УДК 004.056:004.738.5 DOI 10.33111/mise.105.9

Лазарєва С.Ф.,
к.е.н., професор кафедри системного аналізу та кібербезпеки,
КНЕУ імені Вадима Гетьмана
Герасимчук Я.І.,
здобувач освітнього ступеня «Магістр», КНЕУ імені Вадима Гетьмана

Lazarieva Svitlana,
Candidate of Economic Science, Professor of the Department of System Analysis and Cybersecurity, Vadym Hetman Kyiv National University of Economics
Herasymchuk Yaroslav,
Master's degree candidate, Vadym Hetman Kyiv National University of Economics,

АНАЛІЗ КІБЕРЗАГРОЗ ТА МЕТОДИКА ЗАПОБІГАННЯ ВРАЗЛИВОСТІ IOT-СИСТЕМИ КОНТРОЛЮ МІКРОКЛІМАТУ В СКЛАДСЬКИХ ПРИМІЩЕННЯХ

ANALYSIS OF CYBER THREATS AND VULNERABILITY PREVENTION METHODOLOGY FOR AN IOT MICROCLIMATE CONTROL SYSTEM IN WAREHOUSE FACILITIES

Анотація. *Широке впровадження технологій Інтернету речей (IoT) у промислову та складську інфраструктуру значно підвищило операційну ефективність, одночасно створюючи нові виклики кібербезпеці. Системи контролю мікроклімату, розгорнуті на складських об'єктах, представляють собою критичний клас кіберфізичних систем, оскільки вони безпосередньо впливають на якість, безпеку та економічну цінність товарів, що зберігаються. У цій статті наведено комплексний аналіз кіберзагроз, спрямованих на системи моніторингу та контролю мікроклімату на основі IoT, з урахуванням архітектурних, мережевих, протокольних та пристроєвих вразливостей. На основі виявленого ландшафту загроз запропоновано логічно структуровану методологію запобігання вразливостям, що інтегрує організаційні, мережеві, криптографічні та поведінкові механізми безпеки. Методологія підкреслює баланс між ефективністю безпеки та ресурсними обмеженнями, властивими пристроям IoT. Запропонований підхід підвищує стійкість системи, зменшує ризик несанкціонованого втручання та підтримує безперервність складських бізнес-процесів.*
Ключові слова: *безпека IoT; кіберзагрози; запобігання вразливостям; контроль мікроклімату; складські інформаційні системи.*

Abstract. *The widespread adoption of Internet of Things (IoT) technologies in industrial and warehouse infrastructures has significantly increased operational efficiency while simultaneously introducing new cybersecurity challenges. Microclimate control systems deployed in warehouse facilities represent a critical class of cyber-physical systems, as they directly influence the quality, safety, and*

economic value of stored goods. This paper provides a comprehensive analysis of cyber threats targeting IoT-based microclimate monitoring and control systems, considering architectural, network, protocol, and device-level vulnerabilities. Based on the identified threat landscape, a logically structured vulnerability prevention methodology is proposed, integrating organizational, network, cryptographic, and behavioral security mechanisms. The methodology emphasizes a balance between security effectiveness and the resource constraints inherent to IoT devices. The proposed approach enhances system resilience, reduces the risk of unauthorized interference, and supports the continuity of warehouse business processes.
Keywords: *IoT security; cyber threats; vulnerability prevention; microclimate control; warehouse information systems.*

Постановка проблеми у загальному вигляді. Інтернет речей став ключовим технологічним компонентом сучасних інформаційно-управляючих систем, зокрема у сфері логістики та складської інфраструктури, що відображено у сучасних вітчизняних дослідженнях цифрової трансформації промисловості та логістики. Впровадження IoT-сенсорів і контролерів для безперервного моніторингу ключових параметрів мікроклімату, зокрема температури, відносної вологості повітря та концентрації газоподібних речовин, забезпечує автоматизацію технологічних процесів зберігання сільськогосподарської продукції, зменшення впливу людського фактора та підвищення якості управлінських рішень, що підтверджується прикладними дослідженнями у сфері «розумних» складів [1, 2].

Водночас інтенсифікація використання мережевих IoT-пристроїв, які функціонують у відкритих або напіввідкритих середовищах, зумовлює розширення поверхні атаки та зростання кібербезпекових ризиків, що є типовою характеристикою IoT-орієнтованих архітектур і відзначається у вітчизняних аналітичних оглядах з кібербезпеки [3].

На відміну від класичних корпоративних інформаційних систем, IoT-системи контролю мікроклімату відносяться до класу кіберфізичних для яких є характерною тісна інтеграція фізичних технологічних процесів із цифровими механізмами управління та моніторингу. Реалізація кібератак у таких системах може спричинити не лише порушення конфіденційності, цілісності та доступності інформаційних ресурсів, а й призвести до критичних матеріальних наслідків, що підтверджується дослідженнями у сфері безпеки промислових і складських IoT-рішень. До таких наслідків належать порушення оптимальних температурно-вологісних режимів зберігання, деградація якості продукції або її повна втрата, зупинка логістичних операцій, а також фінансові збитки внаслідок невиконання контрактних зобов’язань [5].

Зазначена специфіка актуалізує необхідність проведення комплексного аналізу кіберзагроз і розроблення спеціалізованих методик превентивного захисту, адаптованих до архітектурних і функціональних особливостей IoT-систем мікрокліматичного контролю складських приміщень, з урахуванням обмежених обчислювальних та енергетичних ресурсів кінцевих пристроїв, що підкреслюється у сучасних наукових публікаціях останніх років [6].

Аналіз останніх досліджень і публікацій. У сучасному науковому дискурсі проблеми кібербезпеки Інтернету речей досліджуються переважно через призму загальних архітектурних вразливостей, аналізу ризиків комунікаційних протоколів та розробки криптографічних механізмів для пристроїв з обмеженими обчислювальними ресурсами.

Домінуючий підхід базується на стратифікованій класифікації загроз за триланковою архітектурою IoT, яка включає рівень сенсорів та актуаторів, мережевий рівень і рівень прикладних сервісів. Водночас аналіз наукових праць [1, 2, 3] свідчить про недостатню представленість практично орієнтованих робіт, спрямованих на адаптацію теоретичних моделей до реальних умов функціонування промислових і складських IoT-рішень.

Окремий напрям досліджень [4] присвячено аналізу вразливостей протоколів передачі даних, зокрема MQTT (Message Queuing Telemetry Transport) та CoAP (Constrained Application Protocol), які набули широкого застосування в промислових IoT-екосистемах завдяки низьким накладним витратам та підтримці обмежених пристроїв.

У науковій публікації [5] основний акцент робиться на критичних ризиках інформаційної безпеки, пов’язаних із відсутністю вбудованого шифрування на рівні протоколу, недостатньою криптографічною стійкістю механізмів автентифікації клієнтів та можливістю реалізації атак типу broker spoofing.

Разом із тим, деякі дослідники [6] розглядають протокольні загрози ізольовано, без інтеграції з бізнес-контекстом функціонування систем та без оцінювання потенційних фізичних і економічних наслідків успішної компрометації IoT-інфраструктури.

У роботах, присвячених виявленню аномалій [7], пропонуються статистичні та машино-навчальні підходи до аналізу мережевого трафіку IoT-пристроїв, зокрема методи кластеризації, моделі на основі часових рядів та алгоритми навчання без учителя.

Запропоновані підходи демонструють високу ефективність у виявленні нетипової поведінки пристроїв, але потребують адаптації до специфіки конкретних прикладних систем. Зокрема у

системах мікрокліматичного контролю нормальні режими роботи можуть динамічно змінюватися залежно від технологічних процесів зберігання, що ускладнює формування моделей нормальної поведінки [8].

Невирішені частини загальної проблеми. Незважаючи на значну кількість наукових праць, присвячених питанням кібербезпеки Інтернету речей, залишається низка недостатньо розглянутих аспектів, що суттєво обмежує можливості практичного застосування існуючих підходів у промислових та складських IoT-системах.

По-перше, більшість досліджень зосереджуються на узагальненому аналізі загроз IoT-середовищ без урахування галузевої специфіки прикладних систем. У роботах [1, 3] недостатньо враховується контекст експлуатації систем мікрокліматичного контролю складських приміщень, для яких компрометація даних або управлінських команд може мати безпосередні фізичні та економічні наслідки, пов'язані з порушенням умов зберігання продукції.

По-друге, у наукових публікаціях [5] простежується тенденція до ізольованого розгляду загроз окремих рівнів IoT-архітектури. Сенсорні вузли, мережеві протоколи та серверні компоненти зазвичай аналізуються незалежно один від одного, що не дозволяє врахувати міжрівневі та каскадні ефекти атак . У результаті відсутні комплексні моделі загроз, здатні описувати поширення наслідків компрометації одного елемента на функціонування всієї системи.

По-третє, суттєвою проблемою залишається обмеженість ресурсів IoT-пристроїв, яка ускладнює впровадження традиційних механізмів інформаційної безпеки. Запропоновані у літературі [5, 6] криптографічні та аналітичні рішення часто не враховують компроміс між рівнем захищеності, обчислювальними можливостями та енергоспоживанням сенсорних вузлів, що обмежує їх практичну доцільність у довготривалій експлуатації.

Окремої уваги потребує проблема адаптації методів виявлення аномалій до умов функціонування систем мікрокліматичного контролю. Динамічна зміна режимів роботи, зумовлена технологічними процесами зберігання, ускладнює формування універсальних моделей нормальної поведінки IoT-пристроїв і знижує ефективність існуючих підходів без додаткової прикладної адаптації [7, 8].

Отже, актуальним залишається завдання розроблення комплексної методики аналізу кіберзагроз та превентивного захисту IoT-систем контролю мікроклімату, яка поєднувала б міжрівневий підхід до безпеки, враховувала ресурсні обмеження пристроїв і була

адаптована до реальних умов експлуатації складської інфраструктури. Саме розв'язанню цього завдання присвячена ця стаття.

Основною метою статті є аналіз кіберзагроз, притаманних IoT-системам контролю мікроклімату складських приміщень, з урахуванням їх кіберфізичної природи та міжрівневої взаємодії компонентів, а також обґрунтування методики запобігання вразливостям, що поєднує технічні, організаційні й аналітичні заходи захисту.

Виклад основного матеріалу дослідження. Ефективне забезпечення кібербезпеки IoT-систем контролю мікроклімату неможливе без чіткого усвідомлення спектру кіберзагроз, до яких є вразливими такі системи. Оскільки IoT-рішення поєднують сенсорні пристрої, мережеву інфраструктуру та програмно-апаратні засоби управління, кібератаки можуть мати як інформаційні, так і безпосередні фізичні наслідки. Це зумовлює необхідність систематизованого підходу до аналізу загроз, що дозволяє визначити пріоритетні напрямки захисту та обґрунтувати вибір відповідних заходів безпеки.

Загрози IoT-системи контролю мікроклімату доцільно класифікувати за архітектурним рівнем їх реалізації та характером впливу на функціонування системи. Відповідно можна виділити такі основні групи кіберзагроз:

- загрози мережевого рівня, спрямовані на порушення доступності та конфіденційності передаваних даних;
- загрози прикладного рівня, пов'язані з несанкціонованою модифікацією команд управління;
- загрози рівня кінцевих пристроїв, зумовлені вразливостями апаратного та програмного забезпечення IoT-вузлів.

Запропонована класифікація дозволяє розглядати кіберзагрози комплексно, з урахуванням взаємозв'язку між окремими компонентами системи.

Загрози мережевого рівня. На мережевому рівні найпоширенішими є атаки, спрямовані на порушення доступності та конфіденційності даних [1, 6]. Перехоплення незашифрованого трафіку дозволяє зловмиснику отримати інформацію про поточні параметри мікроклімату або ідентифікатори IoT-пристроїв, що у подальшому може бути використано для реалізації складніших атак.

Окрему небезпеку становлять атаки типу відмови в обслуговуванні, зокрема flooding-атаки, які здатні перевантажити канали зв'язку або брокери повідомлень, що призводить до затримки або втрати критичних телеметричних даних [7, 8].

Загрози прикладного рівня. На прикладному рівні суттєву небезпеку становлять атаки, пов'язані з підміною або несанкціонованою модифікацією команд управління. У разі компрометації облікових даних користувачів або експлуатації вразливостей протоколів обміну повідомленнями зловмисник може змінювати режими роботи системи, наприклад примусово вимикати вентиляцію або коригувати температурні пороги [2, 4, 7]. Такі дії мають безпосередній вплив на фізичний стан складського середовища та можуть призводити до порушення умов зберігання продукції [3].

Загрози рівня кінцевих пристроїв. На рівні кінцевих пристроїв ключовими загрозами є використання стандартних або слабких облікових даних, відсутність захищених механізмів оновлення прошивки та можливість фізичного доступу до обладнання [5, 6]. Компрометація навіть одного IoT-вузла може стати відправною точкою для подальшого розповсюдження атаки у межах всієї системи, зокрема через використання довірених з'єднань між компонентами або повторне використання автентифікаційних даних [7, 8].

Методика запобігання вразливості IoT-системи. Запропонована методика запобігання вразливостям у IoT-системі базується на загальновизнаному принципі багаторівневого захисту (Defense-in-Depth), що передбачає послідовну реалізацію заходів безпеки на всіх рівнях системи — від організаційних політик до активних технічних механізмів виявлення та реагування на загрози. Такий підхід вважається ефективним у розподілених IoT-середовищах, оскільки дозволяє комбінувати різні засоби захисту на рівнях мережі, пристроїв та сервісів з урахуванням їхніх функціональних характеристик і обмежень ресурсів [1, 2, 4, 6]

Логіку запропонованої методики проілюструємо у вигляді ієрархічної моделі пріоритетів захисту IoT-системи, яка відображає послідовність упровадження заходів безпеки — від базових організаційних механізмів до активних процедур виявлення та реагування на інциденти (див. рис. 1).

Рис. 1. Піраміда пріоритетів кібербезпеки IoT-системи

Джерело: розроблено автором на основі [2]

Представлена на рис. 1 модель відображає ієрархічну структуру заходів захисту IoT-системи та підкреслює необхідність комплексного підходу до забезпечення її кібербезпеки.

Модель демонструє, що ефективний захист можливий лише за умови послідовної реалізації організаційних, мережевих, прикладних і операційних механізмів безпеки, кожен з яких відіграє визначальну роль у загальній системі захисту.

Подальший виклад присвячено детальному аналізу функціонального призначення кожного рівня.

Перший етап передбачає формування політики безпеки IoT-системи, яка визначає правила доступу, вимоги до автентифікації, порядок управління обліковими записами та відповідальність за адміністрування. У науковій літературі [1, 2, 5] підкреслюється важливість чітко задокументованих політик і процедур, які забезпечують базовий рівень контролю доступу та зменшують ризик

несанкціонованого втручання як зовні, так і з боку внутрішніх користувачів.

На мережевому рівні доцільно застосовувати логічну сегментацію IoT-пристроїв у відокремлені сегменти або зони з обмеженим доступом до інших частин корпоративної мережі. Дослідження, що розглядають безпеку MQTT-зв'язків та загальні архітектури IoT-систем [3, 6, 8], акцентують увагу на важливості використання ізольованих мереж (VLAN/VPN) й обмежувальних політик доступу для зменшення потенційної шкоди у разі компрометації одного з вузлів.

Передача даних між сенсорами, контролерами та сервером має бути захищена криптографічними механізмами, що гарантують конфіденційність і цілісність інформації. У публікаціях з багаторівневих моделей захисту IoT-систем [4, 6, 7] підкреслюється доцільність застосування сучасних протоколів шифрування (наприклад, TLS/SSL) та аутентифікації на рівні прикладного трафіку як критичний елемент захисту від атак типу MITM і підміни команд.

Важливою частиною запропонованої методики є компонент моніторингу і аналізу поведінки IoT-пристроїв. У наукових дослідженнях, присвячених методам забезпечення безпеки IoT [6, 7], зазначається, що використання статистичних моделей нормальної роботи та алгоритмів виявлення аномалій дозволяє ідентифікувати порушення, що виходять за межі очікуваної поведінки пристроїв.

Як зазначено в роботі [4], такий підхід особливо ефективний у стабільних середовищах, де режим роботи сенсорів та контролерів має передбачувану динаміку, а аномалії часто відповідають реальним загрозам або технічним збоям.

Останній етап методики — організація процесу реагування на інциденти — включає автоматичне сповіщення адміністратора, локалізацію та ізоляцію підозрілих вузлів, відновлення цілісного функціонування системи і документування подій для подальшого аналізу. Комплексні підходи до безпеки IoT, що розглядають як технічні, так і організаційні компоненти, підкреслюють важливість таких механізмів для забезпечення безперервності бізнес-процесів та зниження потенційних наслідків успішних атак.

Для узагальнення запропонованого в методиці підходу та наочного представлення відповідності між рівнями IoT-системи, типовими кіберзагрозами та заходами запобігання вразливостям доцільно використати порівняльну таблицю (див. табл. 1).

Таблиця 1

ВІДПОВІДНІСТЬ РІВНІВ ІОТ-СИСТЕМИ, ТИПОВИХ ЗАГРОЗ ТА ЗАХОДІВ ЗАПОБІГАННЯ

Рівень IoT-системи	Типові кіберзагрози	Заходи запобігання вразливостям	Наукове обгрунтування
Організаційний	Несанкціонований доступ, помилки адміністрування, внутрішні загрози	Формування політики безпеки, розмежування ролей і прав доступу, регламентація відповідальності	Політики безпеки визначають базовий рівень захисту IoT-систем і знижують ризики внутрішніх інцидентів
Сенсорний (perception layer)	Підміна показників сенсорів, фізичний доступ, spoofing	Контроль цілісності даних, базова автентифікація вузлів, моніторинг аномалій вимірювань	Дослідження вказують на ефективність поведінкового аналізу для виявлення компрометації сенсорів
Мережевий	Перехоплення трафіку, MITM-атаки, DoS	Сегментація мережі, ізоляція IoT-вузлів, шифрування переданих даних	Мережева ізоляція та криптографічний захист є ключовими елементами Defense-in-Depth
Прикладний	Несанкціоноване керування виконавчими механізмами, модифікація команд	Автентифікація сервісів, контроль доступу, журналювання подій	Контроль доступу на прикладному рівні знижує ризик керування системою сторонніми особами
Операційний	Запізніле виявлення атак, тривалий простій системи	Моніторинг, сповіщення, ізоляція вузлів, процедури реагування на інциденти	Реагування на інциденти є критичним для забезпечення безперервності бізнес-процесів

Джерело: адаптовано на основі [1–5]

Запропонована методика поєднує стандартизовані моделі захисту, сегментацію мережі, криптографічні засоби, поведінковий моніторинг і операційні процеси реагування, створюючи структурований і адаптований до умов складських IoT-систем підхід до зниження ризиків кібератак.

Висновки та перспективи подальших досліджень. У статті проаналізовано кіберзагрози, що характерні для IoT-систем контролю мікроклімату в складських приміщеннях, та обґрунтовано необхідність комплексного підходу до забезпечення їхньої безпеки. Запропонована методика запобігання вразливостям враховує специфіку IoT-архітектури, обмежені ресурси пристроїв та критичну роль мікрокліматичних параметрів у складській логістиці.

Перспективним напрямом подальших досліджень є інтеграція методів машинного навчання для підвищення точності виявлення складних багатоетапних атак, а також адаптація запропонованої методики до хмарних і гібридних архітектур управління IoT-системами.

Бібліографічні посилання

1. Дудикевич В. Б., Мельник В. М. Кібербезпека: теорія та практика. – Львів: Вид-во Львівської політехніки, 2020. – 212 с.
2. Гнатюк С. О. Методи та засоби забезпечення кібербезпеки. – К. : Центр учбової літератури, 2021. – 286 с.
3. Бурячок В. Л., Толубко В. Б., Хорошко В. О. Кібербезпека об’єктів критичної інфраструктури. – К.: Національний університет оборони України імені Івана Черняховського, 2021. – 312 с.
4. Гнатюк С. О., Юдін О. К., Бурячок В. Л. Кібербезпека кіберфізичних та IoT-систем. – К. : Центр учбової літератури, 2024. – 328 с.
5. Ковальчук В. В. Захист інформації в сучасних інформаційно-комунікаційних системах. – К. : Центр учбової літератури, 2023. – 240 с.
6. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. Security, privacy and trust in Internet of Things: Recent advances and future challenges // *Computer Networks*. – 2020.
7. Humayed A., Lin J., Li F., Luo B. Cyber-Physical Systems Security — A Survey // *IEEE Internet of Things Journal*. – 2021.
8. Boyes H., Watson T. Cybersecurity for Industrial Control Systems and IoT // *Computers in Industry*. – 2021.