УДК: 681.5 DOI 10.33111/mise.103.1

Агутін М.М.,
к.е.н., доцент кафедри системного аналізу та кібербезпеки
КНЕУ імені Вадима Гетьмана
Сусло Т.Ю. ,
студентка за освітньо-професійною програмою «Системний аналіз» ННІ «Інститут інформаційних технології в економіці»
КНЕУ імені Вадима Гетьмана

Agutin M.M.,
PhD in Economics, Associate Professor of System Analysis and Cybersecurity Department
KNEU named after Vadym Hetman
Suslo T.Y.,
student of educational professional program «System Analysis» of SEI «Institute of Information Technologies in Economics»
KNEU named after Vadym Hetman

МОДЕЛЮВАННЯ БЕЗПЕКИ ТА НАДІЙНОСТІ IOT-СИСТЕМ

MODELING THE SAFETY AND RELIABILITY OF IOT SYSTEMS

Анотація. *Системи Інтернет-речей (IoT) стрімко розвиваються, що призводить до нових можливостей, але й до нових ризиків. У статті досліджується проблеми надійності та безпеки IoT-систем. Розглядаються різні методи аналізу надійності та кібербезпеки IoT, а також їхні переваги та недоліки. Ненадійні та небезпечні IoT-системи можуть призвести до серйозних наслідків, таких як фінансові збитки, пошкодження репутації та фізична шкода. Дослідження показало, що аналіз надійності та кібербезпеки IoT-систем є важливим процесом, який допомагає виявити потенційні ризики та проблеми. Існує багато різних методів аналізу, але важливо вибрати ті, які відповідають вашим потребам та ресурсам. Аналіз надійності та кібербезпеки IoT-систем є ітеративним процесом, який потребує постійного моніторингу та оновлення. Важливо враховувати як надійність, так і кібербезпеку на всіх етапах розробки та експлуатації IoT-систем. Існує багато інструментів та ресурсів, які можуть допомогти вам провести аналіз надійності та кібербезпеки IoT-систем. В статті запропоновано один із підходів до оцінки надійності IoT-систем та окреслені необхідні рішення щодо реалізації запропонованого підходу в практичній діяльності.*
Ключові слова: *Інтернет речей, IoT-система, надійність, безпека, аналіз ризиків, кіберзахист.*

Abstract. *Internet of Things (IoT) systems are developing rapidly, which leads to new opportunities, but also to new risks. The article examines the problems of reliability and security of IoT systems. Different methods for IoT reliability and cybersecurity analysis are reviewed, along with their advantages and disadvantages. Untrusted and unsafe IoT systems can lead to serious consequences*

such as financial loss, reputational damage and physical harm. The study found that analyzing the reliability and cybersecurity of IoT systems is an important process that helps identify potential risks and problems. There are many different analysis methods, but it is important to choose the ones that suit your needs and resources. Analyzing the reliability and cyber security of IoT systems is an iterative process that requires constant monitoring and updating. It is important to consider both reliability and cybersecurity at all stages of development and operation of IoT systems. There are many tools and resources that can help you perform reliability and cybersecurity analysis of IoT systems. The article proposes one of the approaches to assessing the reliability of IoT systems and outlines the necessary solutions for the implementation of the proposed approach in practical activities.
Keywords: *Internet of Things, IoT system, reliability, security, risk analysis, cyber protection.*

Постановка проблеми у загальному вигляді. Стрімкий розвиток Інтернету речей (IoT) створює нові можливості для бізнесу та суспільства. Однак, разом з цими можливостями, зростають і ризики, пов'язані з надійністю та безпекою систем IoT. Актуальність розгляду питань безпеки та надійності систем IoT обумовлена тим, що експлуатація ненадійних та небезпечних системи IoT можуть призвести до серйозних наслідків, таких як: фінансові збитки, зупинки роботи, втрати даних та інші фінансові втрати; пошкодження репутації, втрата даних клієнтів; фізична загроза небезпечних систем IoT, які можуть становити загрозу для життя та здоров'я людей.

Отже завданням цієї роботи є розробка методики оцінювання надійності та безпеки систем IoT, яка дозволить: оцінити ймовірність збоїв та відмов системи IoT; ідентифікувати потенційні кіберзагрози; визначити ризики, пов'язані з використанням системи IoT; запропонувати рекомендації щодо підвищення надійності та безпеки системи IoT.

Оцінювання надійності та безпеки систем IoT є важливим завданням, яке має вирішуватися на ранніх стадіях розробки та впровадження цих систем. Розробка методики оцінювання надійності та безпеки систем IoT дозволить підвищити рівень надійності та безпеки цих систем, зменшити ризики, пов'язані з їх використанням, та підвищити довіру до них з боку користувачів та бізнесу.

Аналіз останніх досліджень і публікацій. Проблемам розробки, використання, архітектури та надійності систем Інтернет-речей присвячено роботи як вітчизняних [4, 5] так відомих в світі науковців [1, 2, 3], дослідників систем IoT. Системні підходи до розгляду та моделювання систем Інтернет-речей докладно розглядається в роботі Мамонової Г.В., Майданюк Н.В. [5], в який

виділено методи, необхідні дані та перспективи застосування кожного з математичних інструментів.

Виділення невирішених раніше частин загальної проблеми.

Моделювання надійності IoT-систем є важливим завданням, яке дозволяє оцінити ймовірність збоїв та відмов системи, а також ідентифікувати потенційні слабкі місця. Існує багато різних методів моделювання надійності IoT-систем, кожен з яких має свої переваги та недоліки. Серед основних недоліків відомих та розроблених рішень слід назвати такі :

- Складність. Багато методів моделювання надійності IoT-систем є складними та потребують значних знань та досвіду в галузі математики, статистики та інформатики. Це може ускладнити їх використання для непрофесіоналів.
- Неточність. Жодна модель надійності не може бути абсолютно точною. Моделі завжди ґрунтуються на припущеннях та спрощеннях, які можуть призвести до неточностей в прогнозах.
- Неповнота. Багато моделей надійності IoT-систем не враховують всі фактори, які можуть впливати на надійність системи. Це може призвести до недооцінки ризиків.
- Статичність. Деякі моделі надійності IoT-систем є статичними і не враховують динамічну поведінку системи. Це може зробити їх неточними для систем, які змінюються з часом.

Методи, засновані на теорії надійності добре підходять для моделювання надійності простих компонентів IoT-системи, але вони можуть бути неточними для складних систем з багатьма взаємопов'язаними компонентами. В той же час методи, засновані на моделюванні мереж добре підходять для моделювання надійності мережевих компонентів IoT-системи, але вони можуть бути неточними для систем, які включають компоненти, не пов'язані з мережею.

Не існує універсального рішення для моделювання надійності IoT-систем. Найкращий метод для конкретної системи буде залежати від її складності, доступних даних та ресурсів.

Основною метою дослідження аналіз існуючих способів моделювання та оцінювання надійності та безпеки сучасних IoT-систем, формулювання підходів та методів математичного моделювання IoT-систем з урахуванням інтегрованих показників оцінювання їх функціонування.

Виклад основного матеріалу.

Розглянемо переваги використання систем IoT-систем, та ризики їх впровадження.

Серед переваг використання IoT-систем виділяють такі **:**

- Ефективність та оптимізація бізнес-процесів, оптимізація ресурсів та зменшення витрат.
- Створення комфортного середовища користувачам системи за допомогою розумних IoT-пристроїв.
- Сфера здоров'я. Підвищення якості медичного обслуговування через віддалену діагностику та індивідуальний підхід до лікування.
- Впровадження розумного виробництва для підвищення якості та швидкості виробництва.
- Ефективне управління містами для виявлення та розв'язання громадських проблем.
- Покращення транспортних систем, оптимізація маршрутів, відслідковування вантажів та підвищення безпеки на дорогах.

В той же час використання IoT- систем пов'язано з певними ризиками, пов'язаними з неконтрольованістю таких засобів, особливо під впливом зовнішніх факторів .

До суттєвих ризиків та загроз використання IoT відносят переважно наступне:

- Недостатня безпека даних. Низький рівень захисту може зробити пристрої доступними для хакерів, що загрожує конфіденційності та цілісності даних.
- Ризик зловживання даних. Недоброчесні постачальники можуть використовувати особисті дані користувачів для недобросовісних цілей, що порушує приватність.
- Вразливість інфраструктури. Використання IoT в критичній інфраструктурі може призвести до серйозних наслідків у разі атак або випадкових збоїв.
- Нестабільність мережі. Проблеми зі з'єднанням та доступністю мережі можуть призвести до непрацездатності підключених пристроїв.
- Залежність від технології. Велика залежність від IoT може стати вразливістю, особливо у випадку великої кількості підключених пристроїв.

Розглянемо більш детально загрози для функціонування систем Інтернет-речей.

Існує велика кількість класифікацій загроз для систем Інтернет-речей в залежності від того, який фактор класифікації береться за основу.

Серйозні атаки на пристрої та користувачів відбувалися не тільки з часів появи Інтернету речей. Однак Інтернет речей дає змогу отримати абсолютно новий вимір кібератак завдяки роз-

ширенню мережі та збільшенню кількості мережевих пристроїв. Здебільшого йдеться про наслідки цих атак для захисту даних, але з початком епохи Інтернету речей новий клас пристроїв також з'являється в мережі, що також може висунути питання, пов'язані з безпекою. Атаки зазвичай не мають особливо складної структури і часто діють за однією схемою. Але завдяки великій кількості задіяних пристроїв вони часто можуть досягти більшого ефекту. Крім того, зараз представлено п'ять найвідоміших сценаріїв атак в Інтернеті речей .

1 Ботнет-мережі. За цим сценарієм сукупність підключених пристроїв створює мережу для здійснення більших атак. Мимовільне об'єднання великої кількості систем, які використовуються зловмисною метою, називається ботнет-мережами, або ботнетами. Ці мережі централізовано контролюються відповідними операторами через так звані командно-контрольні сервери. Такі мережі завдають значної шкоди через мільйони запитів до певних систем одночасно, які перевантажені через навантаження та зазвичай руйнуються. У контексті Інтернету речей цей тип мережі також називають роботами, оскільки незалежні мережеві пристрої або речі часто виявляються серед жертв мережевих операторів-ботів. Вони все більше переймають пристрої повсякденного життя, такі як побутова та розважальна електроніка. У більшості випадків користуються їхніми низькими вимогами до безпеки, оскільки багато пристроїв, підключених до Інтернету речей, мають дуже слабкий захист або взагалі відсутні.

Таким чином, подібні стандарти безпеки також повинні бути встановлені для цього класу, наприклад, для онлайн-банківських операцій тощо. Операторам таких ботнетів часто вдається отримати приватну інформацію та, серед іншого, банківські онлайн-рахунки за допомогою великої кількості незахищених пристроїв. На додаток до розподілених атак на відмову в обслуговуванні, ботнети також розсилають масовий спам і фішингові листи.

2. Man-in-the-middle (MITM, «Атака посередника»)

Тип атаки, під час якої зловмисник намагається підслухати та перехопити зв'язок між двома пристроями, називається «атака посередника».

Тоді зловмисник зазвичай намагається перехопити вихідні повідомлення та передати їх у зміненому вигляді фактичному одержувачу. Таким чином цю систему обманюють, вважаючи, що вона все ще спілкується з початковим партнером по розмові. Таким чином зловмисник отримує контроль над пристроєм, що може становити значний ризик для деяких пристроїв у спектрі Інте-

рнету речей. Якщо мова йде не про холодильники, а про зламані транспортні засоби, наприклад, цей сценарій може швидко стати небезпечним для життя людей. Блоки керування промислового виробництва також є популярною мішенню для атак типу «людина посередині», оскільки вони можуть швидко завдати величезних фінансових і матеріальних збитків.

3 Загроза втручання в роботу інформаційних систем та викрадення особистих даних. Поява соціальних мереж і великої кількості пристроїв з підключенням до Інтернету спрощує зловмисникам доступ до особистих даних. Кожен користувач таких пристроїв зберігає там велику кількість дуже приватної інформації. Крадіжка особистих даних спочатку служить для чистого накопичення даних користувача. У подальшому здійснюються спроби маніпулювати власником даних або повністю заволодіти його особистістю. Тоді люди, які контактують із жертвою крадіжки особистих даних, також піддаються ризику від фальшивих запитів від зловмисника. Це часто призводить до великих фінансових вимог, які покриваються довірою особистості жертви. Зважаючи на це, розкриття особистої інформації має здійснюватися обережно.

4. Методи «соціальної інженерії». Методи соціальної інженерії використовуються для отримання конфіденційної інформації від користувачів. Зловмисники намагаються обдурити своїх жертв, щоб отримати доступ до їхніх особистих даних. У більшості випадків для маніпулювання користувачами використовується знайомий інтерфейс сервісу, на якому вони повинні реєструватися. Якщо вони потрапляють на це, зловмисник отримує доступ до їхніх даних для входу, може отримати контроль над обліковим записом користувача та здійснювати транзакції від імені жертви. У більшості випадків заходи соціальної інженерії можна поєднувати з описаними вище методами крадіжки даних і особистих даних, оскільки обидва типи атак переслідують схожі цілі .

5. Відмова в обслуговуванні (DDOS-атаки)

Розподілена атака на відмову в обслуговуванні в контексті ботнетів або речових ботів, зазвичай означає завантаження служби такою кількістю запитів, що вона стає недоступною протягом певного періоду часу. Для цього часто потрібна велика кількість систем, підключених одночасно, тому таку атаку легко можна здійснити за допомогою ботнетів. Успіх або мета такої атаки зазвичай означає втрату репутації та грошей для постраждалих. Однак атаки на відмову в обслуговуванні все частіше виправдовуються ідеалізованими та ідеологічними цілями, що певною мі-

рою робить їх також політичним засобом тиску. Частка пристроїв у цьому сценарії атаки, яка надходить з Інтернету речей, становить 21%, що посилює раніше висловлені проблеми безпеки.

Представлені сценарії атак показують, що Інтернет речей і частини хмарних обчислень повинні продовжувати вирішувати питання безпеки, щоб досягти належного стандарту безпеки. Крім того, показані концепції безпеки мають на меті продемонструвати, що тут також є варіанти захисту або безпечної передачі ідентифікаційних даних. Окрім різної популярності, ці підходи зазвичай відрізняються складністю та архітектурою. Тим не менш, усі підходи впроваджуються великими Інтернет-компаніями, і є зусилля для просування теми безпеки в хмарному середовищі та речах. Перш за все, розширення мереж ставить розробників і користувачів перед проблемою пошуку відповідних рішень для обробки персональних даних.

Визначення ступеню довіри до системи IoT може бути складним процесом внаслідок багафакторності параметрів «довіри»/ надійності системи IoT. вимірювання довіри в системах IoT може бути складним через кілька факторів:

1. *Багатогранність*. Довіра в IoT включає різні аспекти, такі як надійність пристрою, безпека даних, підключення до мережі та поведінка користувачів. Кожен аспект може мати різні показники та міркування, що ускладнює комплексне охоплення загальної довіри.

2. *Динамічне середовище*. Системи IoT працюють у динамічних середовищах, де умови можуть швидко змінюватися. Такі фактори, як коливання мережі, збої в роботі пристроїв або загрози безпеці, можуть вплинути на довіру, вимагаючи постійного моніторингу та адаптації.

3. *Суб'єктивність*. Ступінь довіри часто передбачає суб'єктивне сприйняття та судження. Різні зацікавлені сторони, такі як користувачі, адміністратори або регулятори, можуть по-різному сприймати довіру на основі свого досвіду, очікувань і ролей.

4. *Кількісна оцінка довіри*. Переведення якісних аспектів довіри в кількісні показники може бути складним завданням. У той час як деякі аспекти довірливості можна кількісно визначити за допомогою вимірюваних параметрів, інші можуть покладатися на суб'єктивні оцінки або якісні оцінки.

5. *Взаємозалежність*. На довіру в IoT часто впливають взаємозалежності між пристроями, мережами та програмами. Збій або компроміс в одному компоненті може вплинути на загальну надійність системи, вимагаючи цілісного підходу до вимірювання.

6. Питання безпеки та конфіденційності. Оцінка довіри включає міркування безпеки та конфіденційності, які за своєю суттю є складними в середовищах IoT. Забезпечення безпечних і конфіденційних операцій із збереженням довіри додає рівня складності до вимірювань.

7. Масштабованість: системи IoT можуть масштабуватися, щоб охоплювати величезну кількість пристроїв і взаємодій, що збільшує складність вимірювання довіри в системі. Розміри масштабованості вимагають надійних методологій вимірювання, які можуть адаптуватися до різних масштабів і складності.

8. Контекстуальні фактори: Вимірювання довіри може потребувати врахування контекстуальних факторів, таких як галузеві правила, культурні норми або організаційна політика, що ускладнює процес оцінювання.

Через ці складності вимірювання довіри в системах IoT часто вимагає багатоваріантного підходу, який включає технічний аналіз, погляди зацікавлених сторін, оцінку ризиків і постійний моніторинг. Розробка комплексних структур і методологій, адаптованих до конкретних характеристик і вимог середовищ Інтернету речей, стає важливою для ефективного вимірювання ступеня довіри.

Враховуючи наведені фактори побудуємо узагальнену **модель надійності та безпеки таких систем IoT**.

Пропонуємо фактори, що впливають на надійність системи Інтернету речей (IoT), включити до математичної моделі для кількісного визначення ступеню довіри або надійності. Інтегруючи відповідні фактори у формулу, зацікавлені сторони можуть отримати більш точні залежності та формалізовані вирази. Ось як деякі з цих факторів можуть бути включені:

Формула визначення ступеню довіри:

$$\mathrm{T}=f(Q, U, S, E, N, P, I)\,, \qquad (1)$$

де T — визначає ступінь довіри, Q — якість та виготовлення пристрою, U — оновлення вбудованого програмного забезпечення та програмного забезпечення, S — заходи забезпечення, E — умови середовища, N — з'єднаність мережі, P — живлення та управління енергією, I — взаємодія,

Узагальнена модель надійності системи Інтернет-речей :

$$R=(Q, U, S,E\ , N,P\ ,I\ , M, D\ ) \qquad (2)$$

де:

R — надійність, M — обслуговування та підтримка, D — зберігання та управління даними.

У цих формулах враховуються додаткові фактори, такі як обслуговування та управління даними, для надання всебічного уявлення про надійність.

Модель з ваговими коефіцієнтами:

$$T=w_1\times Q+w_2\times U+w_3\times S+\ldots \quad (3)$$

$$R=w_1\times Q+w_2\times U+w_3\times S+w_4\times M+w_5\times D+\ldots, \quad (4)$$

де w_1 , w_2, w_3, … — це ваги, призначені кожному фактору на основі їх важливості або впливу на довірливість чи надійність.

Ці формули є прикладами загального підходу до моделювання ступеню довіри та надійності системи IoT. Фактичне математичне представлення буде залежати від конкретного контексту, наявності даних та відношень між факторами. Інтегруючи відповідні фактори у математичні моделі, зацікавлені сторони можуть кількісно оцінити та оптимізувати довіру та надійність систем Інтернету речей.

Надійність системи Інтернету речей (IoT) може залежати від багатьох факторів. Зокрема можна навести декілька:

1. Якість IoT-пристроїв і їх виробництва. Якість пристроїв IoT, включаючи їх дизайн, компоненти та виробничі процеси, значно впливає на надійність. Пристрої, виготовлені з високоякісних матеріалів і ретельних випробувань, як правило, мають кращу надійність.

2. Оновлення мікропрограми та програмного забезпечення. Регулярні оновлення мікропрограми та програмного забезпечення пристрою можуть усунути вразливості, покращити продуктивність і підвищити сумісність, тим самим сприяючи загальній надійності системи IoT.

3. Підключення до мережі. Надійність і стабільність мережевих з’єднань, дротових чи бездротових, мають вирішальне значення для підтримки безперервного зв’язку між пристроями IoT і центральною системою.

4. Надійність електроживлення та управління енергією. Адекватне та надійне джерело живлення має важливе значення для пристроїв IoT. Такі фактори, як час автономної роботи, енергоефективні конструкції та рішення для резервного живлення, можуть впливати на надійність систем IoT, особливо у віддалених або складних середовищах.

5. Безпека. Ефективні методи безпеки, включаючи шифрування, автентифікацію та контроль доступу, є критично важливими для захисту пристроїв IoT від несанкціонованого доступу, втру-

чання або зловмисних атак, тим самим підвищуючи надійність системи.

6. Умови навколишнього середовища. робоче середовище, наприклад температура, вологість і вплив пилу або води, може впливати на надійність пристроїв IoT. Пристрої, призначені для роботи в певних умовах навколишнього середовища, мають кращу надійність.

7. Системи зберігання та керування даними. Надійні рішення для зберігання даних і ефективні методи керування даними забезпечують точний збір, зберігання та обробку даних, що є важливим для загальної надійності та функціональності систем IoT.

8. Взаємодія. Здатність пристроїв і компонентів IoT безперебійно працювати один з одним і з існуючими системами або платформами може вплинути на надійність. Тестування взаємодії та сумісності на основі стандартів має вирішальне значення для забезпечення надійної роботи.

9. Технічне обслуговування та підтримка. Профілактичне технічне обслуговування, своєчасне усунення несправностей і оперативна підтримка клієнтів можуть пом'якшити проблеми, усунути збої та підвищити загальну надійність і довговічність IoT-систем.

Враховуючи ці фактори та впроваджуючи відповідні стратегії та практики, стейкхолдери та користувачі систем Інтернету речей можуть підвищити надійність, забезпечуючи постійну продуктивність, безпеку та задоволеність користувачів IoT-систем.

Висновки та пропозиції. Запропоновані нами рішення оцінювання надійності та безпеки систем Інтернет-речей є інтегрованим підходом, який може враховувати множину факторів, які вплив Аналіз надійності та кібербезпеки IoT-систем є важливим процесом, який допомагає виявити потенційні ризики та проблеми.

Існує багато різних методів аналізу надійності та кібербезпеки IoT, кожен з яких має свої переваги та недоліки. Важливо вибрати такі методи аналізу, які відповідають потребам та ресурсам підприємства або власника IoT-системи . Аналіз надійності та кібербезпеки IoT-систем є перманентним та ітеративним процесом, який потребує постійного моніторингу та оновлення.

Надійність та кібербезпека IoT-систем є взаємопов'язаними. Ненадійна система може бути більш схильною до кібератак, і навпаки. Важливо враховувати як надійність, так і кібербезпеку на всіх етапах розробки та експлуатації IoT-систем.

Подальші дослідження IoT-систем можуть бути пов'язані з конкретизацією факторів, які впливають на роботу системи, а також з питаннями: оцінювання найбільш впливових ризиків для надійності та кібербезпеки IoT-систем; розроблення ефективних заходів щодо покращення надійності та кібербезпеки IoT-систем; оцінювання ресурсів, які потрібні для проведення аналізу надійності та кібербезпеки IoT; побудови системи моніторингу для забезпечення постійної надійності та кібербезпеки IoT-систем.

Бібліографічні посилання

1. Giusto, D.; Lera, A.; Morabito, G.; Atzori, L. The Internet of Things; Springer: New York City, NY, USA, 2010.
2. Mamonov, S.; Triantoro, T.M. The strategic value of data resources in emergent industries. Int. J. Inf. Manag. 2018, 39. P.146–155.
3. Pescatore, John and Shpantzer, G «SANS Institute, January: Securing the internet of things survey», 2014.
4. Петренко, К. М. Безпека пристроїв інтернету речей на базі Linux платформи на прикладі інтелектуального транспорту / К. М. Петренко, І. В. Стьопочкіна // XIX Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 13–14 травня 2021 р.) : — Київ : КПІ ім. Ігоря Сікорського, 2021. — С. 396–399.
5. Мамонова Г. В., Майданюк Н. В. Математичний інструментарій для аналізу інтернету речей //Кибернетика и системный анализ. — 2020, Том 56, №4. — С.119-127.
6. Огородников Д. В. Моделювання сценаріїв кіберзагроз для Інтернету речей. — Київ: 2018.

Статтю подано до редакції: 10.11.2023