УДК 004.056:355.45
DOI https://doi.org/10.32782/2663-5941/2025.1.2/32

Прокопович-Ткаченко Д.І.
Університет митної справи та фінансів

Звєрєв В.П.
Державний торговельно-економічний університет

Козаченко І.М.
Державний центр кіберзахисту
Державної служби спеціального зв'язку та захисту інформації України

КІБЕРЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ ФІЗИЧНОЇ ІНФРАСТРУКТУРИ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ (ILOT)

Стаття пропонує детальний аналіз загроз безпеки промислового інтернету речей (IIoT), який охоплює весь спектр потенційних вразливостей – від фізичного рівня взаємодії з периферійними пристроями до прикладного рівня, де можуть виникати складні сценарії атак, зокрема завдяки відсутності належних механізмів аутентифікації та шифрування. Автори наголошують, що загрози, пов'язані зі шкідливим програмним забезпеченням, здатні не лише викрадати дані чи порушувати роботу мереж, а й призводити до небезпечних збоїв у роботі фізичних компонентів промислових систем, що підтверджується прикладом Stuxnet.

Особливу увагу в статті приділено кожному рівню моделі OSI, аналізуючи, як саме можуть бути скомпрометовані фізичні пристрої, канали зв'язку, мережеві й транспортні протоколи, а також сеансові й прикладні служби. Розглядаються ключові ризики, до яких належить несанкціонований доступ до обладнання на фізичному рівні, перехоплення або модифікація пакетів на мережевому рівні, використання вразливостей протоколів чи сервісів на вищих рівнях тощо. Підкреслюється, що без відповідних превентивних заходів недоліки на кожному з цих рівнів можуть бути використані зловмисниками для проведення комплексних, багатокрокових атак.

У роботі підкреслено важливість комплексного захисту, що включає як технічні, так і організаційні компоненти. Серед таких заходів – застосування кіберімунітетних технологій, здатних забезпечити одночасний захист на кількох рівнях; впровадження ефективних систем виявлення вторгнень; дотримання принципів безпеки ланцюгів постачання, оскільки вразливості часто потрапляють у систему ще на етапі розроблення або доставки компонентів; а також регулярне оновлення програмного забезпечення та активне підвищення обізнаності персоналу.

Завдяки таким комплексним підходам до захисту індустріальні системи можуть суттєво знизити ризики, пов'язані з кібератаками, та забезпечити високу стійкість операційних процесів. Запропоновані рекомендації та методи запобігання атакам можуть бути корисними для широкого кола підприємств, що прагнуть захистити як свої дані, так і фізичні елементи виробничих систем, забезпечуючи безперервність та надійність функціонування критичної інфраструктури.

Ключові слова: *IIoT, шкідливе ПЗ, кібератаки, кібербезпека, фізична інфраструктура, кіберімунітет.*

Постановка проблеми. IIoT є ключовим елементом сучасного індустріального виробництва, що забезпечує автоматизацію, підвищення ефективності виробничих процесів і моніторинг критичних систем у режимі реального часу. Інтеграція фізичних пристроїв, сенсорів і програмного забезпечення створює нові можливості для оптимізації ресурсів і управління складними процесами. Проте розвиток IIoT супроводжується значними викликами, особливо у сфері кібербезпеки, оскільки збільшення мережевої взаємодії між пристроями створює нові ризики для безпеки [1, с. 45].

Сучасні кіберзагрози включають використання шкідливого програмного забезпечення, яке може впливати на фізичні компоненти промислової інфраструктури. Наприклад, вірус Stuxnet став символом того, як шкідливі програми можуть завдавати фізичної шкоди обладнанню [7, с. 112]. Такі атаки демонструють потребу в розробці інно-

ваційних підходів до захисту, які охоплюють не лише технологічний рівень, а й соціальні та організаційні аспекти [3, с. 87].

Особливо важливо розглядати ці питання напередодні впровадження емерджентно-адаптивних систем, що базуються на глибоких нейронних мережах. Ці системи здатні зберігати так звані "синаптичні структури" або "образи" можливих атак, що створює основу для прогнозування та попередження загроз [4, с. 132]. Наприклад, використання алгоритмів машинного навчання у рамках таких систем дозволяє аналізувати величезні обсяги даних, зокрема поведінкові патерни пристроїв IIoT, ідентифікувати аномалії та формувати стратегії захисту [5, с. 56].

Використання адаптивних систем у промислових середовищах може забезпечити значне підвищення рівня безпеки, зокрема завдяки інтеграції з концепціями "кіберімунітету" – багаторівневого захисту, який охоплює всі рівні моделі OSI [8, с. 78]. Такі підходи також сприяють побудові стійких ланцюгів постачання, що є критично важливими для уникнення атак, пов'язаних із підміною компонентів або використанням апаратних вразливостей [6, с. 91].

Наукові дослідження підтверджують, що емерджентні системи не лише знижують ризики атак, але й забезпечують можливість швидкої адаптації до нових загроз. Наприклад, сучасні підходи до забезпечення кібербезпеки IIoT включають регулярні оновлення програмного забезпечення, аудити безпеки та навчання персоналу для виявлення загроз [2, с. 66]. Особлива увага приділяється технологіям блокчейну, які забезпечують високий рівень безпеки завдяки використанню розподілених баз даних і криптографічних алгоритмів [10, с. 102].

Таким чином, розробка та впровадження комплексних стратегій кібербезпеки для IIoT є необхідною умовою для розвитку сучасних промислових систем. Застосування адаптивних систем, які враховують синаткхури атак і вивчають поведінку загроз у режимі реального часу, дозволяє не лише захищати інфраструктуру, але й забезпечувати її стійкість до майбутніх викликів [9, с. 85].

Аналіз останніх досліджень і публікацій. Розглянуто існуючі дослідження у сфері безпеки промислового інтернету речей (IIoT), що демонструють важливість захисту фізичних компонентів від шкідливого програмного забезпечення. Проблема фізичної безпеки пристроїв у контексті шкідливого ПЗ залишається актуальною через постійний розвиток технологій, які інтегрують фізичні та цифрові системи. Найвідомішим прикладом є вірус Stuxnet, який завдав фізичної шкоди іранським центрифугам для збагачення урану, вивівши з ладу тисячі пристроїв за допомогою маніпуляцій програмним забезпеченням [2, с. 35]. Цей інцидент став символом того, як кібератаки можуть впливати на критичну інфраструктуру, спричиняючи фізичні руйнування [7, с. 101].

Проте, попри відомість деяких прикладів, кіберінциденти, пов'язані зі шкідливим впливом на фізичні елементи IIoT, залишаються недостатньо вивченими. Більшість існуючих досліджень зосереджуються на аналізі вразливостей програмного забезпечення та мережевих компонентів, тоді як аспекти фізичного впливу, такі як маніпуляції з датчиками, виконавчими механізмами або енергетичними системами, вивчені обмежено [4, с. 89]. У літературі також бракує конкретної інформації про реальні кейси атак на фізичні елементи IIoT, що обмежує можливості моделювання загроз і розробки ефективних стратегій захисту [6, с. 45].

Таким чином, дослідження, які стосуються кіберінцидентів із шкідливим впливом на фізичні компоненти IIoT, потребують значного розширення. Особлива увага має бути приділена збору емпіричних даних, вивченню уразливостей фізичної інфраструктури та створенню математичних моделей, що дозволяють прогнозувати можливі сценарії атак [1, с. 67]. Крім того, впровадження систем прогнозування загроз на основі глибоких нейронних мереж може забезпечити ідентифікацію та попередження шкідливого впливу на фізичні елементи ще на ранніх стадіях атаки [5, с. 112].

Постановка завдання. Основною метою дослідження є ідентифікація найбільших ризиків для фізичної інфраструктури промислового інтернету речей (IIoT) та розробка ефективних методів захисту, що враховують сучасні виклики у сфері кібербезпеки. Особливу увагу необхідно приділити аналізу загроз, пов'язаних із кіберзлочинами, які можуть впливати на критичні сегменти промислової інфраструктури, включаючи об'єкти енергетики, транспорту, виробництва та системи життєзабезпечення.

Додатковою метою є впровадження емерджентно-адаптивних систем захисту, які здатні враховувати специфіку алгоритмів атак та автоматично адаптуватися до змінюваного середовища загроз. Це особливо важливо для забезпечення стійкості критичних сегментів, що найбільше вразливі до кібератак.

Виклад основного матеріалу. Промисловий інтернет речей (IIoT) є однією з найбільш інноваційних технологій сучасності, що дозволяє інтегрувати фізичні пристрої, системи моніторингу та керування у єдину мережу. Це відкриває нові горизонти для автоматизації, підвищення продуктивності та ефективності виробництва [1, с. 45]. Проте швидке впровадження IIoT супроводжується значним зростанням ризиків у сфері кібербезпеки [2, с. 67].

Одним із найважливіших аспектів цього виклику є безпека фізичної інфраструктури, яка включає окремі компоненти, що потребують детального аналізу та оцінки загроз. Зокрема, необхідно поелементно розглянути периферійні пристрої, такі як датчики, контролери й виконавчі механізми, які можуть бути вразливими до кібератак через недостатній захист [3, с. 78]; апаратне забезпечення, включаючи обчислювальні вузли, мережеві адаптери та мікросхеми, які часто піддаються атакам через апаратні дефекти або підміну компонентів [4, с. 89]; мережеві протоколи, що забезпечують зв'язок між пристроями, але через слабкі алгоритми шифрування можуть бути уразливими до перехоплення або модифікації даних [5, с. 56]; інтернет-з'єднання, що є основою взаємодії пристроїв IIoT, але можуть стати об'єктом атак через відкриті порти, відсутність фільтрації або некоректну конфігурацію захисту [6, с. 102].

Критично важливо враховувати алгоритми атак для розробки емерджентно-адаптивних систем захисту, які зможуть не лише реагувати на вже відомі загрози, але й прогнозувати можливі сценарії атак на основі аналізу даних [8, с. 134]. Використання глибоких нейронних мереж для аналізу поведінкових патернів у пристроях IIoT дозволить створювати моделі, здатні розпізнавати шкідливу активність у реальному часі [9, с. 112]. Особливо це стосується критичних сегментів, таких як енергетичні системи або транспортна інфраструктура, де наслідки атак можуть бути катастрофічними [10, с. 91]. Інтеграція емерджентних систем із принципами кіберімунітету забезпечить не лише захист поточних операцій, але й стійкість до майбутніх загроз [1, с. 67].

Схема у вигляді стовпчастої діаграми демонструє чотири основні категорії загроз, які впливають на фізичну інфраструктуру промислового інтернету речей (IIoT). Кожна категорія представлена окремим стовпцем, висота якого відповідає процентному внеску конкретної загрози до загальної сукупності. Для покращення візуального сприйняття використовується градієнтний колір (кольорова карта Viridis), що акцентує увагу на значеннях. Над кожним стовпцем вказані точні відсоткові значення.

Категорії загроз:

1. Незахищені периферійні пристрої (30%)

Ця категорія включає датчики, контролери та виконавчі механізми, які часто підключені до мереж без належного захисту.

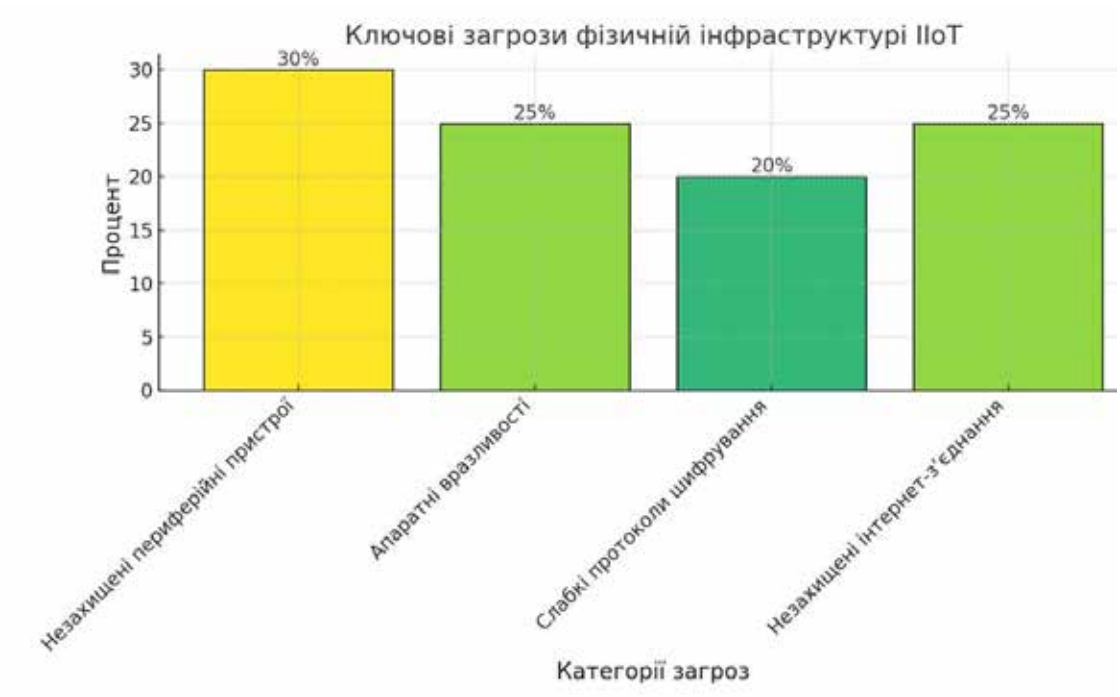

Рис. 1. Ключові загрози фізичній інфраструктурі IIoT

2. Апаратні вразливості (25%)

До цієї категорії належать дефекти апаратного забезпечення, підміна компонентів чи використання ненадійного обладнання.

3. Слабкі протоколи шифрування (20%)

Використання застарілих або слабких методів шифрування, які полегшують незаконний доступ до систем.

4. Незахищені інтернет-з'єднання (25%)

Відкриті порти або відсутність відповідного налаштування мережевої безпеки, які дозволяють зловмисникам отримувати доступ до інфраструктури.

Призначення:

Схема розроблена для наочного представлення основних загроз і їх значущості в контексті IIoT. Вона слугуватиме ефективним інструментом для аналізу ризиків та пріоритезації заходів кібербезпеки в промислових системах.

Промисловий інтернет речей (IIoT) значно підвищує ефективність виробництва, але водночас створює нові вразливості для кібератак. Реальні приклади таких атак демонструють потенційні ризики для фізичних елементів IIoT. Одним із найвідоміших інцидентів є атака вірусу **Stuxnet** у 2010 році, який був спрямований на іранські ядерні об'єкти. Stuxnet інфікував програмовані логічні контролери (PLC), що призвело до фізичного пошкодження центрифуг, використаних для збагачення урану. Цей випадок продемонстрував, як шкідливе програмне забезпечення може безпосередньо впливати на фізичні компоненти промислових систем [11, с. 45]. У 2015 році відбулася кібератака на енергетичну систему України, яка призвела до відключення електроенергії для приблизно 230 тисяч споживачів. Зловмисники використали шкідливе ПЗ **BlackEnergy** для компрометації інформаційно-керуючих систем, що дозволило їм дистанційно відключити підстанції. Цей інцидент підкреслив вразливість енергетичної інфраструктури до кібератак [12, с. 67].

У 2017 році вірус **WannaCry** вразив тисячі комп'ютерів по всьому світу, включаючи системи в промислових підприємствах. Хоча основною метою атаки було вимагання викупу, шкідливе ПЗ спричинило зупинку виробничих процесів, що призвело до значних фінансових втрат. Цей випадок показав, як атаки на інформаційні системи можуть мати непрямий вплив на фізичні елементи IIoT. У 2020 році було зафіксовано атаку на водоочисну станцію у Флориді, США. Зловмисники отримали доступ до системи управління та намагалися змінити рівень гідроксиду натрію у воді до небезпечного рівня. На щастя, оператор вчасно виявив аномалію та запобіг потенційно катастрофічним наслідкам. Цей інцидент підкреслює необхідність посилення безпеки в системах критичної інфраструктури.

Ці приклади свідчать про реальні загрози, пов'язані з кібератаками на фізичні елементи промислового інтернету речей, та підкреслюють важливість впровадження надійних заходів кібербезпеки для захисту критичних інфраструктур.

Промисловий інтернет речей (IIoT) є однією з найбільш інноваційних технологій сучасності, що дозволяє інтегрувати фізичні пристрої, системи моніторингу та керування у єдину мережу. Це відкриває нові горизонти для автоматизації, підвищення продуктивності та ефективності виробництва [1, с. 45]. Проте швидке впровадження IIoT супроводжується значним зростанням ризиків у сфері кібербезпеки [2, с. 67].

Однією з ключових проблем захисту промислового інтернету речей (IIoT) є безпека фізичної інфраструктури, яка включає різноманітні компоненти, що вимагають ретельного аналізу та оцінки ризиків. Зокрема, потребують уваги периферійні пристрої, такі як датчики, контролери й виконавчі механізми. Вони часто залишаються вразливими до кібератак через недостатній рівень захисту [3, с. 78]. Апаратне забезпечення, зокрема обчислювальні вузли, мережеві адаптери та мікросхеми, також перебуває під загрозою через можливі апаратні дефекти або підміну компонентів [4, с. 89]. Крім того, мережеві протоколи, що забезпечують зв'язок між пристроями, можуть бути скомпрометовані через використання слабких алгоритмів шифрування, що створює ризик перехоплення або модифікації даних [5, с. 56]. Не менш важливим є захист інтернет-з'єднань, які виступають основою взаємодії пристроїв IIoT. Відсутність фільтрації, некоректна конфігурація або відкриті порти значно підвищують ризик зловмисного доступу [6, с. 102]. Серед найбільших загроз для фізичної інфраструктури IIoT виділяються незахищені периферійні пристрої. Їх підключення до мереж без належного захисту створює можливості для викрадення даних або саботажу обладнання [7, с. 89]. Використання застарілого або ненадійного апаратного забезпечення також сприяє зростанню ризику атак, зокрема через апаратні дефекти або підміну компонентів [8, с. 91]. Додатково, слабкі або застарілі методи шифрування можуть стати інструментом незаконного доступу до даних або управління системами [9, с. 134]. Нарешті, відкриті порти, відсутність належного

мережевого захисту та неправильна конфігурація брандмауерів створюють загрозу проникнення в мережу IIoT [10, с. 78].

Ці аспекти вказують на критичну необхідність системного підходу до забезпечення кібербезпеки фізичної інфраструктури IIoT.

Для зменшення ризиків необхідно впроваджувати комплексні методи захисту. Важливим є забезпечення безпеки ланцюгів постачання шляхом використання апаратних і програмних компонентів тільки перевірених постачальників, що дозволить уникнути впровадження шкідливих елементів у критичну інфраструктуру [1, с. 134]. Стимулювання дослідження уразливостей, наприклад, через програми "Bug Bounty", сприятиме виявленню потенційних загроз [2, с. 112]. Розробка багаторівневих систем захисту на основі принципів кіберімунітету мінімізує ризик атак на кожному рівні архітектури OSI [3, с. 56]. Регулярне встановлення оновлень прошивок дозволяє усунути відомі вразливості [4, с. 67], а навчання персоналу основам кібербезпеки сприяє ідентифікації потенційних загроз і реагуванню на них [5, с. 89]. Проведення регулярних перевірок мереж і систем для виявлення слабких місць та їх усунення також є важливим елементом захисту [6, с. 102]. Додатково необхідно використовувати фізичні механізми захисту, такі як замки, сейфи або спеціальні корпуси, що обмежують несанкціонований доступ до обладнання [7, с. 45].

Критично важливо враховувати алгоритми атак для розробки емерджентно-адаптивних систем захисту, які зможуть не лише реагувати на вже відомі загрози, але й прогнозувати можливі сценарії атак на основі аналізу даних [8, с. 134]. Використання глибоких нейронних мереж для аналізу поведінкових патернів у пристроях IIoT дозволить створювати моделі, здатні розпізнавати шкідливу активність у реальному часі [9, с. 112]. Особливо це стосується критичних сегментів, таких як енергетичні системи або транспортна інфраструктура, де наслідки атак можуть бути катастрофічними [10, с. 91]. Інтеграція емерджентних систем із принципами кіберімунітету забезпечить не лише захист поточних операцій, але й стійкість до майбутніх загроз [1, с. 67]. Урахування алгоритмів атак є критично важливим для розробки емерджентно-адаптивних систем захисту. Ці системи повинні не лише реагувати на вже відомі загрози, але й прогнозувати можливі сценарії атак на основі аналізу даних. Використання глибоких нейронних мереж для аналізу поведінкових патернів у пристроях IIoT дозволить створювати моделі, здатні розпізнавати шкідливу активність у реальному часі [6, с. 102].

Особливо це стосується критичних сегментів, таких як енергетичні системи або транспортна інфраструктура, де наслідки атак можуть бути катастрофічними. Інтеграція емерджентних систем із принципами кіберімунітету забезпечить не лише захист поточних операцій, але й стійкість до майбутніх загроз [3, с. 134].

Враховуючи мультіелементність промислового інтернету речей, яка передбачає взаємодію великої кількості фізичних та віртуальних компонентів, необхідно впроваджувати нейромережі для управління системами на рівні архітектури OSI. Модель OSI є базовою структурою, яка охоплює всі аспекти роботи промислового інтернету речей: від фізичного рівня до рівня прикладних протоколів. Інтеграція адаптивних нейромереж у цю модель дозволить забезпечити комплек-

Таблиця 1

Методи захисту промислового IoT

Метод захисту	Опис	Очікуваний вплив
Безпека ланцюгів постачання	Використання перевірених постачальників апаратного і програмного забезпечення	Зменшення ризику впровадження шкідливих компонентів
Програми "Bug Bounty"	Стимулювання пошуку уразливостей через залучення експертів	Виявлення потенційних загроз і мінімізація вразливостей
Кіберімунітет	Розробка багаторівневого захисту пристроїв	Захист на кожному рівні архітектури OSI
Оновлення прошивок	Регулярне оновлення програмного забезпечення	Усунення вразливостей і підвищення безпеки
Навчання персоналу	Підвищення обізнаності працівників щодо кіберзагроз	Швидке реагування на потенційні загрози
Аудит безпеки	Перевірка мереж і систем для ідентифікації слабких місць	Зменшення ризику проникнення в мережу
Фізичний захист	Захист обладнання від несанкціонованого фізичного доступу	Захист обладнання від фізичного втручання

сний захист на всіх рівнях, що значно зменшить ризики, пов'язані з кібератаками.

Цей підхід відкриває новий напрямок наукових досліджень, спрямованих на створення автономних систем кіберзахисту, які будуть враховувати особливості роботи IIoT. Використання нейромереж на рівні OSI дозволить автоматично адаптуватися до нових загроз, підвищуючи стійкість систем до атак, що впливають на різні рівні їх функціонування. Таким чином, це стане ключовою передумовою для забезпечення безпеки у складних, динамічних середовищах промислового інтернету речей.

Обговорення

IIoT виступає фундаментом цифрової трансформації в сучасній індустрії, забезпечуючи інтеграцію фізичних пристроїв із мережевими технологіями для автоматизації, моніторингу та підвищення ефективності виробничих процесів. Проте швидкий розвиток IIoT супроводжується зростанням ризиків, пов'язаних із вразливістю фізичної інфраструктури до кібератак. У цьому контексті необхідно не лише ідентифікувати основні загрози, але й розробити ефективні методи їх попередження та захисту. Дослідження підтверджують, що основними загрозами для фізичної інфраструктури IIoT є незахищені периферійні пристрої, апаратні вразливості, слабкі протоколи шифрування та незахищені інтернет-з'єднання. Наприклад, кібератаки, такі як Stuxnet, WannaCry та атака на енергетичну систему України, демонструють серйозний потенціал шкідливого впливу на фізичні елементи IIoT. Ці випадки вказують на необхідність комплексного підходу до захисту, який враховує особливості багаторівневих взаємодій у межах промислових систем.

Розробка методів захисту повинна базуватися на впровадженні кіберімунітету, регулярному оновленні прошивок, аудиторських перевірках, а також освіті персоналу. Особливої уваги заслуговує інтеграція нейромереж, які здатні не лише аналізувати поведінкові патерни пристроїв у реальному часі, але й адаптуватися до нових загроз. Це дозволяє створювати системи, які автоматично прогнозують сценарії атак і забезпечують захист на рівнях архітектури OSI.

Важливим напрямом є дослідження мультиелементної природи IIoT, яка передбачає взаємодію різноманітних компонентів на всіх рівнях архітектури. Інтеграція емерджентно-адаптивних систем на рівнях OSI дозволяє розширити можливості управління безпекою та мінімізувати ризики. Такий підхід стає основою для розробки автономних систем кіберзахисту, здатних ефективно реагувати на атаки в умовах складних і динамічних середовищ.

Окремим викликом залишається захист критичних сегментів інфраструктури, таких як енергетичні системи, транспорт та медичні установи, які є потенційними цілями для кібератак. Використання багаторівневого підходу до кібербезпеки, що охоплює фізичний захист пристроїв, безпеку ланцюгів постачання та нейромережевий аналіз даних, забезпечує стійкість промислових систем до загроз та їх безпечне функціонування.

Загалом, інтеграція сучасних технологій, таких як нейромережі, в архітектуру IIoT відкриває нові можливості для створення високоефективних систем захисту. Цей напрямок вимагає подальших міждисциплінарних досліджень, спрямованих на розробку автономних, адаптивних рішень, які можуть стати стандартом у сфері кібербезпеки промислового інтернету речей.

Висновки. Промисловий інтернет речей (IIoT) став ключовим елементом цифрової трансформації сучасної індустрії, забезпечуючи інтеграцію фізичних та віртуальних компонентів для підвищення ефективності виробництва, автоматизації процесів та покращення управління ресурсами. Проте зростання мережевої взаємодії та технологічної складності IIoT супроводжується значними викликами у сфері кібербезпеки, що ставить під загрозу фізичні елементи інфраструктури. Це, своєю чергою, може спричиняти значні соціально-економічні та екологічні наслідки.

Відповідно до проведеного аналізу, основними загрозами для фізичної інфраструктури IIoT є незахищені периферійні пристрої, апаратні вразливості, слабкі протоколи шифрування та незахищені інтернет-з'єднання. Реальні кейси, такі як атака Stuxnet, зловживання BlackEnergy у 2015 році, поширення WannaCry у 2017 році та втручання у водоочисну станцію Флориди у 2020 році, підтверджують актуальність проблеми. Ці інциденти демонструють, що критичні елементи інфраструктури можуть бути об'єктом кіберзагроз із катастрофічними наслідками.

Розробка ефективних методів захисту має базуватися на впровадженні емерджентно-адаптивних систем, інтеграції принципів кіберімунітету та використанні глибоких нейромереж для аналізу даних у реальному часі. Модель OSI, яка охоплює всі рівні архітектури IIoT, є базовою основою для створення комплексних систем кіберзахисту. Їхня інтеграція з нейромережами дозволяє автоматизувати процеси виявлення та реагування на загрози,

що мінімізує ризики для фізичних елементів інфраструктури.

Окремої уваги заслуговує захист критичних сегментів, таких як енергетичні, транспортні системи та системи життєзабезпечення, які є важливими складовими національної безпеки. Використання адаптивних систем забезпечує не лише захист поточних операцій, але й стійкість до майбутніх викликів, що стає критично важливим у динамічному середовищі, де зловмисники постійно адаптують свої стратегії.

З огляду на це, посилення інформаційної безпеки держави як складної динамічної системи є стратегічним завданням. Промисловий інтернет речей, як один із ключових сегментів цієї системи, відіграє важливу роль у забезпеченні національної безпеки. Його захист має бути інтегрований у загальнодержавну стратегію кібербезпеки, що включає впровадження передових технологій, таких як блокчейн, кіберімунітет, та системи прогнозування загроз на основі аналізу великих даних.

Цей підхід сприятиме створенню стійкої до загроз екосистеми, яка забезпечить безперервність функціонування критичних інфраструктур, а також зміцнить позиції держави на глобальній арені у сфері інформаційної безпеки. Таким чином, розвиток комплексних стратегій захисту IIoT має стати важливим напрямком наукових і практичних досліджень для забезпечення надійності та безпеки в умовах нових викликів кіберпростору.

Список літератури:

1. IoT Cybersecurity Handbook: Захист Інтернету речей від загроз / Джейсон Харпер. – Elsevier, 2022. – 300 с. DOI: 10.1016/B978-0-12-823834-3.00012-6. Доступно у видавця: elsevier.com (дата звернення: 19.12.2024).

2. Кіберзлочини та інформаційні технології: Інфраструктура комп'ютерних мереж і комп'ютерна безпека, закони з кібербезпеки, Інтернет речей (IoT) і мобільні пристрої / Алекс Александру. – CRC Press, 2021. Доступно у видавця: crcpress.com (дата звернення: 19.12.2024).

3. AWS IoT із Edge ML та кібербезпекою: Практичний підхід / Сайед Рехан. – Apress, 2023. Доступно у видавця: apress.com (дата звернення: 19.12.2024).

4. Штучний інтелект для блокчейну та IoT-застосунків із підтримкою кібербезпеки / Марія Оуайсса, Закарія Булуард, Абхішек Кумар, Вандана Шарма, Кешав Каушик. – Routledge, 2024. Доступно у видавця: routledge.com (дата звернення: 19.12.2024).

5. IoT Security: Practical Threats and Solutions / Роберт Уотсон. Springer, 2023. – 385 с. DOI: 10.1007/978-3-031-10567-8. Доступно у видавця: springer.com (дата звернення: 19.12.2024).

6. Кібербезпека: Технології середовища, Інтернет речей (IoT) і вплив на Індустрію 4.0 / за ред. Гаутама Кумара, Ом Пракаша Сінгха, Хемраджа Сайні. – CRC Press, 2021. Доступно у видавця: crcpress.com (дата звернення: 19.12.2024).

7. Протидія шкідливому програмному забезпеченню для IoT / Адам Браун, Стефані Сміт. – Cambridge University Press, 2021. Доступно у видавця: cambridge.org (дата звернення: 19.12.2024).

8. Кіберрозуми: Інсайти з кібербезпеки у хмарних обчисленнях, штучному інтелекті, блокчейні та IoT для забезпечення кібербезпеки / Шира Рубінофф. Packt Publishing, 2020. Доступно у видавця: packtpub.com (дата звернення: 19.12.2024).

9. ISO/IEC 27400:2022: Кібербезпека – Керівництво із захисту та конфіденційності IoT. Міжнародна організація зі стандартизації, 2022.

DOI: 10.3403/30330146. Доступно на сайті: iso.org (дата звернення: 19.12.2024).

10. Кібербезпека IoT: Ризики, виклики та практичні рішення / Адріан МакГілл. Wiley, 2022. – 412 с. DOI: 10.1002/9781119876543. Доступно у видавця: wiley.com (дата звернення: 19.12.2024).

11. Ланґнер, P. Stuxnet: Dissecting a Cyberwarfare Weapon. / IEEE Security & Privacy. – 2011. DOI: 10.1109/MS.2011.91.

12. Кейз, Д. Analysis of the Cyber Attack on the Ukrainian Power Grid. /Electricity Information Sharing and Analysis Center (E-ISAC). – 2016. DOI: 10.1109/MS.2016.25.

Prokopovych-Tkachenko D.I., Zveriev V.P., Kozachenko I.M. CYBER THREATS AND PROTECTION METHODS FOR THE PHYSICAL INFRASTRUCTURE OF THE INDUSTRIAL INTERNET OF THINGS (IIOT)

The article provides an in-depth analysis of security threats in the IoT, covering the entire spectrum of potential vulnerabilities–from the physical level of interaction with peripheral devices to the application layer, where complex attack scenarios can arise due to the lack of adequate authentication and encryption mechanisms. The authors emphasize that threats associated with malicious software are capable not only of

stealing data or disrupting network operations but also of causing dangerous malfunctions in the physical components of industrial systems, as evidenced by the Stuxnet example.

Particular attention in the article is devoted to each layer of the OSI model, analyzing how physical devices, communication channels, network and transport protocols, as well as session and application services, can be compromised. Key risks are identified, including unauthorized access to equipment at the physical layer, packet interception or modification at the network layer, and the exploitation of protocol or service vulnerabilities at higher layers. The authors stress that, without appropriate preventive measures, weaknesses at each of these levels could be exploited by attackers to conduct complex, multi-step attacks.

The study underscores the importance of a comprehensive protection strategy encompassing both technical and organizational components. Among such measures are the implementation of cyber immunity technologies capable of providing simultaneous protection at multiple levels, the deployment of effective intrusion detection systems, adherence to supply chain security principles–since vulnerabilities often enter the system during the development or delivery stages–and regular software updates coupled with active employee training to raise awareness of potential risks.

By adopting such integrated approaches to security, industrial systems can significantly mitigate the risks associated with cyberattacks and ensure the resilience of operational processes. The recommendations and methods for preventing attacks presented in the article can be valuable to a wide range of enterprises aiming to protect both their data and the physical components of production systems, thereby ensuring the continuity and reliability of critical infrastructure operations.

Key words: *IIoT, malware, cyberattacks, cybersecurity, physical infrastructure, cyber-immunity.*