URL: https://www.first.org/cvss/specification-document (дата звернення: 17.12.2025).
11. Ibrahim M., Elhafiz R. Security Assessment of Industrial Control System Applying Reinforcement Learning. DOI: 10.3390/pr12040801.
12. Cheimonidis P., Rantos K. Dynamic Vulnerability Criticality Calculator for Industrial Control Systems. URL: https://arxiv.org/html/2404.16854v1 (дата звернення: 17.12.2025).
13. Lyu X., Ding Y., Yang S. Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*. Vol.4, №3. P. 221-232. DOI: 10.1049/iet-cps.2018.5068.
14. Vilches V., Gil-Uriarte E., Ugarte I., Mendia G., Pisón R., Kirschgens L., Calvo A., Cordero A., Apa L., Cerrudo C. Towards an open standard for assessing the severity of robot security vulnerabilities, the Robot Vulnerability Scoring System (RVSS). DOI: 10.48550/arXiv.1807.10357.
15. Wen H. Vulnerability Assessment of Industrial Control System with an Improved CVSS. DOI: 10.48550/arXiv.2306.08631.
16. Keenan C., Maier H., Delden H., Zecchin A. Bridging the Cyber–Physical Divide: A Novel Approach for Quantifying and Visualising the Cyber Risk of Physical Assets. DOI: 10.3390/w16050637.
17. Okur C., Dener M. Symmetrical Resilience: Detection of Cyberattacks for SCADA Systems Used in IIoT in Big Data Environments. DOI: 10.3390/sym17040480.
18. Do V., Fillatre L., Nikiforov I. Sequential monitoring of SCADA systems against cyber/physical attacks. *IFAC-PapersOnLine (Elsevier).* 2015. Vol.48, №21. P. 746-753. DOI: 10.1016/j.ifacol.2015.09.616.
19. Yadin C. Secure ICS and OT for Industry 4.0. URL: https://devicetotal.com/secure-ics-and-ot-for-industry-4-0/ (дата звернення: 17.12.2025).

Mykhalyuk A. P., Mirkevich R. M. ADVANCED CYBER-PHYSICAL RISK QUANTIFICATION: INTEGRATING SECURITY, CONTEXT AND OPERATIONAL CAPABILITIES IN IIOT AND AUTOMATION ENVIORNMENTS

This paper presents a new approach to quantifying threat levels for critical infrastructure based on the integration of environmental context and capabilities of Industrial Internet of Things (IIoT) and I&C components. The purpose of this study is to address the "metrics crisis" that arises from the inherent conflict between traditional IT security metrics. While traditional IT security metrics focus on the "CIA triad" (Confidentiality, Integrity, Availability) in a specific order, in industrial control systems (ICS) there is a need to reverse this order, where security is the top priority, followed by availability and integrity. The authors of this paper conduct a thorough analysis of the mechanics of the new CVSS v3.1 and v4.0 environmental metrics, including Modified Attack Vector (MAV), Modified Attack Complexity (MAC), Modified Required Privileges (MPR), and Modified Scope of Action (MS). One of the key contributions of this study is the development of the Cyber-Physical Operational Risk Assessment (CP-ORS) model. The CP-ORS model is a mathematical construct that enables scientific risk calculation by transforming static risk assessments into dynamic models that synthesize physical damage, process integrity, and operational feasibility. The CP-ORS model essentially transforms the Security metric (which is only an informative addition to the CVSS v4.0 system) into a primary evaluation criterion. The CP-ORS model takes into account parameters such as Time to Failure (TtF) and Time to Repair (TtR) to measure physical resilience. The applicability of this approach is demonstrated by its ability to adjust severity scores according to network topology using the Purdue model. This ensures that there is neither "alert fatigue" nor critical errors in protection priority decisions that separate vulnerabilities that are theoretically critical but operationally mitigated by physical mitigation measures. The results form the scientific basis for the development of a new generation of automated vulnerability management systems that can accurately reflect real operational risk in Industry 4.0.

Keywords: *robotic systems, heterogeneous systems, automation systems, cyber-physical systems, monitoring, information security.*

Дата першого надходження статті до видання: 16.03.2026
Дата прийняття статті до друку після рецензування: 13.04.2026
Дата публікації (оприлюднення) статті 11.05.2026