*Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 2 (24)*
*ISSN 2522-9818 (print)*
*ISSN 2524-2296 (online)*

УДК 004.056.5
DOI: https://doi.org/10.30837/ITSSI.2023.24.131

Є. Мерзлікін, Є. Бабешко

# АНАЛІЗ КІБЕРБЕЗПЕКИ ВЕБОРІЄНТОВАНИХ ІНДУСТРІАЛЬНИХ *IoT*-СИСТЕМ

У сучасному світі питання кібербезпеки є одним із найважливіших, особливо в контексті динамічного розвитку веборієнтованих індустріальних систем Інтернету речей (*IoT*). **Предметом дослідження** є забезпечення кібербезпеки веборієнтованих індустріальних *IoT*-систем. **Мета статті** – аналіз наявних методів аналізу кібербезпеки, виявлення обмежень і формування вимог до нової концепції оцінювання, що передбачає шляхи усунення виявлених обмежень. **Завдання**, що розв'язуються: аналіз методів, засобів і технологій організації веборієнтованих індустріальних *IoT*-систем і питань забезпечення їх кібербезпеки. Застосовані **методи**: аналіз джерел, системний аналіз. **Результати дослідження**. Аналіз джерел показав, що проблема забезпечення кібербезпеки індустріальних *IoT*-систем є актуальною завдяки використанню в одній системі новітніх інформаційних технологій (IT) і традиційних операційних технологій (OT), таких як індустріальні протоколи тощо. Крім того, постійне зростання кількості та різновидів атак, спрямованих саме на індустріальні *IoT*-системи, є додатковими рушіями подальшого розвитку методів оцінювання та забезпечення кібербезпеки. Пропонується узагальнена концепція оцінювання та забезпечення кібербезпеки веборієнтованих індустріальних *IoT*-систем, яка містить етапи ідентифікації, аналізу, підвищення захищеності, виявлення та захисту. **Висновки**. Питання забезпечення кібербезпеки веборієнтованих індустріальних *IoT*-систем є надзвичайно актуальним, а наявні методи аналізу й засоби забезпечення не повністю задовольняють вимоги до таких систем. Саме тому розроблення та застосування запропонованої концепції оцінювання та забезпечення кібербезпеки дасть змогу суттєво вплинути на підвищення кібербезпеки індустріальних *IoT*-систем.

**Ключові слова**: кібербезпека; *IoT*; Індустрія 4.0; веборієнтовані системи; безпека вебзастосунків; виявлення вразливостей; виявлення вебатак.

## 1. Вступ

Парадигма Інтернету речей (*IoT*) є ключовим кроком на шляху задуму та створення сучасних систем. Об'єднання інтелектуальних пристроїв і серверів, підключених до великої кількості вузлів вимірювання та керування, надає потужну інфраструктуру для розроблення застосунків і систем, що підвищують інтелект і можливості користувачів. Сферами застосування *IoT* є електронна охорона здоров'я, розумне виробництво та автоматизація, розумні міста й багато інших.

Основною концепцією *IoT* є надшвидке наскрізне з'єднання між усіма пристроями, основане на таких досягненнях у мережах, як технологія *5G* і нова концепція *6G*. Інтеграція з іншими парадигмами й технологіями, зокрема *Cloud Computing, Fog Computing, DevOps*, і різноманітними програмними структурами, надала набір інструментів для створення безпрецедентно ефективних застосунків [1].

На сьогодні більшість систем *IoT*, а саме індустріальних *IoT (IIoT)*, або інтенсивно використовують вебвзаємодії, або принаймні мають певну частину, яка застосовує вебпротоколи та інструменти. Не тільки зручність цих систем і програм, але й зв'язок між пристроями ґрунтується на вебтехнологіях і вебпротоколах завдяки стандартам *W3C* [2]. Вебвзаємодії покладаються на протоколи *HTTP* [3] і *HTTPS* [4] і схему *REST* [5]. Крім того, більшість платформ *IoT* побудовано на вебінтерфейсі, що діє як централізована інформаційна панель і уніфікований сервер керування для зв'язку з пристроями системи.

Причина, чому безпека систем *IoT* дедалі більше порушується, залежить від їх природи. Вони містять значну кількість різнорідних пристроїв, таких як датчики, приводи, комп'ютерні вузли та сервери. Крім того, *IoT* сильно взаємопов'язані (зокрема мають доступ до інтернету) і покладаються на програмні платформи, здебільшого розроблені як ізольовані системи. Варто визнати, що впровадження вебтехнологій розширило зону атаки для кіберзлочинців.

Сучасні підходи до підвищення безпеки в *IoT* зосереджені на підмножині компонентів, що містять ці системи, здебільшого пов'язаних із криптографією, мережною передачею, маршрутизацією тощо. Питання безпеки програмного забезпечення також досліджено за допомогою методів аналізу коду, безпеки операційної системи, судової експертизи тощо.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 2 (24)

Цього недостатньо в критичних підсистемах *IoT* / *IIoT*, оскільки помилка може мати катастрофічні наслідки. Однак існує складна рівновага:

– з одного боку, критично важливі системи *IoT* мають забезпечувати гарантії безпеки, щоб зменшити їх вразливість;

– з іншого – серверам *IoT* може знадобитися інтенсивне використання вебтехнологій, програмних інфраструктур і бібліотек, що дають змогу розробникові створити функційні можливості, які інакше були б неможливі.

### *1.1. Мотивація*

Різновидом *IoT* є промисловий (індустріальний) Інтернет речей (*Industrial Internet of Things, IIoT*). *IIoT* є сукупністю мереж і пов'язаного з ними виробничого обладнання, доповненого програмним забезпеченням (ПЗ) і вбудованими датчиками (рис. 1).


**Рис. 1.** Приклад індустріального Інтернету речей (*IIoT*) і технологій Індустрія 4.0

Системи, призначені для збирання інформації, обміну даними, можуть керуватися автоматично, без участі людини.

Індустріальний Інтернет речей створений як загальна концепція застосування Інтернету речей (IoT) до промислового сектора. Ключовою технологією концепції Індустрія 4.0 вважається Інтернет речей, що більше зосереджена на ефективності промислових процесів.

*IIoT* містить усі аспекти промислових операцій і спрямоване не тільки на ефективність процесів, але й на управління активами, обслуговування тощо. Важливими є такі тенденції:

- сучасна концепція Індустрія 4.0 поступово витісняє класичні, ізольовані від мережі Інтернет системи управління від одного вендора;
- їх замінюють індустріальні *IoT*-системи – розподілені системи, у яких обмінюються інформацією різноманітні пристрої, активно використовуються хмарні та вебтехнології;
- відкритість систем такого типу робить їх уразливими до кібератак;
- вплив атак може спричинити суттєві фізичні та економічні збитки.

Індустріальний Інтернет речей значною мірою ґрунтується на застосуванні вебтехнологій. Це зручно, оскільки дає змогу спостерігати за системою в реальному часі, оперативно впливати на неї, але й зростає потенційна загроза кібератак (рис. 2).


**Рис. 2.** Ризики безпеки *IIoT*

**Приклад атаки на *IIoT*-систему:** хакери зламали водоочисні споруди у Флориді, отримали доступ до внутрішньої платформи *ICS* і змінили рівень хімікатів, зробивши воду небезпечною для споживання [37]. Сталося це тому, що для злочинців стала доступна комп'ютерна система співробітника, яка давала змогу віддалено усувати проблеми системи водоочисних споруд.

*Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 2 (24)*
*ISSN 2522-9818 (print)*
*ISSN 2524-2296 (online)*

У такий спосіб хакерам вдалося змінити кількість гідроксиду натрію у воді від 100 до 11100 частин на мільйон.

Отже, будь-які компанії мають зважати на такі запобіжні заходи:

- використання технологій *VPN* – забезпечення безпечного тунелю й облікових даних, що надаються співробітникам для доступу до внутрішніх ресурсів і захисту критичних систем;
- правильна реєстрація та вимкнення: коли співробітники приєднуються до компанії, важливо переконатися, що доступ надається лише за потреби та негайно скасовується, коли працівники залишають її;
- розділення доступу до мережі: гарантуйте, що працівники мають доступ лише до тих систем, які їм потрібні;
- розміщення різних систем у різних мережах, доступ до яких мають лише ті групи співробітників, яким вони потрібні; це гарантує, що в разі злому менше систем може бути скомпрометовано;
- надання робочих пристроїв: коли постає необхідність швидкого переходу на дистанційну роботу (як це було 2020 р.), чимало співробітників отримують віддалений доступ до систем; працівникам надаються спеціальні пристрої замість того, щоб дозволяти доступ до корпоративної мережі з власних ґаджетів або ПК; це дасть змогу IT-відділам ефективніше контролювати інфраструктуру компанії;
- регулярне навчання співробітників: набуття навичок розпізнавати фішингові листи так само важливо, як і запровадити захисні системи; мірою того як зловмисники знаходять нові способи проникнення в мережі, підготовка співробітників лише посилить безпеку системи.

### *1.2. Мета й структура роботи*

Метою статті є аналіз сучасних методів, засобів і технологій організації веборієнтованих індустріальних *IoT*-систем та визначення проблем щодо забезпечення кібербезпеки *IIoT*.

У секції 2 наведено класифікацію проаналізованих джерел. У секції 3 подано результати аналізу джерел за визначеними напрямами класифікації. У секції 4 описано здобуті результати. Секція 5 містить висновки та подальші етапи дослідження.

## 2. Класифікація джерел

Проаналізовані джерела класифіковано за такими напрямами:

- порівняння й аналіз огляду літератури: [19, 20, 21, 22, 23, 24, 25, 26, 27, 30, 33, 34];
- оцінювання безпеки інструментів вебзастосунків: [1, 2, 3, 4, 5, 7, 9, 16, 17, 34, 35, 38, 39, 40];
- методи й рішення забезпечення безпеки Інтернету речей: [6, 7, 8, 9, 10, 11, 12, 13, 14];
- структура систем індустріального Інтернету речей і технології Індустрія 4.0: [9, 15, 16].

Крім того, джерела було розподілено за типом (рис. 3):


**Рис. 3.** Класифікація джерел

## 3. Аналіз джерел за напрямами

### *3.1. Методи оцінювання та забезпечення кібербезпеки веборієнтованих індустріальних IoT-систем на різних етапах життєвого циклу*

Основні організації, такі як Міжнародна організація стандартизації (ISO) 27001, сформували вимоги щодо впровадження та покращення параметрів безпеки для вебзастосунків [38].

Для компаній і розробників регулярно публікується десятка найкритичніших загроз [39], щоб підвищити поінформованість про безпеку вебзастосунків і зменшити збитки, які завдають потенційні вразливості. Однак, відповідно, існують

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 2 (24)

рекомендовані шаблони програмування, що допомагають користувачам виправляти небезпечні конфігурації та мінімізувати ризики [40].

Нижче наведено набір ризиків безпеки для вебінтерфейсів.

- *Порушений контроль доступу*. Контроль доступу змушує користувачів діяти чітко в межах ділянки програми, до якої їм надано дозвіл. Якщо застосована політика контролю доступу не є успішною для користувача, отже, він / вона мають доступ до цінних ресурсів.
- *Криптографічні збої* призводять до розкриття конфіденційних даних. З цієї причини шифрування інформації має відповідати найновішим стандартам, уникаючи того, щоб системи (браузер, база даних тощо) використовували застарілі криптографічні функції для шифрування даних, паролів тощо. Також необхідно класифікувати рівень безпеки всіх системних даних, щоб визначити, які криптографічні алгоритми використовувати та як сертифікувати приймач і підтвердити його.
- *Ін'єкція* передбачає низку ризиків, наприклад, *міжсайтовий сценарій (XSS) та ін'єкцію SQL*. Ін'єкція відбувається, коли введена користувачем інформація не перевіряється належним чином і не фільтрується, і вона стає частиною вебсторінки або бази даних. Якщо зловмисний вхід безпосередньо використовується програмою, ворожа інформація може бути впроваджена в записи програми або базу даних, спричиняючи тривалу шкоду системі. Це можна частково виправити, якщо виокремити команди від даних і перевірити вхідну інформацію за допомогою відповідних фільтрів, безпечніших за *API* та елементів керування *SQL*, що обмежують неавторизовані операції та уникають розголошення конфіденційних даних, а також якщо переглядати вихідний код.
- *Неправильна конфігурація безпеки* часто виникає, коли вмикаються, вимикаються, установлюються чи видаляються функції, залишається обліковий запис і пароль за замовчуванням без змін, використовуються застарілі комплектувальні елементи, а також не вмикаються останні функції безпеки.
- *Помилки ідентифікації та автентифікації* зазвичай є результатом атак грубої сили та/або криптографічних збоїв за допомогою сценаріїв, що постійно намагаються автоматично перевірити комбінації імен користувачів і паролів. Такі дії відомі як атаки грубою силою. Ризики існують, коли облікова база даних має слабку автентифікацію (наприклад, користувач адміністратора з паролем *abc123*) або коли зловмисники користуються витоком ідентифікаторів сесії, щоб отримати контроль над зв'язком. Більше кроків для перевірки (наприклад, код, безпечні запитання, використання інших пристроїв, таких як мобільний телефон, розпізнавання обличчя тощо) можуть зменшити ризик атак грубою силою. Іншими заходами захисту є використання складних паролів і видалення простих тестових облікових записів.
- Якщо програма залежить від ненадійних бібліотек, модулів та/або інших ресурсів, можуть виникнути *збої програмного забезпечення* та *цілісності даних*.
- *Збої в журналі безпеки та моніторингу* мають бути постійним завданням для виявлення активних атак. Створення журналів невдалих спроб входу є основною стратегією запобігання небезпек. Однак цього може бути недостатньо з кількох причин: деякі невдалі спроби входу можуть не реєструватися. Крім того, попередження та помилки можуть не давати чіткого уявлення про ситуацію. Розробник має переконатися, що все керування доступом і збої можуть бути записані з достатньою кількістю даних користувача, зареєстровані відомості зашифровані в разі ін'єкції, і встановлено механізм звіту про помилки.
- *Підроблення запиту* з боку сервера відбувається, коли програма отримує віддалений ресурс без перевірки URL-адреси, наданої користувачем. Унаслідок зловмисник може надіслати створений запит на несподівані посилання, навіть якщо застосунок захищено брандмауером або *VPN*. Застосунок має запобігти цьому, фільтруючи та перевіряючи всі дані, надіслані користувачем, установлюючи низку схем URL-адрес і уникаючи надсилання необроблених відповідей клієнту.

Згідно зі статистикою 19 % уразливостей сканованих вебзастосунків дають змогу зловмиснику контролювати програму й операційну систему. 2019 р. звіт про вразливості в корпоративних інформаційних системах [1] показав, що майже 75 % векторів проникнення в локальну мережу (*LAN*) мають уразливості в захисті вебзастосунків. Подібним чином лазівки в процесі розроблення створюють серйозні загрози для вебзастосунків.

Крім того, змін у налаштуваннях конфігурації достатньо для усунення лише 17 % вразливостей.

*Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 2 (24)*
*ISSN 2522-9818 (print)*
*ISSN 2524-2296 (online)*

Більшість з них мають низький рівень складності. Зауважимо, що 50% витоків спричиняють розкриття інформації облікового запису та персональних даних, а близько 91% відсканованих вебзастосунків зберігають і обробляють особисту інформацію.

Вибір правильної методології тестування на проникнення для конкретного типу вразливості [43] відіграє важливу роль у скануванні вебзастосунку для виявлення вразливості. Навіть більше, автоматизація тестування вебзастосунків корисна для *pen-tester*, що не тільки знизило обсяг роботи, час, ресурси та вартість, але й зменшило залежність тестувальників від знань людини [44].

Крім того, сканер зберіг людські знання про *pen-testing*, створивши виконувані комп'ютерні програми. Отже, розроблення автоматизованих сканерів безпеки вебзастосунків зробило ручне тестування популярною тенденцією досліджень. У цій сфері розробники перетворюють методи *pen-testing* (*penetration test* / тест на проникнення) у виконувані програми, щоб краще виявляти вразливості вебзастосунків.

### *3.2. Огляд літератури щодо оцінювання вебзастосунків*

Оцінювання зосереджено здебільшого на можливостях обраних вебзастосунків щодо *XSS* (міжсайтових сценаріїв), на застосуванні *SQL*, упровадженні коду й несправних елементів керування доступом. Виявлені вразливості було класифіковано, щоб оцінити 17 уразливостей.

У цьому огляді обговорюються різні інструменти. Незважаючи на те, що порівняння та підсумковий аналіз літератури подано в табл. 1, деякі з цих досліджень обмежуються кількома виявленими вразливими місцями, а інші лише порівнюють обмежені сканери.

Однак у цьому опитуванні 11 власних сканерів вебзастосунків із відкритим вихідним кодом порівнювалися з можливостями виявлення десяти найпопулярніших уразливостей *OWASP*.

Інструменти оцінювання вебзастосунків можна знайти як з відкритим кодом, так і запатентовані. Запатентовані інструменти зазвичай пропонують безкоштовні пробні пакети для користувачів і тестерів пера, однак їх можливості та функції обмежені. Існує кілька аспектів, пов'язаних із вибором одного сканера над іншим.

Сканер має виконувати такі функції:

- підтримувати протоколи й алгоритми автентифікації, що використовуються вебзастосунками;
- підтримувати основні типи методів доправлення вхідних даних і мати змогу виявляти вразливості у вебзастосунку з низьким рівнем хибно позитивних результатів;
- перебувати в межах технічних можливостей особи, яка буде ним користуватися;
- бути стабільним і регулярно оновлюватись останніми можливостями безпеки, щоб покрити поточні виявлені вразливості;
- бути обраним, зберігаючи водночас вартість і ліцензування в межах бюджету.

*Методи, засоби й технології організації веборієнтованих індустріальних IoT-систем і проблеми забезпечення їх кібербезпеки*

Проаналізовано 15 статей за 2019–2022 рр. Виявлено, що для досліджуваних систем пропонуються такі рішення:

- методи забезпечення безпеки *IoT* за допомогою машинного (*Machine Learning*) та глибокого навчання (*Deep Learning*) [10, 11];
- метод оцінювання кібербезпеки вебзастосунків на основі систем керування вмістом [10, 41];
- метод забезпечення кібербезпеки вебсистем шляхом обрання заходів захисту [42];
- методи збирання та аналізу даних пристроїв *IoT* [42];
- методи побудови *VPN*-лацюгів між кінцевими користувачами віртуальної мережі [42].

*Огляд методів машинного й глибокого навчання для безпеки Інтернету речей*

*Рішення*:

- *ML* і *DL* дають змогу розробити різні потужні аналітичні методи, що використовуватимуться для підвищення безпеки (рис. 4);
- аналіз трафіку на основі потоку допомагає виявляти зловмисну поведінку без необхідності поглибленого аналізу пакетів;
- інтеграція *ML* і *DL* з блокчейном для безпеки *IoT*.

*Проблеми та виклики:*

- такий підхід потребує чимало часу для поглибленого аналізу, крім того, він погано масштабується;
- цей метод потребує досить багато часу на навчання *ML*.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 2 (24)

**Таблиця 1.** *Аналіз літературних джерел і напрямів досліджень*

| Дослідник | Оцінений сканер | Оцінені вразливості | Основні здобутки | Обмеження |
|---|---|---|---|---|
| Doupé et al. (2010) [19] | Acunetix 174, AppScan Burp, Grendel-Scan, Hailstorm, Milescan, N-Stalker, NTOSpider, Paros, W3af, Webinspect | SQL Injection, Cross-Site Scripting, Code, Injection, Broken Access Controls | точність, час виконання та показники загрози | обсяг виявлення вразливостей дуже обмежений |
| Bau et al. (2010) [20] | Acunetix, Cenzic, McAfee SECURE, WebInspect, N-Stalker, QualysGuard | Cross-Site Scripting, SQL Injection, Cross-Channel Scripting, Session Management, Cross-Site Request Forgery | Scanner footprint, виявлення вразливості, помилкове спрацьовування | сканери можуть виявляти прості атаки ін'єкцій *XSS* і *SQL*, але не змогли виявити форму ін'єкцій *XSS* і *SQL* другого порядку |
| Parvez et al. (2015) [21] | Acunetix, Rational AppScan, ZAP | SQL Injection, Stored, XSS | швидкість виявлення для *SQLI* та *XSS* | порівнюються лише два комерційні сканери |
| Suteva et al. (2012) [22] | NetSparker, N-Stalker, OWASP-ZAP, W3af, Iron WASP, Vega | SQL Injection, Command Injection, File Inclusion, XSS | NetSparker має кращий рівень виявлення, ніж інші | Linux, MAC, Windows |
| El drissi et al. (2017) [23] | BurpSuite, Acunetix, Netsparker, AppSpider, Arachni, Wapiti, SkipFish, W3AF, IronWASP, ZAP and Vega | SQL Injection, Local and Remote File Inclusion, XSS, Path Traversal | уразливості *XSS* і *SQL* мають вищий рівень виявлення, *Arachni* краще працює в інструментах з відкритим кодом | Linux, MAC, Windows |
| Elahen, Claire et al. (2013) [24] | User Generated Content (UGC) evaluation | Assessing and Ranking UGC Assessment of healthcare systems | хибно позитивний рівень | |
| Mohit et al. (2017) [25] | BurpSuite, Acunetix, Wapiti, SkipFish, Netsparker, W3AF, AppSpider, Arachni, ZAP, Vega | Cross-Site scripting, SQL injection, Remote code execution, File inclusion | точність, відкликання та *F-measure* | обмежується ризиками помилкової тривоги й точністю |
| Gaurav et al. (2018) [26] | Penetration system for malware detection and web assessment using cloud services | OWASP's Vulnerabilities | економічне рішення для вебоцінки | обмежується окремими вебзастосунками |
| Mehreen et al. (2018) [27] | | | оцінювання на основі опитувальника з позитивними результатами | для мети оцінювання технічні деталі не надаються |
| Ashikali et al. (2018) [28] | W3af, Havij, Fimap, Metasploit, Acunetix, Nexpose | OWASP'S Vulnerabilities | основні методи оцінювання вразливості та тестування на проникнення | не проведено жодного порівняльного аналізу |
| Rawaa (2016) [38] | Paros, Wapiti, Skipfish, Nikto, Wfuzz, NetSparker, HP WebInspect | SQL Injection, Cross-Site Scripting | аналітичне порівняння шести інструментів з відкритим кодом | обговорюється обмежена кількість уразливостей |
| Mark and Rudolph (2006) [30] | Commercial and Free/Open-source Tools | | переваги й недоліки окремих інструментів | окремі засоби не популярні |
| Fang et al. (2018) [31] | AppScan, AWVS, Netspark, Vega, W3af | | виокремлена функція за допомогою згорткової нейронної мережі точно ідентифікує сканери | модель не можна динамічно покращувати |
| Alsaleh, Mansour et al. (2017) [32] | Arachni, Wapiti, Skipfish | SQL, Cross-Site Scripting | сканер *Arachni* може перевірити 100 % тестів *SQL* | немає істотної різниці в продуктивності між вибраними сканерами |
| Terry et al. (2018) [33] | OpenVAS, Kismet, Aircrack, SQLMAP, Wapiti | Cross-Site Scripting, Buffer overflow | | обмежено лише інформаційною системою охорони здоров'я |

*Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 2 (24)*
*ISSN 2522-9818 (print)*
*ISSN 2524-2296 (online)*

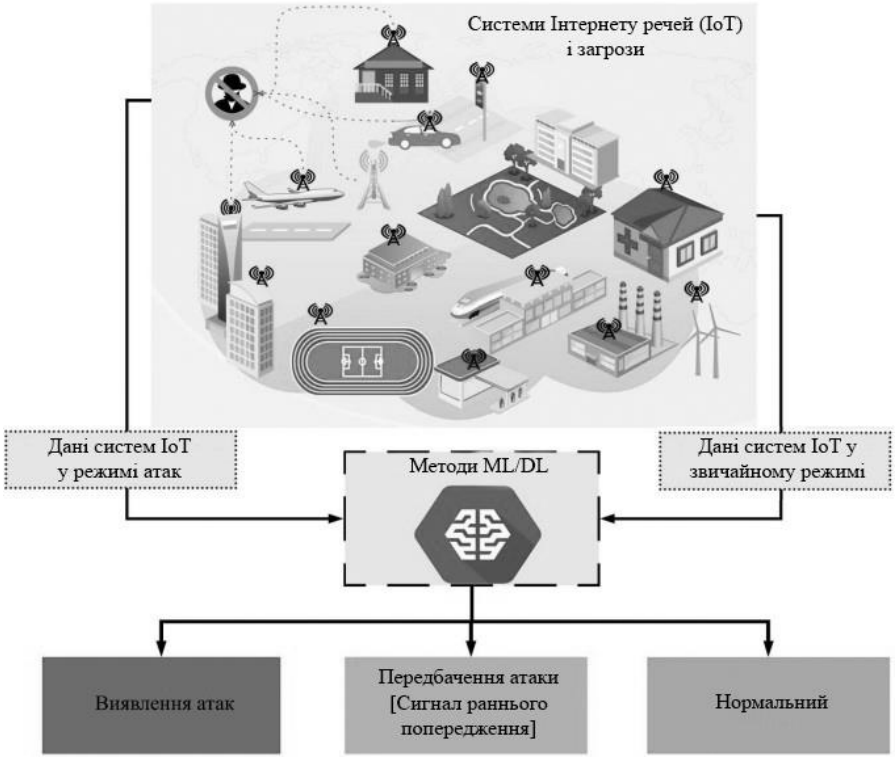



**Рис. 4.** Потенційна роль *ML/DL* у безпеці *IoT*

*Поглиблене вивчення та виявлення вразливостей і атак на вебзастосунки: системний огляд*

Архітектура вебзастосунків (рис. 5):

- вебпрограми є основним мережним рішенням для надання стандартних вебслужб;
- розроблення цих застосунків ґрунтується на клієнтській і серверній розробці;
- серверний блок містить вебсервер, вебзастосунок і сервер бази даних; він використовує серверні мови сценаріїв, зокрема *.NET, PHP* тощо; клієнтський блок працює у веббраузері користувача за допомогою зовнішніх мов сценаріїв, зокрема *CSS/HTML, Javascript* і под.

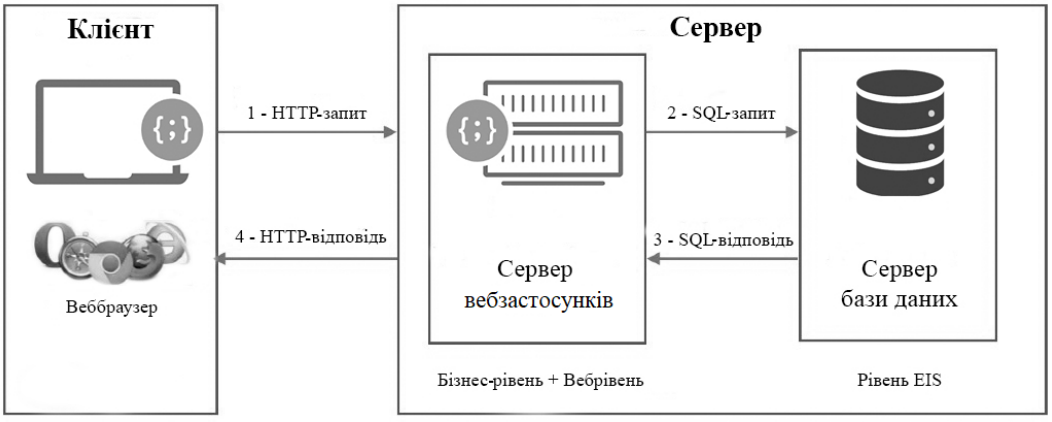
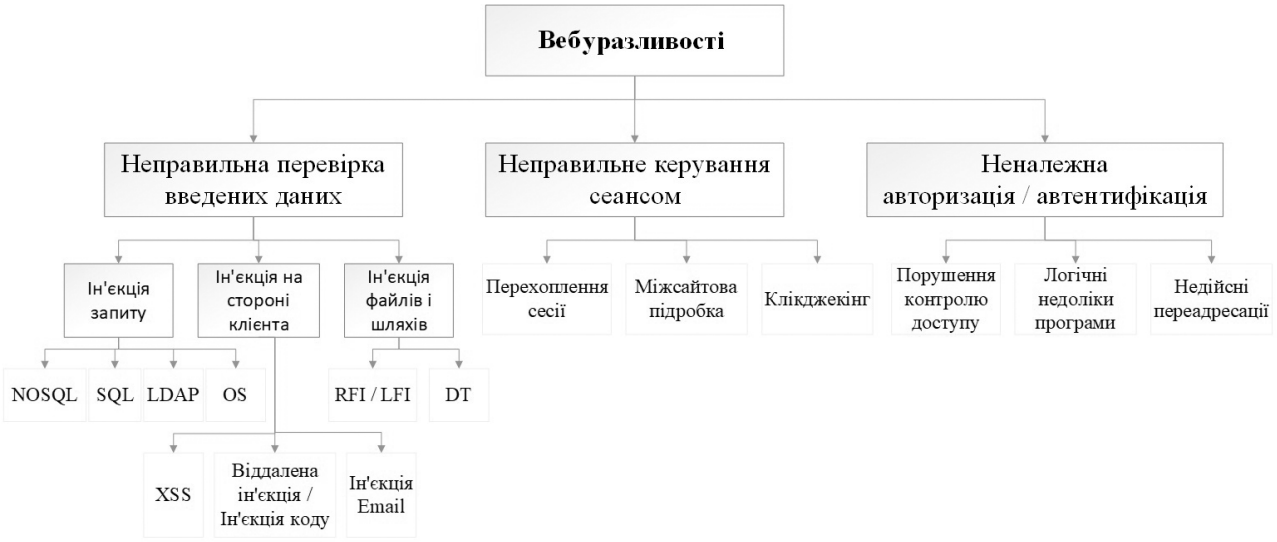



**Рис. 5.** Огляд вебархітектури

Вразливості вебзастосунків (рис. 6):

- міжсайтова підробка запитів (*CSRF*);
- упровадження *SQL* і міжсайтовий сценарій (*XSS*) як приклади вебатак;
- підробка сертифікатів;
- *DDOS*-атаки;
- слабкі паролі адміністраторів;
- використання ненадійних пристроїв.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 2 (24)




**LDAP** (Lightweight Directory Access Protocol) - Полегшений протокол доступу до директорій / каталогів
**OS** (Operating Systems) - Операційна система
**RFI** (Remote File Inclusion) - Віддалене виконання коду
**LFI** (Local File Inclusion) - Локальне виконання коду, в межах сервера
**DT** (Directory Traversal attack) - Атака обходу каталогу використовує недостатню перевірку безпеки

**Рис. 6.** Типи вебуразливостей [41]



- Зі збільшенням кількості пристроїв, підключених до мереж із підтримкою Індустрії 4.0, поверхня атаки також розширюється. Останні впровадження Індустрії 4.0 передбачають такі технології, як хмарні обчислення, штучний інтелект, пристрої *cps* або *iot*.
- У разі зламу ці пристрої можуть завдати серйозної шкоди матеріальним благам, наприклад продуктам на виробничій лінії, або нематеріальним благам, таким як витік конфіденційної інформації чи промислових секретів.
- Подано загальний систематичний огляд поточних атак на кібербезпеку, уразливостей і засобів захисту в сценаріях Індустрії 4.0 і 5.0.
- Наведено детальний аналіз і класифікацію щодо атак, уразливостей і захисту окремих досліджень.

## 4. Результати аналізу

*У проаналізованих публікаціях* увагу зосереджено на проблемах кібербезпеки *IoT*-систем загалом та індустріальних *IoT*-систем зокрема:

- безпека мережного рівня архітектури *IoT* залишається привабливою до атак;
- існують ризики безпеки для вебінтерфейсів;
- криптографічні збої також трапляються зі зростанням *IoT*;
- пропонуються локальні рішення, спрямовані на усунення виявлених уразливостей у конкретних компонентах;
- відсутній методологічний підхід забезпечення кібербезпеки вказаних систем на різних етапах життєвого циклу;
- розроблені методи й підходи швидкого виявлення вразливостей безпеки працюють недостатньо ефективно;
- сканери безпеки вебзастосунків мають різні недоліки й часто генерують неправильні результати тестування.

## 5. Концепція аналізу та забезпечення кібербезпеки

На рис. 7 зображена запропонована концепція аналізу й забезпечення кібербезпеки.

На першому етапі ("Ідентифікація") відбувається виявлення компонентів і протоколів обміну даними між цими компонентами. Цей етап є надзвичайно важливим, адже сучасні індустріальні системи зазвичай передбачають не ексклюзивні розробки, а типові компоненти, що використовуються і в інших системах (вебсервери, підсистеми логування тощо). Уразливості таких компонентів можуть бути привабливою метою для ініціаторів атак.

*Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 2 (24)*
*ISSN 2522-9818 (print)*
*ISSN 2524-2296 (online)*

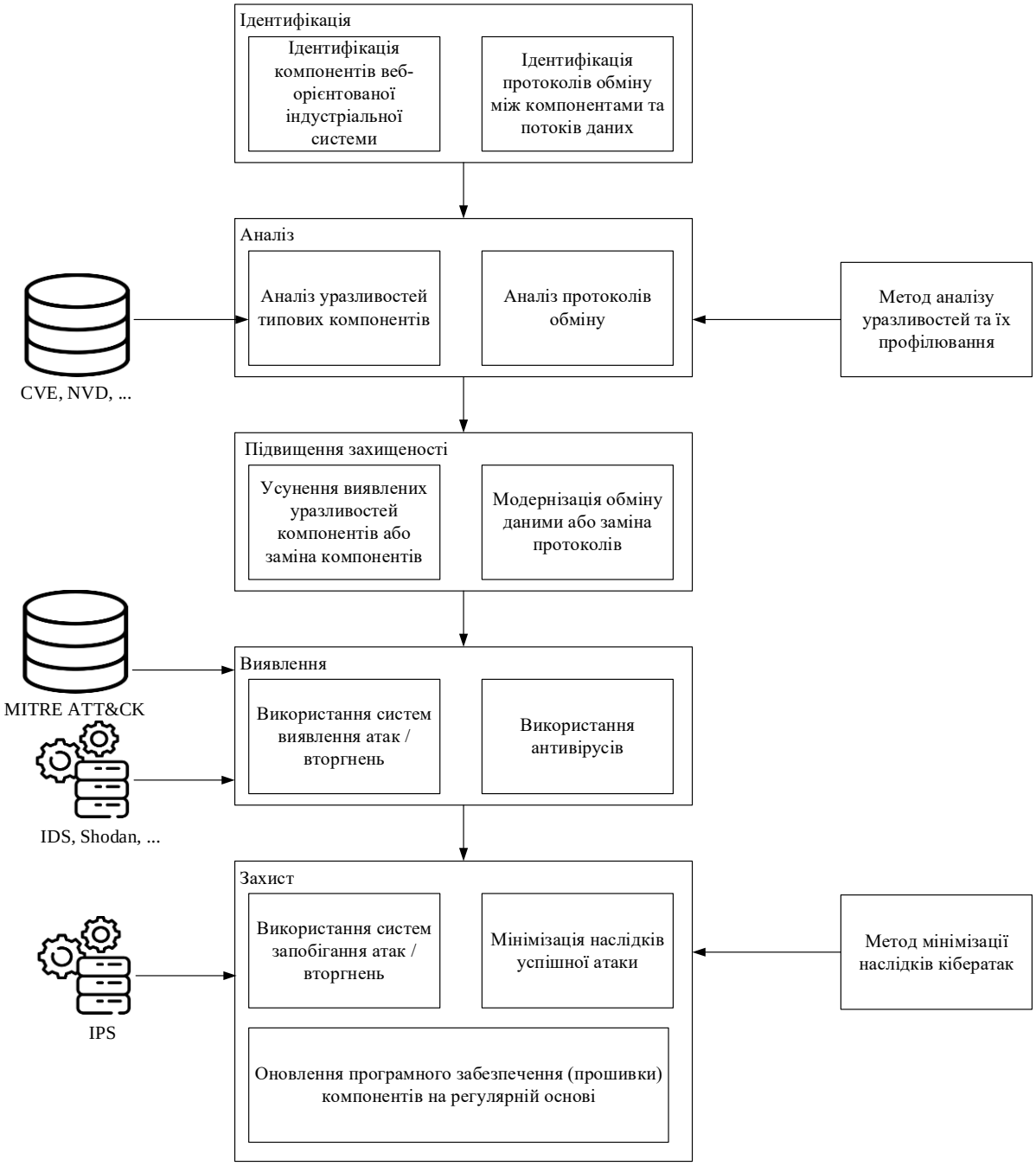



**Рис. 7.** Концепція аналізу та забезпечення кібербезпеки веборієнтованих індустріальних *IoT*-систем

На наступному етапі ("Аналіз") аналізуються вразливості типових компонентів із використанням таких баз, як *CVE (Common Vulnerabilities and Exposures)* [46], *NVD (National Vulnerability Database)* [47] тощо. Крім того, необхідним є аналіз протоколів обміну в частині захищеності даних і критичності їх компроментації.

На третьому етапі ("Підвищення захищеності") здійснюються заходи з усунення вразливостей, виявлених на попередньому етапі, або заміна компонентів у разі неможливості такого усунення. Крім того, вживаються заходи щодо модернізації обміну даними (наприклад, рознесення моніторингу та керування) або заміна протоколів, якщо вони не відповідають вимогам з кібербезпеки.

Наступний етап ("Виявлення") виконується під час експлуатації систем і передбачає розпізнавання несанкційних вторгнень у функціонування системи. Застосовуються системи виявлення атак / вторгнень (*IDS, Intrusion Detection System*) для розпізнавання

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 2 (24)

атак у автоматичному режимі та використання наявних баз сценаріїв типових атак (*MITRE ATT&CK* [48] тощо) для виявлення в ручному режимі.

На останньому етапі ("Захист") передбачається використання систем запобігання атакам / вторгненням (*IPS, Intrusion prevention system*), здійснення активностей для підтримки компонентів у захищеному стані (оновлення прошивок тощо), а також формування переліку контрзаходів для мінімізації ризиків у разі успішної кібератаки.

Для підтримки етапу "Аналіз" пропонується розробити метод аналізу вразливостей та їх профілювання (класифікації за впливом на функційну безпеку тощо). Для підтримки етапу "Захист" пропонується розробити метод мінімізації наслідків кібератак (ранжування ризиків, мінімізація ризиків способом упровадження контрзаходів тощо).

## 6. Висновки

### *6.1 Обговорення результатів*

Оцінка вебзастосунків містить багато дій, спрямованих на підвищення загальної безпеки й надійності проти різних кібератак. Розробники й тестувальники використовують чимало інструментів для сканування застосунків вебсерверів і динамічного виявлення всіх можливих уразливостей. Багато сканерів вебуразливостей потребують удосконалення для мінімізації рівня хибно позитивного виявлення. Хибно позитивні вразливості здебільшого з'являються з високою частотою за допомогою автоматизованих інструментів, що може призвести до неправильного оцінювання безпеки цільових вебсистем.

Упровадження заходів безпеки, таких як шифрування, автентифікація, контроль доступу, безпека мережі й застосунків для пристроїв Інтернету речей та їх властивих уразливостей, є не достатньо ефективним.

Існує низка методів, підходів виявлення вразливостей у веборієнтованих індустріальних *IoT*-системах, що покращують усю систему загалом, але потребують удосконалення.

Запропонована концепція дасть змогу впровадити необхідні активності до життєвого циклу індустріальних *IoT*-систем, спрямованих на підвищення кібербезпеки.

### *6.2 Подальші етапи дослідження*

Подальшим напрямом роботи є аналіз нормативної бази у сфері Інтернету речей, *IIoT*, їх кібербезпеки з урахуванням вебскладника для формування профілю та перевірки виконання вимог до систем такого типу, а також подальша деталізація запропонованої концепції та методів.

**Список літератури**

1. García-Valls M., Dubey A., Botti V. Introducing the new paradigm of Social Dispersed Computing: Applications, Technologies and Challenges. *Journal of Systems Architecture*. 2018. № 91. P. 83–102. DOI: https://doi.org/10.1016/j.sysarc.2018.05.007

2. W3C. The World Wide Web Consortium. The World Wide Web Consortium. 2021. URL: www.w3.org (дата звернення 30.05.2022).

3. Fielding R., Gettys J., Mogul J., Frystyk H., Masinter L., Leach P., Berners-Lee T. HyperText Transfer Protocol v1.1 HTTP (RFC 2616). The Internet Society: Reston, VA, USA. 1999. URL: https://datatracker.ietf.org/doc/html/rfc2616

4. Rescorla E. HTTP over TLS, RFC 1818. Internet Engineering Task Force. 2000. URL: https://datatracker.ietf.org/doc/rfc2818/

5. Fielding R. T. Representational State Transfer (REST). Architectural Styles and the Design of Network-based Software Architectures. *University of California, Irvine*. CA, USA. 2000. Vol. 5. P. 76–147. URL: https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm

6. Pedreira V., Barros D., Pinto P. A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead, Sensors. *MDPI Journals, Sensors*. 2021. Vol. 21(15). № 5189. DOI: https://doi.org/10.3390/s21155189

7. García-Valls M., Song L. Improving Security of Web Servers in Critical IoT Systems through Self-Monitoring of Vulnerabilities. *MDPI Journals, Sensors*. 2022. Vol. 22. № 5004. DOI: https://doi.org/10.3390/s22135004

8. Fang Z., Fu H., Gu T., Qian Z., Jaeger T., Hu P., Mohapatra P. A model checking-based security analysis framework for IoT systems. *Journal of High-Confidence Computing.* 2021. № 100004. DOI: https://doi.org/10.1016/j.hcc.2021.100004

9. Sarwar A., Alnajim A., Marwat S. N. K., Ahmed S., Alyahya S., Khan W. U. Enhanced Anomaly Detection System for IoT Based on Improved Dynamic SBPSO. *MDPI Journals, Sensors*. 2022. Vol. 22. № 4926. DOI: https://doi.org/10.3390/s22134926

10. Ervural B. C., Ervural B. Overview of Cyber Security in the Industry 4.0 Era. *Managing The Digital Transformation*. 2017. P. 267–284. DOI: https://doi.org/10.1007/978-3-319-57870-5_16

11. Alaoui R. L., Nfaoui E. H. Deep Learning for Vulnerability and Attack Detection on Web Applications: A Systematic Literature Review. *MDPI Journals, Future Internet*. 2022. Vol. 14. № 118. DOI: https://doi.org/10.3390/fi14040118

*Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 2 (24)*
*ISSN 2522-9818 (print)*
*ISSN 2524-2296 (online)*

12. Al-Garadi M. A., Mohamed A., Al-Ali A. K., Guizani M., et al. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Internet of Things Journal*. 2020. № 19890478. DOI: https://doi.org/10.1109/COMST.2020.2988293

13. Shahid J., Hameed M. K., Javed I. T., Qureshi K. N., Ali M., Crespi N. A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. *MDPI Journals, Applied Sciences*. 2022. Vol. 12. № 4077. DOI: https://doi.org/10.3390/app12084077

14. Pathak G., Gutierrez J., Ghobakhlou A., Rehman S. U. LPWAN Key Exchange: A Centralised Lightweight Approach. *MDPI Journals, Sensors*. 2022. Vol. 22. № 5065. DOI: https://doi.org/10.3390/s22135065

15. Surej H. I., Ma M., Su R. A FeedForward–Convolutional Neural Network to Detect Low-Rate DoS in IoT. *Engineering Applications of Artificial Intelligence.* 2022. Vol. 114. № 105059. DOI: https://doi.org/10.1016/j.engappai.2022.105059

16. Ferrer B. R., Mohammed W. M., Chen E., Martinez Lastra J. L. Connecting Web-Based IoT Devices to a CloudBased Manufacturing Platform. *IEEE Internet of Things Journal*. 2017. № 17431808. DOI: https://doi.org/10.1109/IECON.2017.8217516

17. Aazam M., Zeadally S., Harras K. A. Deploying Fog Computing in Industrial Internet of Things and Industry 4.0. *IEEE Internet of Things Journal*. 2018. № 18133157. DOI: https://doi.org/10.1109/TII.2018.2855198

18. Kabla H., Anbar M., Manickam S., Al-Amiedy T. A., Cruspe P. B., Al-Ani A. K., Karuppayah S. Applicability of Intrusion Detection System on Ethereum Attacks: A Comprehensive Review. *IEEE Access Journal*. 2022. Vol. 10. № 21863800. DOI: https://doi.org/10.1109/ACCESS.2022.3188637

19. Gupta A. The IoT Hacker's Handbook. *Apress Berkeley.* CA, 2019. 320 p. DOI: https://doi.org/10.1007/978-1-4842-4300-8

20. Doupé A., Cova M., Vigna G. Why Johnny can't pentest: An analysis of black-box web vulnerability scanners. *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Bonn, Germany. 2010. Springer: Berlin/Heidelberg. Germany. 2010. P. 111–131. DOI: https://doi.org/10.1007/978-3-642-14215-4_7

21. Bau J., Bursztein E., Gupta D., Mitchell J. State of the Art: Automated Black-Box Web Application Vulnerability Testing. *IEEE Symposium on Security and Privacy.* Oakland. CA. USA. 2010. P. 332–345. DOI: https://doi.org/10.1109/SP.2010.27

22. Parvez M., Zavarsky P., Khoury N. Analysis of effectiveness of black-box web application scanners in detection of stored SQL injection and stored XSS vulnerabilities. *IEEE: Piscataway*. NJ. USA. 2015. P. 186–191. DOI: https://doi.org/10.1109/ICITST.2015.7412085

23. Suteva N., Zlatkovski D., Mileva A. Evaluation and testing of several free/open source web vulnerability scanners. *Conference for Informatics and Information Technology (CIIT 2013).* Bitola. Macedonia. 2013. P. 221–224. URL: https://www.researchgate.net/publication/261033249_Evaluation_and_Testing_of_Several_FreeOpen_Source_Web_Vulnerability_Scanners

24. Idrissi S., Berbiche N., Guerouate F., Shibi M. Performance evaluation of web application security scanners for prevention and protection against vulnerabilities. *International Journal of Applied Engineering Research*. 2017. Vol. 12. № 21. P. 11068–11076. URL: https://www.ripublication.com/ijaer17/ijaerv12n21_76.pdf

25. Momeni E., Cardie C., Diakopoulos N. A survey on assessment and ranking methodologies for user-generated content on the web. *ACM Comput. Surv. (CSUR).* 2015. Vol. 48(3). P. 1–49. DOI: https://doi.org/10.1145/2811282

26. Kumar M., Majithia S., Bhushan S. An Efficient Model for Web Vulnerabilities Detection based on Probabilistic Classification. *Int. J. Technol. Comput. (IJTC). Techlive Solut.* 2016. P. 50–58. URL: www.semanticscholar.org/paper/An-Efficient-Model-for-Web-Vulnerabilities-based-on-Kumar-Majithia/f09ddc0501358e234a5f8e9ebec359beb91db8f1 (дата звернення 12.04.2022).

27. Raj G., Mahajan M., Singh D. Security testing for monitoring web service using Cloud. *IEEE: Piscataway.* NJ, USA. 2018. № 18043392. P. 316–321. DOI: https://doi.org/10.1109/ICACCE.2018.8441734

28. Ahmed M., Adil M., Latif S. Web application prototype: State-of-art survey evaluation. *IEEE: Piscataway.* NJ, USA. 2015. № 15756740. P. 19–24. DOI: https://doi.org/10.1109/NSEC.2015.7396339

29. Hasan A., Meva D. Web Application Safety by Penetration Testing. *Int. J. Adv. Stud. Sci. Res*. 2018. URL: www.academia.edu/38248493/Web_Application_Safety_by_Penetration_Testing (дата звернення 12.04.2022).

30. Mohammed R. Assessment of Web Scanner Tools. *Int. J. Comput. Appl*. 2016. Vol. 133(5). P. 1–4. DOI: https://doi.org/10.5120/ijca2016907794

31. Curphey M., Arawo R. Web application security assessment tools. *IEEE Secur. Priv*. 2006. Vol. 4. P. 32–41. DOI: https://doi.org/10.1109/MSP.2006.108

32. Fang Y., Long X., Liu L., Huang C. DarkHunter: A fingerprint recognition model for web automated scanners based on CNN. *2nd International Conference on Cryptography, Security and Privacy.* Guiyang, China. 2018. ACM: New York, NY, USA. 2018. P. 10–15. DOI: https://doi.org/10.1145/3199478.3199504

33. Alsaleh M., Alomar N., Alshreef M., Alarifi A., Al-Salman A. Performance-based comparative assessment of open source web vulnerability scanners. *Secur. Commun. Netw*. 2017. URL: www.hindawi.com/journals/scn/2017/6158107 (дата звернення 12.04. 2022).

34. Terry M., Oigiagbe O. D., Acharya S. A comprehensive security assessment toolkit for healthcare systems. *Colonial Academic Alliance Undergraduate Research Journal*. 2015. Vol. 4. P. 1–6. URL: https://scholarworks.wm.edu/caaurj/vol4/iss1/6

35. Furrer F. J. Safety and Security of Cyber-Physical Systems. Engineering dependable Software using Principle-based Development. 2022. 521 p. DOI: https://doi.org/10.1007/978-3-658-37182-1

36. Wu D., Ren A., Zhang W., Fan F., Liu P., Fu X., Terpenny J. Cybersecurity for digital manufacturing. *J. Manuf. Syst*. 2018. Vol. 48. P. 3–12. DOI: https://doi.org/10.1016/j.jmsy.2018.03.006

37. Bublil S., Kessler A. How Industrial IoT could Trigger the Next Cyber Catastrophe. 2020. URL: www.kovrr.com/reports/how-industrial-iot-could-trigger-the-next-cyber-catastrophe-2 (дата звернення 22.03.2020).

38. Henriquez M. Hacker breaks into Florida water treatment facility, changes chemical levels. Security Magazine. 2021. URL: https://www.securitymagazine.com/articles/94552-hacker-breaks-into-florida-water-treatment-facility-changes-chemical-levels (дата звернення 9.02.2021).

*ISSN 2522-9818 (print)*
*ISSN 2524-2296 (online)* *Innovative technologies and scientific solutions for industries. 2023. No. 2 (24)*

39. ISO/IEC 27001. Information Technology. Security Techniques. Information Security Management Systems-Requirements. ISO/IEC International Standards Organization: Geneva, Switzerland. 2005. URL: https://www.google.com/aclk?sa=l&ai=DChcSEwjp6qK3paCAAxWgn2gJHddUA2QYABABGgJ3Zg&sig=AOD64_1a4QKpT5Or3O6oAT-YqyvW4zlqgQ&q&adurl&ved=2ahUKEwifwpG3paCAAxWTiFwKHThIBeIQ0Qx6BAgPEAE

40. Top 10 Web Application Security Risks. The OWASP Foundation. 2022. URL: https://www.owasp.org (дата звернення 30.05.2022).

41. Agreindra Helmiawan M., Firmansyah E., Fadil I., Sofivan Y., Mahardika F., Guntara A. Analysis of Web Security Using Open Web Application Security Project 10. *8th International Conference on Cyber and IT Service Management (CITSM).* Pangkal, Indonesia. 2020. P. 1–5. DOI: https://doi.org/10.1109/CITSM50537.2020.9268856

42. OWASP Application Security Verification Standard. OWASP. 2022. URL: http://www.owasp.org/index.php/ASVS (дата звернення 20.02.2022).

43. Morozova O. I., Nicheporuk A. O., Tets'kyy A. H., Tkachov V. M. Methods and technologies for ensuring cybersecurity of industrial and web-based systems and networks. *National Aerospace University – "Kharkiv Aviation Institute": Scientific work.* № 4. 2021. P. 145–156 DOI: https://doi.org/10.32620/reks.2021.4.12

44. Bhorkar G. Security Analysis of an Operations Support System. School of Science. Master's Programme in Computer, Communication and Information Sciences. *Aalto University.* 2017. URL: https://aaltodoc.aalto.fi/handle/123456789/29252 (дата звернення 12.04.2022).

45. Seng L. K., Ithnin N., Said S. Z. M. The approaches to quantify web application security scanners quality: a review. *Int. J. Adv. Comput. Res*. 2018. Vol. 8. P. 285–312. DOI: https://doi.org/10.19101/IJACR.2018.838012

46. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org/

47. National Vulnerability Database. URL: https://nvd.nist.gov/

48. MITRE ATT&CK for ICS. URL: https://attack.mitre.org/techniques/ics/

**References**

1. García-Valls, M., Dubey, A., Botti, V. (2018), "Introducing the new paradigm of Social Dispersed Computing: Applications, Technologies and Challenges", *Journal of Systems Architecture*, No. 91. P. 83–102. DOI: https://doi.org/10.1016/j.sysarc.2018.05.007.

2. "W3C. The World Wide Web Consortium, The World Wide Web Consortium 2021", available at: www.w3.org. (last accessed 30.05.2022).

3. Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T. (1999), "HyperText Transfer Protocol v1.1; HTTP (RFC 2616)", The Internet Society: Reston, VA, USA, available at: https://datatracker.ietf.org/doc/html/rfc2616

4. Rescorla, E. (2000), "HTTP over TLS, RFC 1818", Internet Engineering Task Force, available at: https://datatracker.ietf.org/doc/rfc2818/

5. Fielding, R.T. (2000), "Representational State Transfer (REST). Architectural Styles and the Design of Network-based Software Architectures", *University of California, Irvine*, CA, USA, Vol. 5, P. 76–147, available at: https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm

6. Pedreira, V., Barros, D., Pinto, P. (2021), "A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead, Sensors", *MDPI Journals, Sensors*, Vol. 21(15), No. 5189. DOI: https://doi.org/10.3390/s21155189

7. García-Valls, M., Song, L. (2022), "Improving Security of Web Servers in Critical IoT Systems through Self-Monitoring of Vulnerabilities", *MDPI Journals, Sensors*, Vol. 22, No. 5004. DOI: https://doi.org/10.3390/s22135004

8. Fang, Z., Fu, H., Gu, T., Qian, Z., Jaeger, T., Hu, P., Mohapatra, P. (2021), "A model checking-based security analysis framework for IoT systems", *Journal of High-Confidence Computing*, No. 100004. DOI: https://doi.org/10.1016/j.hcc.2021.100004

9. Sarwar, A., Alnajim, A., Marwat, S. N. K., Ahmed, S., Alyahya, S., Khan, W.U. (2022), "Enhanced Anomaly Detection System for IoT Based on Improved Dynamic SBPSO", *MDPI journals, Sensors*, Vol. 22, No. 4926. DOI: https://doi.org/10.3390/s22134926

10. Ervural, B. C., Ervural, B. (2017), "Overview of Cyber Security in the Industry 4.0 Era", *Managing the Digital Transformation*, P. 267–284. DOI: https://doi.org/10.1007/978-3-319-57870-5_16

11. Alaoui, R. L., Nfaoui, E. H. (2022), "Deep Learning for Vulnerability and Attack Detection on Web Applications: A Systematic Literature Review", *MDPI Jjournals, Future Internet*, Vol. 14, No. 118. DOI: https://doi.org/10.3390/fi14040118

12. Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Guizani, M. et al. (2020), "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security", *IEEE Internet of Things Journal*, No. 19890478. DOI: https://doi.org/10.1109/COMST.2020.2988293

13. Shahid, J., Hameed, M. K., Javed, I. T., Qureshi, K. N., Ali, M., Crespi, N. (2022), "Comparative Study of Web Application Security Parameters: Current Trends and Future Directions", *MDPI Journals, Applied Sciences*, Vol. 12, No. 4077. DOI: https://doi.org/10.3390/app12084077

14. Pathak, G., Gutierrez, J., Ghobakhlou, A., Rehman, S. U. (2022), "LPWAN Key Exchange: A Centralised Lightweight Approach", *MDPI Journals, Sensors*, Vol. 22, No. 5065. DOI: https://doi.org/10.3390/s22135065

15. Surej, H. I., Ma, M., Su, R. (2022), "A Feed Forward–Convolutional Neural Network to Detect Low-Rate DoS in IoT", *Engineering Applications of Artificial Intelligence*, Vol. 114, No. 105059. DOI: https://doi.org/10.1016/j.engappai.2022.105059

16. Ferrer, B. R., Mohammed, W. M., Chen, E., Martinez Lastra, J. L. (2017), "Connecting Web-Based IoT Devices to a CloudBased Manufacturing Platform", *IEEE Internet of Things Journal*, No. 17431808. DOI: https://doi.org/10.1109/IECON.2017.8217516

*Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 2 (24)*
*ISSN 2522-9818 (print)*
*ISSN 2524-2296 (online)*

17. Aazam, M., Zeadally, S., Harras, K. A. (2018), "Deploying Fog Computing in Industrial Internet of Things and Industry 4.0", *IEEE Internet of Things Journal*, No. 18133157. DOI: https://doi.org/10.1109/TII.2018.2855198

18. Kabla, H., Anbar, M., Manickam, S., Al-Amiedy, T. A., Cruspe, P. B., Al-Ani, A. K., Karuppayah, S. (2022), "Applicability of Intrusion Detection System on Ethereum Attacks: A Comprehensive Review", *IEEE Access Journal*, Vol. 10, No. 21863800. DOI: https://doi.org/10.1109/ACCESS.2022.3188637

19. Gupta, A. (2019), *The IoT Hacker's Handbook*, Apress Berkeley, CA, 320 p. DOI: https://doi.org/10.1007/978-1-4842-4300-8

20. Doupé, A., Cova, M., Vigna, G. (2010), "Why Johnny can't pentest: An analysis of black-box web vulnerability scanners", *In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Bonn, Germany, Springer: Berlin/Heidelberg, Germany. P. 111–131. DOI: https://doi.org/10.1007/978-3-642-14215-4_7

21. Bau, J., Bursztein, E., Gupta, D., Mitchell, J. (2010), "State of the Art: Automated Black-Box Web Application Vulnerability Testing", *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, P. 332–345. DOI: https://doi.org/10.1109/SP.2010.27

22. Parvez, M., Zavarsky, P., Khoury, N. (2015), "Analysis of effectiveness of black-box web application scanners in detection of stored SQL injection and stored XSS vulnerabilities", *IEEE: Piscataway*, NJ, USA, P. 186–191. DOI: https://doi.org/10.1109/ICITST.2015.7412085

23. Suteva, N., Zlatkovski, D., Mileva, A. (2013), "Evaluation and testing of several free/open source web vulnerability scanners", *Conference for Informatics and Information Technology (CIIT 2013)*, Bitola, Macedonia, P. 221-224, available at: https://www.researchgate.net/publication/261033249_Evaluation_and_Testing_of_Several_FreeOpen_Source_Web_Vulnerability_Scanners

24. Idrissi, S., Berbiche, N., Guerouate, F., Shibi, M. (2017), "Performance evaluation of web application security scanners for prevention and protection against vulnerabilities", *International Journal of Applied Engineering Research*, Vol. 12, No. 21, P. 11068–11076, available at: https://www.ripublication.com/ijaer17/ijaerv12n21_76.pdf

25. Momeni, E., Cardie, C., Diakopoulos, N. (2015), "A survey on assessment and ranking methodologies for user-generated content on the web", *ACM Comput. Surv (CSUR)*, Vol. 48(3), P. 1–49. DOI: https://doi.org/10.1145/2811282

26. Kumar, M., Majithia, S., Bhushan, S. (2016), "An Efficient Model for Web Vulnerabilities Detection based on Probabilistic Classification", *Int. J. Technol. Comput. (IJTC), Techlive Solut*, P. 50–58, available at: www.semanticscholar.org/paper/An-Efficient-Model-for-Web-Vulnerabilities-based-on-Kumar-Majithia/f09ddc0501358e234a5f8e9ebec359beb91db8f1. (last accessed 12.04.2022).

27. Raj, G., Mahajan, M., Singh, D. (2018), "Security testing for monitoring web service using Cloud", *IEEE: Piscataway*, NJ, USA, No. 18043392. P. 316–321. DOI: https://doi.org/10.1109/ICACCE.2018.8441734

28. Ahmed, M., Adil, M., Latif, S. (2015), "Web application prototype: State-of-art survey evaluation", *IEEE: Piscataway*, NJ, USA, No. 15756740, P. 19–24. DOI: https://doi.org/10.1109/NSEC.2015.7396339

29. Hasan, A., Meva, D. (2018), "Web Application Safety by Penetration Testing", *Int. J. Adv. Stud. Sci. Res.*, available at: www.academia.edu/38248493/Web_Application_Safety_by_Penetration_Testing (last accessed 12.04.2022)

30. Mohammed, R. (2016), "Assessment of Web Scanner Tools", *Int. J. Comput. Appl*., Vol. 133(5), P. 1–4. DOI: https://doi.org/10.5120/ijca2016907794

31. Curphey, M., Arawo, R. (2006), "Web application security assessment tools", *IEEE Secur. Priv*., Vol. 4, P. 32–41. DOI: https://doi.org/10.1109/MSP.2006.108

32. Fang, Y., Long, X., Liu, L., Huang, C. (2018), "DarkHunter: A fingerprint recognition model for web automated scanners based on CNN", *2nd International Conference on Cryptography, Security and Privacy*, Guiyang, China, ACM: New York, USA, P. 10–15. DOI: https://doi.org/10.1145/3199478.3199504

33. Alsaleh, M., Alomar, N., Alshreef, M., Alarifi, A., Al-Salman, A. (2017), "Performance-based comparative assessment of open source web vulnerability scanners", *Secur. Commun. Netw*, available at: www.hindawi.com/journals/scn/2017/6158107 (last accessed 12.04. 2022).

34. Terry, M., Oigiagbe, O. D., Acharya, S. (2015), "A comprehensive security assessment toolkit for healthcare systems", *Colonial Academic Alliance Undergraduate Research Journal*, Vol. 4, P. 1–6, available at: https://scholarworks.wm.edu/caaurj/vol4/iss1/6

35. Furrer, F. J. (2022), *Safety and Security of Cyber-Physical Systems*, Engineering dependable Software using Principle-based Development, 521 p. DOI: https://doi.org/10.1007/978-3-658-37182-1

36. Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., Terpenny, J. (2018), "Cybersecurity for digital manufacturing", *J. Manuf. Syst*., Vol. 48, P. 3–12. DOI: https://doi.org/10.1016/j.jmsy.2018.03.006

37. Bublil, S., Kessler, A. (2020), "How Industrial IoT could Trigger the Next Cyber Catastrophe", available at: www.kovrr.com/reports/how-industrial-iot-could-trigger-the-next-cyber-catastrophe-2 (last accessed 22.03.2020)

38. Henriquez, M. (2021), "Hacker breaks into Florida water treatment facility, changes chemical levels", Security Magazine, available at: https://www.securitymagazine.com/articles/94552-hacker-breaks-into-florida-water-treatment-facility-changes-chemical-levels (last accessed 9.02.2021)

39. ISO/IEC 27001 (2005), "Information Technology. Security Techniques", Information Security Management Systems–Requirements. ISO/IEC International Standards Organization: Geneva, Switzerland, available at: https://www.google.com/aclk?sa=l&ai=DChcSEwjp6qK3paCAAxWgn2gJHddUA2QYABABGgJ3Zg&sig=AOD64_1a4QKpT5Or3O6oAT-YqyvW4zlqgQ&q&adurl&ved=2ahUKEwifwpG3paCAAxWTiFwKHThIBeIQ0Qx6BAgPEAE

40. "Top 10 Web Application Security Risks" (2022), The OWASP Foundation, available at: https://www.owasp.org (last accessed 30.05.2022).

41. Helmiawan, M. A., Firmansyah, E., Fadil, I., Sofivan, Y., Mahardika, F., Guntara, A. (2020), "Analysis of Web Security Using Open Web Application Security Project 10", *International Conference on Cyber and IT Service Management (CITSM)*, Pangkal, Indonesia, P. 1–5. DOI: https://doi.org/10.1109/CITSM50537.2020.9268856

*ISSN 2522-9818 (print)*
*ISSN 2524-2296 (online)* *Innovative technologies and scientific solutions for industries. 2023. No. 2 (24)*

42. OWASP Application Security Verification Standard, (2022), *OWASP*, available at: http://www.owasp.org/index.php/ASVS (last accessed 20.02.2022).

43. Morozova, O. I., Nicheporuk, A. O., Tets'kyy, A. H., Tkachov, V. M. (2021), "Methods and technologies for ensuring cybersecurity of industrial and web-based systems and networks", *National Aerospace University – "Kharkiv Aviation Institute": Scientific work*, No. 4. P. 145–156. DOI: https://doi.org/10.32620/reks.2021.4.12

44. Bhorkar, G. (2017), "Security Analysis of an Operations Support System", School of Science, Master's Programme in Computer, Communication and Information Sciences, *Aalto University*, available at: https://aaltodoc.aalto.fi/handle/123456789/29252 (last accessed 12.04.2022).

45. Seng, L. K., Ithnin, N., Said, S. Z. M. (2018), "The approaches to quantify web application security scanners quality: a review", *Int. J. Adv. Comput. Res.*, Vol. 8, P. 285–312. DOI: https://doi.org/10.19101/IJACR.2018.838012

46. "Common Vulnerabilities and Exposures", available at: https://cve.mitre.org/

47. "National Vulnerability Database", available at: https://nvd.nist.gov/

48. "MITRE ATT&CK for ICS", available at: https://attack.mitre.org/techniques/ics/

*Received 16.06.2023*

*Відомості про авторів / About the Authors*

**Мерзлікін Євген Васильович** – Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, Харків, Україна; e-mail: y.v.merzlikin@csn.khai.edu; ORCID ID: https://orcid.org/0000-0001-8613-1121

**Бабешко Євген Васильович** – кандидат технічних наук, доцент, Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", доцент кафедри комп'ютерних систем, мереж і кібербезпеки, Харків, Україна; e-mail: e.babeshko@csn.khai.edu; ORCID ID: https://orcid.org/0000-0002-4667-2393

**Merzlikin Eugene** – National Aerospace University "Kharkiv Aviation Institute", PhD Student, Computer Systems, Networks and Cybersecurity Department, Kharkiv, Ukraine.

**Babeshko Ievgen** – PhD (Engineering Sciences), Associate Professor, National Aerospace University "Kharkiv Aviation Institute", Associate Professor at the Computer Systems, Networks and Cybersecurity Department, Kharkiv, Ukraine.

## CYBERSECURITY ANALYSIS OF WEB-ORIENTED INDUSTRIAL IOT-SYSTEMS

In modern world cybersecurity ensuring is one of the most crucial issues, especially in the context of the dynamic development of web-oriented industrial Internet of Things (IoT) systems. The subject of research of the paper is cybersecurity ensuring of web-oriented industrial IoT systems. **The purpose** of the paper is to analyze existing methods of cybersecurity analysis, identify limitations, and formulate requirements for a new assessment concept, which includes ways to eliminate identified limitations. **Tasks to be solved**: analysis of existing methods, tools and technologies for the organization of web-oriented industrial IoT systems and the problems of ensuring their cyber security. Applied **methods**: source analysis, system analysis. Obtained **results**: The analysis of sources has shown that the problems of industrial IoT systems cybersecurity ensuring are relevant due to the use in one system of both the latest information technologies (IT) and traditional operational technologies (OT), such as industrial protocols, etc. In addition, the ever-increasing number and types of attacks aimed specifically at industrial IoT systems are additional drivers for the further development of the cybersecurity assessing and ensuring methods. A generalized concept of the cybersecurity assessing and ensuring process of web-oriented industrial IoT systems is proposed, which includes the stages of identification, analysis, security enhancement, detection and protection. **Conclusions**: The issue of the cybersecurity ensuring of the web-oriented industrial IoT systems is extremely relevant, and the existing analysis methods and ensuring means do not fully satisfy the existing requirements for such systems. That is why the development and implementation of the proposed concept of cybersecurity assessing and ensuring will allow to significantly influence the improvement of industrial IoT systems cybersecurity.

**Keywords:** cyber security; IoT; Industry 4.0; web-oriented systems; web-application security; detection of vulnerabilities; detection of web attacks.

*Бібліографічні описи / Bibliographic descriptions*

Мерзлікін Є. В., Бабешко Є. В. Аналіз кібербезпеки веборієнтованих індустріальних *IoT*-систем. *Сучасний стан наукових досліджень та технологій в промисловості*. 2023. № 2 (24). С. 131–144. DOI: https://doi.org/10.30837/ITSSI.2023.24.131

Merzlikin, E., Babeshko, I. (2023), "Cybersecurity analysis of web-oriented industrial IOT-systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (24), P. 131–144. DOI: https://doi.org/10.30837/ITSSI.2023.24.131