https://orcid.org/0000-0002-5080-1856
https://orcid.org/0009-0004-2606-8166

УДК 004.056.5

Ю.М. ЛИСЕЦЬКИЙ[*], О.Б. САЛИВОН[*]

КОМПЛЕКСНИЙ ПІДХІД ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

[*]ДП «ЕС ЕНД ТІ УКРАЇНА», м. Київ, Україна

Анотація. *Поняття промислового інтернету речей (Industrial Internet of Things, IIoT) вперше було озвучене в 2011 р. у рамках Індустріальної революції 4.0 на міжнародній виставці в Ганновері й стало підсумком діяльності німецьких науковців, які на рівні концепції поєднали використання великої кількості датчиків та контролерів, об'єднаних у мережу для досягнення певного виробничого результату. Це концепція, яка поєднує в собі потужність глобальної інформаційної мережі та традиційної промисловості. Сучасні виробничі підприємства все більше інтегрують цифрові технології, перетворюючись на складні системи, що поєднують фізичні та кібернетичні компоненти. Це підвищує ефективність виробництва, але водночас створює нові ризики, тому що системи IIoT набагато вразливіші до кібератак порівняно зі звичайними комп'ютерними мережами. І це відбувається внаслідок таких причин: складність і масштабність; різноманітність протоколів; застаріле обладнання; недостатня увага до безпеки; відсутність кваліфікованих фахівців; відсутність єдиного стандарту безпеки. Наслідки кібератак на системи IIoT можуть бути катастрофічними і мати такі результати: зупинка виробництва; пошкодження обладнання; витік конфіденційної інформації про виробничі процеси, технології тощо; репутаційні втрати. Для досягнення своєї мети зловмисники використовують такі способи: атака підбором паролів; атака «людина посередині»; підробка ідентифікаторів; використання незахищених портів та протоколів; пошук вразливостей ПЗ; застосування комп'ютерних вірусів; атака та відмова в обслуговуванні. Цілеспрямовані та розподілені атаки можуть зробити систему IIoT недоступною, що зі свого боку призведе до зупинки виробництва. Запропоновано комплексний підхід щодо захисту систем IIoT та описано заходи, які він містить. Наведена загальна архітектура захисту системи IIoT, яка поєднує три методи апаратного захисту (PUF, TRM, HSM), що створює багаторівневий захист даних. Кожен із цих методів виконує свою унікальну роль, доповнюючи один одного і забезпечуючи високий рівень кібербезпеки.*

Ключові слова: *промисловий інтернет речей, способи атак, архітектура захисту, методи захисту, комплексний підхід.*

Abstract. *The concept of the Industrial Internet of Things (IIoT) was first mentioned in 2011 as part of Industry 4.0 at an international exhibition in Hannover. It was the result of the work of German scientists who combined the use of a large number of sensors and controllers connected to a network to achieve a specific production result. This concept combines the power of a global information network with traditional industry. Modern manufacturing enterprises are increasingly integrating digital technologies, transforming into complex systems that combine physical and cybernetic components. This increases production efficiency but at the same time creates new risks because IIoT systems are much more vulnerable to cyberattacks than conventional computer networks. This is due to the following factors: complexity and scale, diversity of protocols, outdated equipment, insufficient attention to security, the lack of qualified specialists, and the absence of a single security standard. The consequences of cyberattacks on IIoT systems can be catastrophic and result in production stoppages, equipment damage, leaks of confidential information about production processes, technologies, etc., and reputational damage. To achieve their goals, attackers use the following methods: password guessing attacks, man-in-the-middle attacks, identifier spoofing, use of unprotected ports and protocols, search for software vulnerabilities, use of computer viruses, and denial-of-service attacks. Targeted and distributed attacks can render the IIoT system inaccessible, which in turn will lead to production stoppages. A comprehensive approach to protecting IIoT*

ISSN 1028-9763. Математичні машини і системи. 2026. № 1

systems is proposed and its measures are described. A general architecture for protecting IIoT systems is presented, combining three hardware protection methods (PUF, TRM, HSM) to create multi-layered data protection. Each of these methods plays a unique role, complementing each other and ensuring a high level of cybersecurity.
Keywords: *Industrial Internet of Things, attack methods, protection architecture, protection methods comprehensive approach.*

DOI: 10.34121/1028-9763-2026-1-15-20

1. Вступ

Поняття промислового інтернету речей (Industrial Internet of Things, IIoT) вперше було озвучене в 2011 р. у рамках Індустріальної революції 4.0 на міжнародній виставці в Ганновері і стало підсумком діяльності німецьких науковців, які на рівні концепції поєднали використання великої кількості датчиків та контролерів, об'єднаних у мережу для досягнення певного виробничого результату [1].

IIoT — це концепція, яка поєднує в собі потужність глобальної інформаційної мережі та традиційної промисловості [2]. Вона об'єднує новітні досягнення в сфері інформаційних та виробничих технологій, як-от штучний інтелект, високошвидкісний обмін даними, бездротові технології, обробка великих об'ємів інформації в режимі реального часу та багато іншого. На практиці це реалізація виробництва товарів, де на кожному етапі створення товару, починаючи від проєктування до надання споживачу результату, воно перебуває під контролем інформаційних систем: кожна машина, кожен інструмент та навіть найменша деталь на підприємстві підключені до мережі та обмінюються даними в реальному часі. Це і є мережа промислового інтернету речей, яка впливає на роботу обладнання, що виготовляє товари та надає послуги. Виникає інтеграція фізичного та цифрового світів. IIoT створює місток між фізичними об'єктами — сенсорами, контролерами, роботами та цифровим світом, який містить у собі програмне забезпечення, центри обробки даних та надання аналітики [3].

Використання концепції IIoT на практиці дає можливість набагато більше пришвидшити цикли виробництва, надання послуг та прийняття управлінських рішень. Разом з тим використання IIoT хоча і відкриває перед виробниками великі перспективи, воно також створює нові ризики, пов'язані з кібербезпекою. Зростання кількості підключених пристроїв робить промислові підприємства більш вразливими до хакерських атак, що може призвести до порушення виробничих процесів і значних фінансових втрат. Тому проблема забезпечення кібербезпеки систем IIoT потребує більш глибоких досліджень.

Мета статті — дослідити особливості систем IIoT у контексті вразливості для кібератак та запропонувати заходи щодо забезпечення їх кібербезпеки.

2. Особливості систем IIoT

Сили кібероперацій різних країн, терористичні угрупування та злочинці цікавляться можливістю впливу на реальність за допомогою втручання в роботу глобальної інформаційної мережі і мереж IIoT, які є її частиною [4]. Кількість втручань зростає з кожним роком. Спочатку це виглядає як розвідка та з'ясування того, яка конфіденційна інформація може бути отримана, далі отримання цієї інформації в режимі реального часу. Але з часом змінюються задачі та можливості впливу через інформаційні системи (ІС). Перехоплення, керування військовими дронами, саботаж на транспортних шляхах та виробництві можуть призвести до реальних жертв, а не лише до фінансових та репутаційних збитків, як у випадку з втручанням в автоматизовані ІС [5]. Промисловий інтернет речей, незважаючи на всі свої переваги, стикається з низкою серйозних загроз, які можуть призвести до порушення виробничих процесів, значних фінансових втрат та навіть

фізичної шкоди. Всесвітній економічний форум викликав певну тривогу, зазначивши, що «саме виробництво було найбільшим об’єктом для кібератак».

Компанія IBM підрахувала, що у 2022 році понад третина всіх спроб вимагання грошей кіберзлочинцями за розблокування даних була спрямована саме на виробничі підприємства. Це пояснюється тим, що такі підприємства не можуть дозволити собі тривалі простої. Зі свого боку, компанія SonicWall повідомила, що у 2023 році кількість шкідливих програм, які атакують пристрої інтернету речей, зросла на 37 %. Це означає, що хакери все частіше націлюються на різні пристрої, підключені до інтернету, наприклад, датчики, контролери, камери та промислове обладнання.

Отже, сучасні виробничі підприємства все більше інтегрують цифрові технології, перетворюючись на складні системи, що поєднують фізичні та кібернетичні компоненти. Це підвищує ефективність виробництва, але водночас створює нові ризики, тому що системи IIoT набагато вразливіші до кібератак порівняно зі звичайними комп'ютерними мережами. І це відбувається внаслідок таких причин:

1. Складність і масштабність. Системи IIoT складаються з великої кількості взаємопов'язаних пристроїв, від датчиків і контролерів до роботів і систем автоматизації. Така масштабність ускладнює їх захист, оскільки кожна нова ланка в системі може стати потенційною вразливістю.

2. Різноманітність протоколів. Різні пристрої в системах IIoT можуть використовувати різні комунікаційні протоколи, що ускладнює забезпечення єдиного рівня безпеки для всієї системи.

3. Застаріле обладнання. Багато промислових підприємств використовують обладнання, яке було встановлено багато років тому. Таке обладнання часто має вбудоване програмне забезпечення (ПЗ) зі значними вразливостями, якими можуть скористатися зловмисники.

4. Недостатня увага до безпеки. Історично склалося так, що безпека промислових систем часто відходила на другий план. Підприємства більше зосереджувалися на підвищенні продуктивності та зниженні витрат, ніж на захисті своїх систем від кібератак.

5. Відсутність кваліфікованих фахівців. Існує дефіцит фахівців із кібербезпеки, які мають досвід роботи з промисловими системами. Це ускладнює захист таких систем від кібератак.

6. Відсутність єдиного стандарту безпеки. На відміну від IT-інфраструктури, в промисловій автоматизації немає єдиного набору стандартів безпеки, що ускладнює забезпечення захисту. Наслідки кібератак на системи IIoT можуть бути катастрофічними і мати такі результати: зупинка виробництва, пошкодження обладнання, витік конфіденційної інформації про виробничі процеси, технології тощо, репутаційні втрати.

3. Способи атак на системи IIoT

Для здійснення атак на системи IIoT зловмисники намагаються проникнути в середину мережі. Вони можуть підібрати варіант проникнення всередину, використовуючи вади ПЗ, конфігурування системи, недостатню підготовку обслуговуючого персоналу або поєднати та комбінувати існуючі недоліки системи IIoT. Для досягнення своєї мети зловмисники використовують такі способи:

1. Атака підбором паролів. Слабкі паролі є легкою мішенню для зловмисників.

2. Атака «людина посередині». Полягає в перехопленні даних між елементами системи та порушенні їхньої цілісності або маніпулюванні ними. Зміна даних, що передаються між пристроями, може призвести до прийняття помилкових рішень та пошкодження обладнання.

3. Підробка ідентифікаторів. Наявність проблем з автентифікацією, що призведе до отримання несанкціонованого доступу до системи.

4. Використання незахищених портів та протоколів. Помилки в конфігурації пристроїв можуть створити вразливості, якими можуть скористатися зловмисники.

5. Пошук вразливостей ПЗ. Застаріле ПЗ з відомими вразливостями, які не були виправлені, може бути легко зламане.

6. Застосування комп'ютерних вірусів. Наявність вірусної небезпеки призводить до того, що комп'ютерний вірус, розрахований на контролери та системи керування, може зіпсувати роботу обладнання або продукцію, яку виробляє підприємство.

7. Атака та відмова в обслуговуванні. Цілеспрямовані та розподілені атаки можуть зробити систему IIoT недоступною, що зі свого боку призведе до зупинки виробництва.

4. Комплексний підхід щодо захисту систем IIoT

Щоб захистити системи IIoT, необхідно застосовувати комплексний підхід, який містить у собі такі заходи:

1. Zero Trust. Прийняття архітектури нульової довіри на підприємстві є стратегічним кроком для підвищення безпеки систем IIoT. Цей підхід ґрунтується на фундаментальному принципі, що нікому не довіряти та все треба перевіряти. Доступ надається виключно за принципом «необхідність знати», що значно знижує ризик несанкціонованого входу та потенційних кіберзагроз.

2. Audit. Усунення ризиків кібербезпеки в системі IIoT вимагає чіткого плану, починаючи з детальної оцінки ризиків. Оцінка ризику допомагає зрозуміти, що може піти не так, наскільки ймовірно це станеться та які наслідки будуть, якщо це станеться. Тут розглядаються пристрої, датчики, контролери, пункти керування та способи їх взаємодії. Після визначення та ранжування ризиків необхідно розробити план заходів для їх зменшення.

3. Security Awareness. Наскільки б досконалими не були технічні засоби захисту, останнє слово завжди залишається за людиною. Тому важливо систематично навчати співробітників основам кібербезпеки, прищеплюючи їм звичку використовувати складні паролі, двофакторну автентифікацію та інші ефективні методи захисту.

4. Update. Для забезпечення кібербезпеки систем IIoT протягом усього їхнього життєвого циклу необхідно розробити ефективні процеси автоматичного оновлення. Це особливо важливо в умовах, коли кількість пристроїв у мережі постійно зростає. Підприємства мають віддавати пріоритет структурованим процесам оновлення, вибираючи системи, які підтримують автоматичні оновлення та мають тривалий термін експлуатації.

5. LAN Segmentation. Відокремлення мереж для підключених машин від загальних офісних або гостьових мереж має важливе значення для підвищення безпеки. Доступ до цих спеціалізованих мереж необхідно суворо контролювати, а облікові дані надавати лише необхідному персоналу, щоб запобігти несанкціонованому доступу та потенційним порушенням безпеки.

6. Access Management. Контроль доступу, автентифікація та шифрування є основними для захисту каналів мережевого зв'язку. Не підлягає обговоренню гарантія безпеки всіх комунікацій, включаючи передачу даних і віддалений доступ між пристроями IIoT та системами керування. Крок за кроком мережа захищається від несанкціонованого проникнення, а цілісність даних, що передаються, зберігається. Впровадження та використання систем Privileged Access Management (PAM) та Secure Remote Access (SRA) можна вважати обов'язковими для підприємств з IIoT.

7. Unified cybersecurity management. Централізація управління кібербезпекою має важливе значення для підвищення рівня захисту в IT-мережі організації та мережі систем IIoT. Уніфікована платформа моніторингу та керування дозволяє підрозділу кібербезпеки спостерігати за всіма процесами та швидко впроваджувати засоби контролю та політики в ІС.

8. Використання методів апаратного захисту. Physically Unclonable Function (PUF), Trusted Platform Module (TRM) та Hardware Security Module (HSM). Кожен із методів може бути використаний як окремо, так і в поєднанні з іншими. Поєднання методів PUF, TRM та HSM в одній системі IIoT створює багаторівневий захист даних. Кожен із цих методів виконує свою унікальну роль, доповнюючи один одного і забезпечуючи високий рівень кібербезпеки.

Загальна архітектура захисту системи IIoT, що поєднує всі три методи, має бути така:

1. На базовому рівні знаходиться PUF, якій генерує унікальний цифровий відбиток, заснований на фізичних характеристиках пристрою. Цей відбиток неможливо точно відтворити, що робить його ідеальним для автентифікації пристрою в системі IIoT. PUF може використовуватися для зберігання частини ключа шифрування, що робить його більш стійким до атак.

2. На середньому рівні знаходиться TRM, задачею якого є перевірка цілісності системи IIoT. TRM постійно моніторить її стан, перевіряючи, чи не було внесено змін до програмного забезпечення або апаратного забезпечення. TRM може генерувати криптографічні ключі для шифрування даних та автентифікації, які зберігає в безпечному середовищі, захищаючи їх від несанкціонованого доступу.

3. На верхньому рівні знаходиться HSM. Це спеціалізовані пристрої, призначені для захисту криптографічних ключів і конфіденційних даних, запобігаючи несанкціонованому доступу та підробці. Їх інтеграція в інфраструктуру безпеки знижує ризик компрометації даних. HSM виконує складні криптографічні операції, як-от шифрування, дешифрування та підпис цифрових документів. Він захищений від фізичних атак і має вбудовані механізми захисту від програмних атак.

Взаємодія методів PUF, TRM та HSM відбувається так:

1. PUF та TRM. PUF забезпечує унікальний ідентифікатор пристрою, який використовується TRM для перевірки цілісності системи. TRM може також використовувати PUF для генерації частини ключа, що зберігається в HSM.

2. TRM та HSM. TRM генерує ключі, які передаються в HSM для зберігання. HSM виконує криптографічні операції з використанням цих ключів.

Отже, поєднання TRM, PUF і HSM створює потужну і гнучку архітектуру для захисту даних. Ця архітектура може бути використана в різних галузях, де висуваються високі вимоги до кібербезпеки, як-от фінанси, охорона здоров'я, державні установи тощо.

5. Висновки

Досліджено особливості систем IIoT у контексті вразливості для кібератак і способи здійснення атак на них. Запропоновано комплексний підхід щодо захисту систем IIoT та описано заходи, які він містить. Наведено загальну архітектуру захисту системи IIoT, яка поєднує три методи апаратного захисту (PUF, TRM, HSM), що створює багаторівневий захист даних. Кожен із цих методів виконує свою унікальну роль, доповнюючи один одного і забезпечуючи високий рівень кібербезпеки.

Отже, системи промислового інтернету речей стають дедалі більш поширеними, але разом з тим вони також стають все більш вразливими до кібератак. Захист систем IIoT є досить складним завданням, яке вимагає комплексного підходу. Промислові та інфраструктурні підприємства і організації мають інвестувати в безпеку своїх систем IIoT і за допомогою розглянутих засобів і методів покращити їх захист, щоб уникнути серйозних наслідків кібератак.

СПИСОК ДЖЕРЕЛ

1. Boyes H., Hallaq B., Cunningham J., Watson T. The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*. 2018. Vol. 101. P. 1–12.
2. Industrial Internet of Things (IIoT). URL: https://www.incom-tech.com.ua/iiot (дата звернення: 15.03.2025).
3. Калбазов Д.Й., Лисецький Ю.М. Технологія Internet of Things. *Математичні машини і системи*. 2019. № 2. С. 43–50.
4. Лисецький Ю.М., Данченко О.І. Аналіз проблем забезпечення кібербезпеки при використанні технології Інтернету речей. *Вісник воєнної розвідки*. 2024. № 82. С. 46–50.
5. Бобров С.І., Лисецький Ю.М. Нові небезпеки інформаційної безпеки або зброя масового зараження. *Математичні машини і системи*. 2018. № 1. С. 41–50.

Стаття надійшла до редакції 16.12.2025 / прийнята до друку 12.02.2026