МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____С.М. Нужний
«18» 06 2025 р.

Кваліфікаційна робота
на правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ПРИСТРОЇВ ІНТЕРНЕТ РЕЧЕЙ

Ступінь вищої освіти: БАКАЛАВР
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконав: студент 4 курсу групи 4381
Туриця Нікіта Андрійович

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Туриця Н.А.

Керівник: доцент кафедри комп'ютерних технологій та інформаційної безпеки к.т.н., доцент **Сірівчук Андрій Сергійович** _____

Миколаїв – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ

Гарант освітньої програми, к.т.н.,
доцент, завідувач кафедри КТІБ
_____С.М. Нужний
«18» ____06____ 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студент: Туриця Нікіта Андрійович

Курс:4

Група: 4381

Ступінь вищої освіти: бакалавр

Галузь знань: 12 Інформаційні технології

Спеціальність: 125 «Кібербезпека та захист інформації»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: «Дослідження властивостей пристроїв Інтернет речей»

затверджена наказом НУК від «_23__» _квітня_____2025 р. № УЧ- 343

2. Вихідні дані до роботи: система класу Інтернет речей; аналіз вразливостей; рішення в безпеці систем Інтернет речей.

3. Перелік питань, які необхідно розробити: зробити опис структури та області застосування систем Інтернет речей; провести аналіз нормативно-правової бази; провести аналіз загроз та шляхів їх зменшення; провести моделювання загроз системи Інтернет речей.

4. Терміни виконання завдання:

термін видачі завдання: «_03_» _лютого_ 2025 р.

термін подання роботи: «18» _червня_ 2025 р.

6. План-графік виконання кваліфікаційної роботи

№ п/п	Заходи	Дата		Готовність	Відмітка про виконання
		Навч. тиждень	Контрольна дата		
1.	Організаційні збори.	23	03.02.2025	Вибір теми, визначення мети, завдань, об'єкта та предмета дослідження	вик
2.	Організаційні збори	25	20.02.2025	Попередній варіант оглядових розділів, підбір і опрацювання списку використаних джерел	вик
3.	Рубіжний контроль	31	03.04.2025	Попередній варіант повної КР.	вик
4.	Рубіжний контроль	33	20.04.2025	Попередній варіант презентації.	вик
5.	ЄДКІ на рівень «бакалавр»	34	29.04.2025	Здавання ЄДКІ зі спеціальності на ступінь бакалавра	вик
6.	Перевірка на плагіат	42	14.06.2025	1. Електронний варіант кваліфікаційної роботи; 2. Подання КР на перевірку на плагіат.	вик
7.	Кафедральний захист	43	18.06.2025	1. Оформлена КР (в форматі pdf) (передається студентом на кафедрі для внутрішньої рецензії, висновок керівника). У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).	вик
8.	Подання документів на захист	44	24.06.2025	1. Подання щодо захисту КР 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Висновок кафедри про КР, допуск до захисту; 4. Електронний варіант та роздрукована презентація в кількості 5 примірників. 5. Електронний варіант КР на диску	вик
9.	Захист КР	44	25.06.2025	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.	вик

ПРИМІТКА: Завдання додається до виконаної роботи та подається до атестаційної комісії.

Керівник
Доцент кафедри комп'ютерних технологій
та інформаційної безпеки, к.т.н., доцент _____ А.С. Сірівчук

Студент _____ Н.А. Туриця

АННОТАЦІЯ

Туриця Н. А. Дослідження вразливостей пристроїв Інтернет речей – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття ступеня вищої освіти «бакалавр» за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології», освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2025.

Пояснювальна записка: 72 с., 6 таб., 1 рис., 22 посилання.

У роботі розглядаються теоретичні та практичні аспекти вразливостей пристроїв Інтернет речей (IoT), що стають об’єктом численних кіберзагроз. Об’єктом дослідження є пристрої та системи IoT, які активно застосовуються у різних сферах, але мають низку вразливостей через особливості архітектури, обмежені ресурси і розподілену структуру. Предметом дослідження є типи атак, шляхи реалізації загроз, а також механізми захисту і управління ризиками в IoT-системах.

Метою роботи є комплексний аналіз сучасних загроз для IoT-пристроїв, огляд нормативно-правової бази, методів побудови моделей загроз, а також розробка рекомендацій щодо зниження кіберризиків на рівні організаційних, технічних і програмних рішень.

У роботі проведено систематизацію основних типів атак на IoT, розглянуто особливості нормативних документів, що регламентують кібербезпеку цих систем, описані методи побудови моделей загроз і стратегії управління ризиками, а також наведено приклади реалізації в реальних проектах. Результати дослідження можуть бути використані для підвищення рівня захищеності IoT-систем, оптимізації управління кіберризиками та впровадження ефективних засобів захисту у промислових і комерційних середовищах.

Ключові слова: Інтернет речей, кібербезпека, вразливості, загрози, моделі загроз, управління ризиками, захист інформації.

ANNOTATION

Turytsia N. A. Research on the vulnerabilities of Internet of Things devices. – Qualification work presented as a manuscript.

Bachelor's qualification work for obtaining the degree of higher education "Bachelor" in specialty 125 "Cybersecurity and Information Protection", field of knowledge 12 "Information Technologies", educational-professional program "Technical Information Security Systems, Automation of Information Processing". – Admiral Makarov National University of Shipbuilding, Mykolaiv, 2025.

Explanatory note: 72 p., 6 tab., 1 fig., 22 references.

The work examines theoretical and practical aspects of vulnerabilities in Internet of Things (IoT) devices, which have become targets of numerous cyber threats. The object of research is IoT devices and systems that are actively used across various domains but have a number of vulnerabilities due to their architecture, limited resources, and distributed structure. The subject of research is types of attacks, threat realization methods, as well as mechanisms for protection and risk management in IoT systems.

The purpose of the work is a comprehensive analysis of current threats to IoT devices, review of the regulatory framework, methods for constructing threat models, and the development of recommendations for reducing cyber risks at organizational, technical, and software solution levels.

The work systematizes the main types of attacks on IoT, considers the specifics of regulatory documents governing cybersecurity of these systems, describes methods for building threat models and risk management strategies, and provides examples of implementations in real projects. The results of the research can be used to increase the security level of IoT systems, optimize cyber risk management, and implement effective protection measures in industrial and commercial environments.

***Keywords**: Internet of Things, cybersecurity, vulnerabilities, threats, threat models, risk management, information protection.*

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 4
ВСТУП 5
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ЗАСТОСУВАННЯ СИСТЕМ ІНТЕРНЕТ РЕЧЕЙ 7
1.1 Поняття та структура систем Інтернет речей 7
1.2 Області застосування систем Інтернет речей 11
1.3 Аналіз нормативно-правової бази що відносяться до систем Інтернет речей 14
2 АНАЛІЗ ВРАЗЛИВОСТЕЙ СИСТЕМ ІНТЕРНЕТ РЕЧЕЙ 24
2.1 Аналіз та шляхи реалізації загроз 24
2.2 Типи атак та наслідки 26
3 АНАЛІЗ РІШЕННЬ БЕЗПЕКИ СИСТЕМ ІНТЕРНЕТ РЕЧЕЙ 33
3.1 Організаційні рішення 33
3.2 Технічні рішення 34
3.3 Програмні рішення 36
4 МОДЕЛЮВАННЯ ЗАГРОЗ ІНТЕРНЕТУ РЕЧЕЙ 39
4.1 Основи побудови моделей загроз для Інтернет речей 39
4.2 Опис об’єкту моделювання 42
4.3 Аналіз загроз та оцінка ризиків для локальних зон використання 46
4.4 Рекомендації щодо контролю безпеки 58
ВИСНОВКИ 69
ПЕРЕЛІК ПОСИЛАНЬ 70

ПЕРЕЛІК СКОРОЧЕНЬ

IDS – Intrusion Detection System (системи виявлення вторгнень)

IoT –Internet of Things (Інтернет речей)

IPS – Intrusion Prevention System (системи запобігання вторгненням)

АС – автоматизована система

АСУ ТП – автоматизованих систем управління технологічними процесами

ЗЗІ – засоби захисту інформації

ІКТ – інформаційно-комунікаційні технології

ІТ – інформаційні технології

КС – комп’ютерні системи

ОТ – операційні технології

ПЗ – програмне забезпечення

ТЗІ – технічний захист інформації

ВСТУП

Інтернет речей (*Internet of Things* (*IoT*)), або як його часто називають, стрімко інтегрується у наше сьогодення, стаючи основою передових технологій, котрі застосовуються на виробництві, в сучасних домівках, у медицині, транспорті та інших галузях. На жаль, цей процес супроводжується підвищенням ризиків кібербезпеки, адже більшість пристроїв *IoT* не мають належного рівня захисту. Вразливості, знайдені в таких пристроях, можуть відкрити двері для несанкціонованого доступу, витоку важливої інформації, керування фізичними об'єктами на відстані та організації масштабних кібератак.

Вивчення та аналіз слабких місць в *IoT*-пристроях є надзвичайно важливим аспектом для гарантування їх безпеки та стабільної роботи. Недостатній рівень захисту може спричинити серйозні проблеми як для пересічних споживачів, так і для державних та комерційних організацій. Відтак, виявлення, детальний аналіз та розробка ефективних методів захисту для *IoT*-пристроїв стають ключовими завданнями у сучасній кібербезпеці.

Метою кваліфікаційної роботи є дослідження вразливостей пристроїв Інтернету речей, аналіз сучасних загроз кібербезпеки, що виникають у процесі їх використання, та розробка рекомендацій щодо підвищення рівня їхнього захисту.

Об’єктом кваліфікаційної роботи є системи Інтернету речей та їхні вразливості, що можуть бути використані зловмисниками для проведення атак.

Предметом кваліфікаційної роботи є аналіз вразливостей пристроїв Інтернету речей, а також методи забезпечення їхнього захисту від потенційних загроз.

Для вирішення поставленої мети вирішено наступні завдання:

– зробити опис структури та області застосування систем Інтернет речей;

– провести аналіз нормативно-правової бази;

– провести аналіз загроз та шляхи їх зменшення;

– провести моделювання загроз системи Інтернет речей.

Дана кваліфікаційна робота може бути використана:

– в якості довідкового матеріалу для розробників *IoT*-рішень, які прагнуть покращити рівень безпеки своїх пристроїв.

– для підвищення обізнаності серед користувачів *IoT*-пристроїв щодо можливих загроз та способів їхнього уникнення.

– як основа для подальших досліджень у сфері кібербезпеки та розробки нових методів захисту.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ЗАСТОСУВАННЯ СИСТЕМ ІНТЕРНЕТ РЕЧЕЙ

1.1 Поняття та структура систем Інтернет речей

Інтернет речей (*Internet of Things* (*IoT*)) – це філософія, що передбачає з'єднання реальних предметів з вмонтованими сенсорами, програмами та іншими механізмами в загальну систему, що використовує інтернет для збору та передачі інформації автономно, без втручання людей. Ці прилади можуть бути найрізноманітнішими: від домашніх приладів до автомобілів, промислових машин та інших пристроїв, які мають можливість комунікувати як між собою, так і з зовнішнім світом [1].

Пристрої *IoT* мають багато переваг, включаючи підвищення продуктивності, прогнозний аналіз, швидке реагування, зменшення людських помилок, створення нових бізнес-можливостей, нові можливості прогнозування та реагування, потужні функції моніторингу, розширений діалог з клієнтами, точне налаштування послуг і продуктів, нові потоки доходів та покращення контролю операційних процесів. Підвищення продуктивності показує, що пристрої *IoT* дозволяють висвітлювати та контролювати різні процеси, що оптимізує різні операції, що підвищує продуктивність та ефективність. Прогнозний аналіз показує, що технології *IoT* дозволяють бачити повторювані закономірності та сприяють технічному обслуговуванню. Швидке реагування показує, що дані дозволяють контролювати системи, що працюють, у режимі реального часу.

Відмінності між пристроями *IoT* та традиційними комп’ютерами можна побачити в їхньому різному призначенні та різному дизайні. Зазвичай пристрої *IoT* не схожі на традиційні комп’ютери. Вони не мають типового інтерфейсу клавіатури та миші, і часто мають інтерфейс користувача, не зосереджений навколо монітора чи іншого екрана, заповненого текстом. Крім того, вони відрізняються тим, як користувачі взаємодіють з цими пристроями. Деякі

пристрої *IoT* вимагають дуже обмеженої взаємодії з боку користувачів. Після налаштування пристрою датчики дозволяють йому автономно генерувати дані. Інші пристрої сприяють більшій взаємодії з користувачем, надаючи більший спектр доступу. Щоб традиційний пристрій можна було оновити та вважати пристроєм Інтернету речей, «він повинен будь-яким чином підключатися до Інтернету та інтегруватися з технологіями за допомогою датчиків, виконавчих механізмів та функціонального програмного забезпечення. Коли вони поєднуються, вони створюють пристрій Інтернету речей. Крім того, традиційні пристрої споживаються на запит, тоді як *IoT* споживається шляхом надсилання технології як сповіщення або дії, коли виявляється ситуація.

Основні компоненти систем *IoT* включають: кінцеві прилади, мережеве обладнання, платформи обробки даних та інтерфейси користувача [2].

1) Кінцеві пристрої в Інтернеті речей – це фізичні об'єкти, які підключаються до мережі та можуть надсилати або отримувати дані. Це «речі», що складають екосистему *IoT*. Прикладами є датчики, виконавчі механізми, смартфони, розумні прилади та різні інші пристрої, оснащені датчиками та можливостями підключення.

Типи кінцевих пристроїв *IoT*:

– датчики –збирають дані з фізичного середовища, такі як температура, вологість, освітлення, тиск або рух;

– виконавчі механізми –реагують на сигнали даних і можуть керувати фізичними процесами, такими як увімкнення світла, регулювання термостата або відкриття клапана;

– розумні пристрої – це пристрої з вбудованою технологією, яка дозволяє їм підключатися до мережі та виконувати певні функції. Прикладами є розумні годинники, розумні телевізори, розумна побутова техніка (холодильники, пральні машини) та розумні системи безпеки;

– прикордонні пристрої –можуть виконувати певну обробку даних локально, перш ніж передавати їх у хмару або на центральний сервер. Це може

включати такі речі, як розумні камери з вбудованим відеоаналізом або маршрутизатори, які керують трафіком даних;

– мобільні пристрої – смартфони, планшети та інші портативні пристрої можуть виступати в ролі кінцевих пристроїв Інтернету речей, особливо коли вони використовуються для керування або моніторингу інших підключених пристроїв.

2) Мережеве обладнання. Зібрану інформацію потрібно транспортувати до обчислювального центру. Для цієї мети застосовуються різноманітні комунікаційні протоколи та технології. Пристрої Інтернету речей використовують різні мережеві інтерфейси для підключення, включаючи *Wi-Fi*, *Bluetooth*, стільниковий зв'язок (наприклад, 4*G* та 5*G*), *Zigbee* та *LPWAN* (низькоенергетичні широкосмугові мережі). Ці технології забезпечують зв'язок між пристроями та Інтернетом, що дозволяє обмін даними та керування ними. Вибір інтерфейсу залежить від таких факторів, як дальність дії, споживання енергії, вимоги до пропускної здатності та вартість.

Поширені мережеві інтерфейси Інтернету речей:

– *Wi-Fi* – ідеально підходить для зв'язку на великій відстані та з високою пропускною здатністю, підходить для таких застосувань, як розумні будинки;

– *Bluetooth* – зв'язок на малій відстані та з низькою пропускною здатністю, часто використовується для підключення пристроїв до смартфонів або концентраторів;

– стільниковий зв'язок (4*G*/5*G*) – забезпечує покриття на великій відстані, підходить для віддалених датчиків, промислових машин та застосувань, що потребують надійного з'єднання;

– *Zigbee* – низькоенергетичний протокол mesh-мережі, який зазвичай використовується в домашній автоматизації та промислових умовах;

– *LPWAN* (низькоенергетична широкосмугова мережа) – розроблений для зв'язку на великій відстані та з низькою пропускною здатністю, підходить для таких застосувань, як розумне сільське господарство та моніторинг навколишнього середовища;

– *Ethernet* – забезпечує дротове підключення для пристроїв, що потребують високої пропускної здатності та надійного зв'язку.

– *RFID* – радіочастотна ідентифікація, що використовується для відстеження та ідентифікації.

3) Сторонні платформи слугують для обробки великих обсягів даних, що генеруються підключеними пристроями. Ці платформи часто надають функції для отримання даних, їх зберігання, обробки в режимі реального часу, аналітики та візуалізації. Деякі популярні варіанти включають A*WS IoT, Azure IoT, Google Cloud IoT, IBM Watson IoT* та варіанти з відкритим кодом, такі як *ThingsBoard* та *ThingSpeak*.

Корпоративні хмарні платформи:

– *AWS IoT* – комплексна платформа від *Amazon Web Services*, що пропонує керування пристроями, безпечне підключення та сервіси обробки даних, такі як AWS IoT Analytics;

– *Azure IoT* – пакет *Azure IoT* від *Microsoft* забезпечує керування пристроями, аналіз даних та інтеграцію з іншими сервісами *Azure*, включаючи *Stream Analytics* для обробки в режимі реального часу;

– *Google Cloud IoT* – пропозиція *IoT* від *Google Cloud Platform* включає *IoT Core* для керування пристроями та *Dataflow* для потокової та пакетної обробки, а також інші аналітичні сервіси;

– *IBM Watson IoT* – платформа IBM зосереджена на підключенні, управлінні та аналізі даних *IoT*, використовуючи штучний інтелект та когнітивні обчислення для розширеної аналітики та висновків.

Платформи з відкритим кодом та спеціалізовані платформи:

– *ThingsBoard* – платформа з відкритим кодом для збору, обробки, візуалізації та керування пристроями даних, відома своєю масштабованістю та підтримкою різних протоколів підключення;

– *ThingSpeak* – Платформа для збору, візуалізації та аналізу потоків даних Інтернету речей, особливо корисна для створення прототипів та розробки рішень Інтернету речей;

– *Apache Kafka* – розподілена потокова платформа для високопродуктивних, відмовостійких конвеєрів даних, часто використовується для обробки даних у реальному часі в Інтернеті речей.

– *Apache Flink* – фреймворк для обробки потоків, відомий низькою затримкою та обчисленнями з урахуванням стану, ідеальний для обробки складних подій у застосунках Інтернету речей.

4) Користувацький інтерфейс для Інтернету речей діє як місток між користувачами та підключеними пристроями, дозволяючи їм взаємодіяти та керувати пристроями та даними, які вони генерують. Цей інтерфейс може мати різні форми, включаючи фізичні інтерфейси, такі як кнопки та дисплеї, та цифрові інтерфейси, такі як додатки для смартфонів або веб-панелі керування:

– мобільні застосунки – забезпечують можливість дистанційного доступу та керування пристроями *IoT* за допомогою смартфонів чи планшетів.

– веб-інтерфейси – надають користувачам можливість отримувати дані та керувати пристроями через інтернет-браузер.

– голосові помічники: Інтеграція з голосовими асистентами, такими як *Amazon Alexa* або *Google Assistant*, для керування пристроями за допомогою голосу.

Ефективні інтерфейси *IoT* надають пріоритет ясності, простоті використання та адаптивності до різних контекстів, гарантуючи, що користувачі можуть легко взаємодіяти з підключеними пристроями та розуміти надану ними інформацію.

1.2 Області застосування систем Інтернет речей

Інтернет речей нині є однією з найбажаніших технологій сучасності, що дає змогу з'єднувати фізичні пристрої через мережу для обміну даними та їх автоматичної обробки без прямого впливу людини. Основними аспектами використання *IoT* є автоматизація процесів, покращення ефективності й оптимізація ресурсів. Застосування технологій *IoT* стосується багатьох сфер,

таких як розумні міста, охорона здоров'я, транспорт, промисловість, сільське господарство, фінанси та інші. Завдяки цим системам виникають нові можливості для управління та моніторингу в режимі реального часу, що значно поліпшує якість життя [3].

Пристрої Інтернету речей можуть використовуватися в багатьох різних сферах та мати багато різних цілей. Їх можна розділити на три різні категорії залежно від того, кому вони служать. Ці категорії включають громадськість, бізнес та особисте використання. Пристрої Інтернету речей можна додатково класифікувати за способом їх використання в громадському, бізнес та особистому секторах.

Особистий використання:

– розумне здоров'я та благополуччя. Ці пристрої дозволяють споживачам носити їх у вигляді одягу, годинників та телефонів, поки вони займаються іншими справами, такими як фізичні вправи, харчування, робота, сон тощо. Цей тип пристрою Інтернету речей контролює здоров'я людини (фізичне, психічне, емоційне), аналізує її одужання, повідомляє відповідні установи (лікарів, родину, 911), надає рекомендації або допомагає з відповідними діями. Наприклад, вони можуть допомогти відстежувати цілі фітнесу. Це також допомагає в бізнесі та державному секторі, оскільки лікарні можуть використовувати ці системи для моніторингу медичного обладнання, ліків та інструментів за допомогою пристроїв *IoT*. Лікарні та медичні заклади використовують монітори пацієнтів, рентгенівські прилади, трекери та інші носимі пристрої, які підключаються до мережі, а пристрої *IoT* значно скорочують витрати;

– розумний дім. Цей тип пристроїв *IoT* постійно контролює безпеку будинку (виявлення руху, диму, газу), навколишнє середовище (тепло, повітря), побутову техніку, обладнання, безпеку та спостереження, надає рекомендації або системи для певних станів (температури). Користувачами цих пристроїв можуть бути будь-хто, від немовлят до людей похилого віку. Крім того, користувач може контролювати та керувати побутовою технікою, розважальними пристроями та, зрештою, всім будинком;

– розумна освіта. Цей тип пристроїв *IoT* дозволяє постійно контролювати учня та заохочувати його, рекомендувати навчальні матеріали та ставити відповідні запитання залежно від прогресу учня. Крім того, пристрій може повідомляти вчителя, адміністратора та батьків про прогрес учня.

Громадське застосування:

– розумне середовище. Цей тип системи Інтернету речей контролює навколишнє середовище та повідомляє користувачів про забруднення, радіацію, екстремальні погодні умови, стихійні лиха тощо. Рятувальники можуть використовувати цю систему Інтернету речей, щоб допомогти врятувати людей у небезпеці. Також системи Інтернету речей можна використовувати для територіального моніторингу, спостереження та захисту кордонів;

– розумні комунальні послуги. Ці системи Інтернету речей можна використовувати для розумного обліку, обслуговування та виставлення рахунків за комунальні послуги;

– розумне місто/громада. Це стосується автоматизації всього міста або середовища та управління ним через Інтернет. Наприклад, керування світлофорами та моніторинг забруднення.

Бізнес-підрозділ:

– розумна будівля. Цей тип пристроїв Інтернету речей допомагає контролювати та контролювати доступ до будівлі та середовище, таке як освітлення, температура, обладнання та використання ресурсів. Їх можна використовувати для вимірювання для контролю енергії, щоб можна було знизити витрати. Крім того, їх можна використовувати для безпеки та спостереження, у разі надзвичайної ситуації та вживати відповідних заходів.

– розумна промисловість. Цей тип системи Інтернету речей можна використовувати на розумних заводах, у виробництві, гірничодобувній промисловості та будівництві для покращення виробництва. Багато компаній зацікавлені в хімічних датчиках та системах, і вони хочуть використовувати *IoT* для моніторингу операційної інфраструктури, оскільки зростає потреба в підключенні сучасних машин;

– розумні послуги. Цей тип системи *IoT* може використовуватися у фінансовій, банківській, страховій, сервісній сфері для моніторингу людей, даних та ресурсів для покращення своїх послуг;

– розумна роздрібна торгівля та логістика. Цю форму системи *IoT* можна використовувати для відстеження продуктів, моніторингу вантажів, щоб вони могли оптимізувати рівень запасів та запасів, зменшити крадіжки та підтримувати якість. Крім того, вони можуть контролювати продукти на складі та транспорті, надавати рекомендації та сповіщати, коли продукти не зберігаються відповідно до вимог;

– розумний транспорт. Ці системи *IoT* можуть використовуватися для моніторингу пасажирів, транспортних засобів, багажу, контейнерів та інфраструктури для оптимізації транспортування наземним, повітряним або водним транспортом. Підключені автомобілі та розумні транспортні засоби взаємодіятимуть, щоб уникнути аварій, покращити інформаційно-розважальну систему та зменшити затори, споживання енергії, забруднення та втрати часу. Розумне управління автопарком зменшить витрати, час доставки, втрачений простір на коліях тощо. Нарешті, транспортування небезпечних матеріалів (наприклад, їдких, легкозаймистих, токсичних, вибухових) буде покращено;

– розумне сільське господарство. Системи *IoT* контролюватимуть ферму, посіви, виноградники, теплиці, худобу, тварин, сільськогосподарське обладнання та техніку (трактори, розподіл добрив), надаватимуть рекомендації або вживатимуть відповідних заходів (наприклад, зрошення, підживлення) для підвищення якості та кількості продукції.

1.3 Аналіз нормативно-правової бази що відносяться до систем Інтернет речей

1.3.1 Проблеми правової бази використання Інтернет речей.

В Україні наразі не існує окремих законів, що безпосередньо регулювали б питання *IoT*[4]. Це призводить до правової невизначеності для розробників,

виробників і споживачів *IoT*-рішень. Більшість аспектів діяльності в цій сфері врегульовано загальними нормами законів про інформацію, телекомунікації та захист особистих даних. Зокрема, Закон України «Про інформацію» та Закон України «Про захист персональних даних» містять загальні положення, які можуть бути застосовані до *IoT*, але не беруть до уваги специфіку цієї технології.

Пристрої інтернету речей (IoT) нерідко фіксують та обробляють значні обсяги особистої інформації. Відсутність зрозумілих правил стосовно збору, зберігання та обробки такої інформації може спричинити порушення права людей на конфіденційність. Є Необхідно враховувати міжнародний досвід, особливо Загальний регламент про захист даних (*GDPR*) Європейського Союзу, котрий встановлює високі вимоги до захисту особистих даних.

Розмаїття пристроїв і платформ *IoT* зумовлює необхідність вироблення узгоджених стандартів для забезпечення їхньої взаємодії та безпечної роботи. За відсутності цих стандартів можуть виникнути технічні й правові складнощі, пов’язані з інтегруванням різнорідних систем та гарантуванням їхньої захищеності.

Зростання кількості гаджетів, що інтегруються в мережу, породжує серйозні кіберзагрози. Вимагається створення законодавчих актів, що окреслюють стандарти захисту для *IoT*-пристроїв та санкції за їх ігнорування. Закон України "Про основні засади забезпечення кібербезпеки України" закладає фундамент для захисту національних інтересів в кіберпросторі, проте специфіка *IoT* в ньому відсутня. Тому актуальним є внесення поправок до чинного закону, або ж розробка окремого нормативного документа, цілком присвяченого безпеці *IoT*.

Законодавство України наразі не передбачає уніфікованої системи ліцензування й сертифікації пристроїв *IoT*. Відсутність чітких правил сертифікації може генерувати небезпеки стосовно якості та безпечності таких пристроїв. Впровадження обов'язкової сертифікації могло б позитивно вплинути на зростання рівня довіри до технологій *IoT* та зменшення ризиків, асоційованих з кібератаками.

Закон не пропонує чітких правил, які б визначали відповідальність виробників, постачальників послуг або користувачів *IoT* у випадку збоїв або порушень безпеки. Це може ускладнювати вирішення суперечок та захист прав споживачів. Варто розробити правові механізми, які б врегульовували питання відповідальності за неналежну роботу *IoT*-систем.

1.3.2 Нормативні документи України, що регламентують роботу *IoT*-систем.

1) Наказ Адміністрації Держспецзв’язку від 14.09.2024 № 505 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту при використанні технології хмарних обчислень та Методичних рекомендацій щодо оцінки відповідності хмарних послуг рівням безпеки (впевненості)»[5]. Даний документ регламентує оцінку відповідності у сфері хмарних послуг вимог законодавства у сферах захисту інформації та кіберзахисту.

Приведені методики є одним з етапів побудови системи безпеки, що ґрунтується на моделі ПВПД (плануй – виконуй – перевіряй – дій), що представлена в *ISO/IEC* 27001:2022.

2) Наказ Адміністрації Держспецзв'язку від 29.05.2023 № 463 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами» [6]. Цей нормативний акт представляє собою ключовий елемент національного нормативно-методичного підґрунтя у сфері кібербезпеки об'єктів критичної інформаційної інфраструктури, особливо автоматизованих систем управління технологічними процесами (АСУ ТП), котрі активно інтегруються з середовищем Інтернету речей.

Завданням прийняття цих методичних рекомендацій було гарантування єдиного підходу до організації системи кіберзахисту АСУ ТП, враховуючи інтеграцію з *IoT*-пристроями. Документ визначає вимоги до проектування, реалізації, супроводу та покращення заходів кібербезпеки в технологічних середовищах.

Мета розробки методичних рекомендацій полягала в запровадженні уніфікованого підходу до організації системи кібербезпеки АСУ ТП, враховуючи також інтеграцію з *IoT*-пристроями. Даний документ визначає норми щодо проєктування, реалізації, супроводу та вдосконалення заходів кіберзахисту в технологічних середовищах.

Основні аспекти цього документу передбачають:

– уточнення характерних загроз та способів атак, здатних проникнути в АСУ ТП крізь *IoT*-пристрої. Це включає несанкціонований доступ до мережевих компонентів, втручання в процес управління, а також зміни показників телеметрії;

– положення щодо зонування мережі: рекомендації щодо фізичного та логічного розділення IT та OT мереж. Це сприяє скороченню зони потенційного впливу та локалізації можливих загроз;

– нормативне встановлення вимог до впровадження систем виявлення вторгнень (*IDS/IPS*), механізмів контролю доступу, ведення журналів подій та регулярного аудиту безпеки;

– визначення етапів життєвого циклу АСУ ТП, для кожного з яких передбачено застосування відповідних заходів кібербезпеки – від планування і розгортання до безпосереднього використання та виведення з експлуатації;

– рекомендації стосовно розробки документації з безпеки: політики безпеки, моделі загроз, плани реагування на інциденти та процедури резервного копіювання.

Окрему увагу зосереджено на інтеграції з *IoT*-компонентами, що часто функціонують як датчики або виконавчі механізми в технологічних інфраструктурах. Методичні поради підкреслюють потребу в автентифікації *IoT*-приладів, застосуванні протоколів із шифруванням (*TLS, VPN* та інші), а також у лімітуванні доступу до зовнішніх мереж.

Додатково, документ виділяє значущість навчання персоналу, регулярного тестування системи безпеки (враховуючи симуляції атак) і впровадження інструментів моніторингу в режимі реального часу.

Отже, Наказ №463 постає як приклад актуального нормативного документа, що приймає до уваги специфіку як традиційних промислових систем, так і нових викликів, пов'язаних із поширенням *IoT* у критичних галузях. Його пункти носять рекомендаційний характер, але вони закладають фундамент для подальшої стандартизації та впровадження обов'язкових вимог у сфері кіберзахисту в Україні.

3) НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

НД ТЗІ 2.5-004-99 - це ключовий нормативний акт у галузі технічного захисту інформації (ТЗІ) на теренах України [7]. Його настанови зберігають свою вагу навіть з огляду на швидке вдосконалення технологій Інтернету речей (*IoT*), адже він визначає базові стандарти для оцінки захищеності даних, що опрацьовуються в усіх комп’ютерних системах, включаючи розподілені та вбудовані *IoT*-рішення.

Головне завдання цього документу - формування єдиного підходу до класифікації ступенів захисту інформації в інформаційних системах, з оглядом на вид інформації, що обробляється, рівень її важливості та ймовірність неправомірного доступу.

Ключові положення стандарту:

– встановлення рівнів захищеності комп’ютерних систем (КС), починаючи від найвищого, першого, до четвертого, що визначає мінімальні вимоги. Ці рівні розглядають кількість та різновиди застосованих заходів безпеки, таких як аутентифікація, управління доступом, криптографічні засоби, аудит, ізоляція процесів та інші;

– критерії оцінки базуються на аналогії з міжнародним стандартом *Trusted Computer System Evaluation Criteria* (*TCSEC*), беручи до уваги специфіку національного середовища. Кожен рівень передбачає обов’язкові вимоги до захисних функцій та їх практичної реалізації;

– методика перевірки відповідності КС визначеному рівню: визначено механізми оцінювання відповідності критеріям, надано опис вимог до

обґрунтування використаних технічних і програмних засобів захисту, а також процедури сертифікаційної експертизи.

Для *IoT*-систем цей документ має значний зиск, бо надає можливість сформулювати вимоги щодо базової захищеності окремих елементів – контролерів, сенсорів, шлюзів, – які обмінюються інформацією в локальній чи глобальній мережі. Скажімо, при створенні системи збору даних з датчиків, які відправляють інформацію до обчислювального центру, важливо встановити, на якому рівні має бути здійснено контроль доступу до даних і як захищено сам канал передавання.

Попри те, що документ було розроблено для традиційних комп'ютерних систем, його засади, зокрема багаторівневий підхід до оцінювання безпеки та використання моделі захисту, здатні адаптуватися до *IoT*-середовища, котре часто включає гетерогенні пристрої з обмеженими обчислювальними можливостями.

Окрім цього, НД ТЗІ 2.5-004-99 визначає теоретичну базу для імплементації процедур сертифікації інформаційної системи, що має критичне значення для промислових або державних *IoT*-рішень, де відповідність державним нормам є обов'язковою умовою.

Відтак, цей нормативний документ залишається актуальним джерелом методології для оцінки захищеності інформації навіть в умовах сучасних кіберзагроз та розвитку розподілених цифрових технологій.

4) НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і формування стандартних функціональних профілів захищеності інформації від несанкціонованого доступу».

Документ НД ТЗІ 2.5-005-99 створено в рамках загального стратегічного плану розбудови національної системи технічного захисту інформації, слугуючи логічним продовженням НД ТЗІ 2.5-004-99 [8]. Основна мета цього документа полягає у встановленні основ класифікації автоматизованих систем (АС), беручи до уваги умови обробки даних та можливі загрози, що виникають через несанкціонований доступ до цих систем.

У документі міститься стандартизований підхід до створення функціональних профілів захисту, що забезпечує системний підхід до проєктування безпеки в ІТ-інфраструктурах, зокрема, й у сучасних *IoT*-рішеннях.

Ключові моменти документа передбачають:

– категоризацію автоматизованих систем за рівнями захищеності, що враховують тип інформації, з якою вони працюють (відкрита, конфіденційна, службова, державна та інші), кількість користувачів, структуру системи та підключення до зовнішніх мереж, включаючи мережу Інтернет.

– визначення стандартних функціональних профілів захисту, які містять типові набори функцій безпеки, що повинні бути впроваджені в системах певного типу. Це сприяє стандартизації вимог до захисту та мінімізує суб'єктивність під час сертифікації або оцінювання безпеки.

– регламентацію складових профілю захищеності, включаючи: аутентифікацію користувачів, контроль доступу, криптографічний захист, аудит дій, резервне копіювання, захист від шкідливого програмного забезпечення тощо;

– опис процедур застосування профілів у реальних проєктах, починаючи з аналізу вимог і до впровадження заходів безпеки. Також, документ радить регулярно перевіряти відповідність фактичної реалізації системи вибраному профілю.

У сфері Інтернету речей, документ стає надзвичайно важливим, надаючи розробникам та адміністраторам систем *IoT* можливість визначати оптимальний функціональний профіль безпеки. Вибір залежить від конкретних завдань системи, характеру даних, які вона обробляє, та середовища, де вона працює.

Зокрема, для *IoT*-систем, призначених для охорони або збору телеметричних даних в критичній інфраструктурі, профілі захисту відповідно до вимог НД ТЗІ 2.5-005-99 можуть передбачати обов’язкове впровадження засобів контролю доступу до пристроїв, шифрування даних при передачі, аутентифікацію вузлів мережі та проведення регулярного аудиту активностей.

Отже, НД ТЗІ 2.5-005-99 виступає як стандартизований підхід до кібербезпеки, який значно полегшує створення захищених, масштабованих та керованих *IoT*-систем. Це забезпечує чітку відповідність національним стандартам у галузі захисту інформації.

1.3.3 Міжнародні нормативні документи, що регламентують роботу IoT-систем.

Формування ефективних, безпечних та взаємосумісних систем Інтернету речей (*IoT*) неможливе без опори на нормативно-правову та стандартизовану базу. Міжнародні стандарти, розроблені організаціями *ISO* та *IEC*, регламентують ключові аспекти побудови та експлуатації таких систем – від визначення термінології до моделювання архітектури, забезпечення сумісності, захисту даних і гарантій надійності. Нижче наведено аналіз низки актуальних документів, що становлять основу для проектування і впровадження *IoT*-рішень у сучасних інформаційних середовищах.

ISO/IEC 20924:2018 – Інформаційні технології – Інтернет речей – Словник. [9] Цей стандарт є фундаментальним з точки зору формування уніфікованого понятійного апарату в сфері *IoT*. Він встановлює однозначне трактування базових термінів (наприклад, «пристрій *IoT*», «платформа *IoT*», «послуги *IoT*»), що сприяє узгодженості між технічними розробниками, споживачами, регуляторними органами та міжнародними партнерами. Забезпечення термінологічної узгодженості є передумовою для міждисциплінарної інтеграції *IoT*-технологій у суміжні галузі – від медицини до енергетики.

ISO/IEC 21823-1:2019 – Сумісність систем Інтернету речей – Частина 1: Фреймворк [10]. Документ визначає методологію забезпечення міжсистемної сумісності між гетерогенними *IoT*-пристроями, які можуть використовувати різні протоколи, формати обміну та мережеві інтерфейси. Він описує загальну модель побудови сумісного середовища, у якому пристрої можуть обмінюватися інформацією без необхідності уніфікації на апаратному рівні. Реалізація

подібного фреймворку є критично важливою для масштабування IoT-інфраструктур та їх стійкості до зміни постачальників.

ISO/IEC 30141:2018 – Еталонна архітектура Інтернету речей.[11] Даний стандарт розглядає модельну архітектуру *IoT*-систем із поділом на функціональні рівні: фізичний (сенсори, виконавчі пристрої), мережевий, рівень обробки даних, управління, сервісів та взаємодії з користувачем. Стандарт задає принципи побудови модульних, масштабованих і безпечних систем, приділяючи особливу увагу питанням автентифікації, контролю доступу, керування ідентичностями пристроїв та моніторингу стану мережі.

ISO/IEC 29182-3:2014 – Сенсорні мережі: еталонна архітектура – Частина 3: Типи архітектур [12]. У документі наведено класифікацію архітектур сенсорних мереж відповідно до особливостей предметної області. Стандарт дозволяє адаптувати загальні принципи побудови до галузевих вимог (екологія, сільське господарство, безпека тощо), забезпечуючи відповідну гнучкість *IoT*-систем. Також він містить рекомендації щодо розподілу обчислювального навантаження, енергозбереження та організації топології мережі залежно від умов застосування.

ISO/IEC 30128:2014 – Загальний інтерфейс застосування для сенсорних мереж [13]. Стандарт визначає принципи побудови абстрактного програмного інтерфейсу, через який сенсорні пристрої можуть взаємодіяти з платформами обробки даних. Його реалізація дозволяє забезпечити інтероперабельність між пристроями різних виробників та різного покоління, а також підтримувати масштабованість інфраструктури без потреби в її глибокій реконфігурації. Особлива увага приділяється ефективності передавання даних у режимі реального часу та обмеженням затримок у критичних застосуваннях.

ISO/IEC 30147 — Методологія забезпечення надійності систем *IoT*. [14] Документ охоплює повний життєвий цикл *IoT*-систем — від проектування та тестування до обслуговування й модернізації. Стандарт формулює вимоги до надійності функціонування систем у довготривалій перспективі, включаючи такі аспекти, як резервування, відновлення після збоїв, захист від одиничних точок

відмови, а також вимоги до оновлення програмного забезпечення без порушення основних сервісів. Це має особливе значення для *IoT*-рішень у сферах охорони здоров'я, транспортної логістики та промислової автоматизації.

*ISO/IEC NP*30161:2020– Вимоги до платформ обміну даними *IoT*. [15] Стандарт розглядає концептуальні основи створення платформ, які дозволяють забезпечити безпечний та уніфікований обмін даними між різними сервісами та компонентами *IoT*-інфраструктури. Документ визначає технічні вимоги до протоколів взаємодії, механізмів верифікації автентичності даних, управління доступом, а також до моделей зберігання й маршрутизації інформації. Створення таких платформ є ключем до формування відкритих, масштабованих екосистем, що охоплюють кількох провайдерів послуг.

ISO/IEC 27001 - це міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою (*ISMS*) в організаціях [16]. Цей стандарт спрямований на забезпечення захисту інформації та даних, включаючи особисті дані, від різних загроз, таких як кібератаки, неправомірний доступ, втрати даних та інші інформаційні ризики.

Стандарт *ISO/IEC* 29100 є міжнародним стандартом [17], який визначає загальні вимоги до управління приватністю та захисту даних для інформаційно-комунікаційних технологій (ІКТ) та систем. Основна мета цього стандарту полягає в забезпеченні високого рівня захисту приватності індивіда в контексті використання та обробки ІКТ-даних.

2 АНАЛІЗ ВРАЗЛИВОСТЕЙ СИСТЕМ ІНТЕРНЕТ РЕЧЕЙ

2.1 Аналіз та шляхи реалізації загроз

Пристрої Інтернету речей піддаються більшому ризику, ніж традиційні пристрої, з кількох різних причин, як обговорюється нижче [18].

– вразливості на рівні апаратного забезпечення. Пристрої Інтернету речей зазвичай виготовляються з низькою обчислювальною потужністю та апаратними обмеженнями, що не дозволяє використовувати вбудовані засоби безпеки. Функції безпеки для пристроїв Інтернету речей додаються лише за необхідності та лише якщо віддалені атаки вважаються основною загрозою. Тому ці пристрої мають вразливості на рівні апаратного забезпечення, оскільки їх можна використовувати віддалено. Крім того, хакерам неважко використовувати прості методи для проникнення в системи. Ось чому важливо зробити все можливе, як споживачі та виробники, щоб підготувати системи до атак;

– попит і пропозиція. Компанії змагаються, щоб скористатися перевагами Інтернету речей, оскільки вони стають все більш популярними. Компанії намагаються бути першими на ринку та йти в ногу з темпами розвитку цих пристроїв, тому вони ігнорують проблеми безпеки, які можуть виникнути. Зосереджуючись переважно на функціональності пристрою Інтернету речей, пристрій залишається відкритим і може бути небезпечним, оскільки не може захистити конфіденційну інформацію;

– облікові дані за замовчуванням. Багато споживачів не скидають паролі на пристроях Інтернету речей, а багато компаній роблять облікові дані слабкими, легкими для вгадування або жорстко закодованими. Жорстко закодовані паролі – це незашифровані паролі, які вони залишають у вихідному коді пристрою.

– скомпрометований інтерфейс. Інтерфейс, який пристрій Інтернету речей використовує для підключення до більшої мережі, такої як мережі 5*G*, може бути скомпрометований. Коли інтерфейс стає скомпрометованим, це зазвичай

трапляється через відсутність автентифікації чи авторизації під час доступу до пристрою;

– відсутність перевірки прошивки. Якщо на пристрої виявлено вразливість, деякі пристрої неможливо оновити, оскільки не реалізовано перевірку прошивки. Оновлення буде у вигляді простого тексту, або користувач не буде повідомлений про оновлення, і немає «механізмів захисту від відкату». Механізми захисту від відкату завадять зловмисникам понизити версію пристрою до старішої, яку зловмисник може використати.

Основними шляхами реалізації загроз є:

. Фізичний доступ до пристроїв. Оскільки чимало *IoT*-пристроїв розташовуються у відкритих місцях (наприклад, камери спостереження чи розумні лічильники води), до них можливий фізичний доступ. Через порт *UART* або інші інтерфейси на апаратному рівні зловмисники здатні скинути налаштування, перепрошити нове ПЗ або зламати систему захисту. У деяких випадках навіть просто вимкнення живлення може перезавантажити пристрій у режимі налагодження. Атаки типу *side-channel* або *glitching* теж можуть бути використані для фізичного злому.

5. Вразливості в прошивках пристроїв.

Проблеми з прошивками здебільшого виникають через використання застарілих бібліотек чи відсутність оновлень від виробника. Деякі виробники припиняють підтримку пристроїв після продажу, тому не виправляють виявлені уразливості. Наприклад, дослідники безпеки неодноразово знаходили уразливості у популярних маршрутизаторах, що дозволяло отримати *root*-доступ до системи. Також можуть траплятися *hardcoded credentials* або небезпечні API-інтерфейси без обмежень доступу.

6. Компрометація шлюзів *IoT*.

IoT-шлюзи – це центральні точки, через які йде весь потік даних від пристроїв до серверів. Якщо зловмисник отримає доступ до шлюзу, він може коригувати чи підміняти трафік, ініціювати атаки "людина посередині", або ж вивести з ладу всю систему. Наприклад, вразливість в протоколах *MQTT* або

CoAP дозволяє атакувальникам перехоплювати незашифровані повідомлення. Також існує ризик використання підроблених сертифікатів для перехоплення *TLS*-з’єднань.

Вразливості, знайдені в протоколах комунікації, таких як *MQTT, CoAP, Zigbee* або *Bluetooth Low Energy*, також є джерелом серйозних ризиків. Коли бракує шифрування або автентифікації, це дає зловмисникові змогу перехоплювати, змінювати або підробляти повідомлення, які передаються, що може порушити стабільність роботи цілих систем.

Окрім того, існує загроза ін'єкційних атак, коли зловмисник надсилає згубні команди, що модифікують роботу пристрою. Ці команди здатні вимикати сигнали тривоги, вмикати або блокувати системи захисту, а також ініціювати дії, які несуть небезпеку для користувача.

Останній, проте не менш значущий різновид загроз — це атаки на процедуру оновлення прошивки. Коли оновлення не мають цифрового підпису або ж завантажуються через незашифровані шляхи, зловмисник може підмінити прошивку на змінену версію, що може надати йому абсолютний контроль над пристроєм і дасть змогу виконувати будь-які команди.

7. Використання підробок або несертифікованих пристроїв.

Поширення дешевих і несертифікованих пристроїв з Китаю чи інших місць становить серйозну небезпеку. Такі пристрої можуть містити бекдори – спеціальні механізми доступу, встановлені на етапі виробництва. Крім цього, низька якість складання та відсутність оновлень сприяють появі уразливостей, які ніхто не виправляє. Часто ці пристрої не відповідають міжнародним стандартам безпеки (наприклад, *ISO/IEC* 27030).

2.2 Типи атак та наслідки

Системи Інтернету речей (*IoT*) дедалі частіше потрапляють у поле зору кіберзлочинців. Причина криється у їхній розподіленій природі, великій кількості точок входу, обмеженості обчислювальної потужності та часто

недосконалій системі безпеки. Серед численних видів атак, що застосовуються, особливу увагу слід звернути на найбільш поширені, які можуть мати серйозні наслідки як для звичайних користувачів, так і для важливої інфраструктури [19].

Серед основних атака слід виділити такі:

– використання кейлогеру – це тип програмного забезпечення для моніторингу, яке записує послідовність клавіш та натискання клавіш на веб-сайт або в програму та надсилає їх назад третій стороні. Ці файли журналів можуть навіть містити ваші особисті ідентифікатори електронної пошти та паролі. Також відомий як захоплення клавіатури, він може бути як програмним, так і апаратним. У той час як програмні кейлогери націлені на програми, встановлені на комп'ютері, апаратні пристрої націлені на клавіатури, електромагнітне випромінювання, датчики смартфонів тощо.

Кіберзлочинці мають реєстратори натискань клавіш у своїх інструментах для захоплення фінансової інформації, такої як банківські дані та дані кредитних карток, особиста інформація, така як електронні адреси та паролі, або імена та адреси чи конфіденційна бізнес-інформація, включаючи процеси та майно. Вони мають можливість продавати таку інформацію іншим організаціям у рамках більшої атаки.

– атака відмови в обслуговуванні відбувається (*DDoS*), коли користувачі не можуть отримати доступ до інформаційних систем або мережевих ресурсів через те, що зловмисник виводить з ладу сайт або сервер (шляхом перевантаження цільового хоста або мережі трафіком, доки ціль не зможе відповісти або просто не вийде з ладу, перешкоджаючи доступу для законних користувачів). *DoS*-атаки можуть коштувати організації як часу, так і грошей, поки її ресурси та послуги недоступні.

Розподілена атака відмови в обслуговуванні (*DDoS*) відбувається, коли кілька пристроїв атакують одну ціль. Багато зловмисників використовують ботнети (групу викрадених пристроїв, підключених до Інтернету, для здійснення масштабних атак). Ці атаки дозволяють надсилати експоненціально більше запитів до цілей і ускладнюють ідентифікацію джерела;

– фішинг – це атака соціальної інженерії, яка використовується для крадіжки даних користувачів, таких як облікові дані для входу та паролі. Це відбувається, коли хакер копіює найчастіше відвідувані сайти, електронні листи або повідомлення та ловить жертву, надсилаючи це підроблене посилання. Це призводить до встановлення шкідливого програмного забезпечення, яке може мати руйнівні наслідки. Це може спричинити несанкціонований доступ. покупки та крадіжка особистих даних;

– підслуховування – використовуючи пасивні атаки, хакери можуть моніторити комп'ютерні системи, щоб отримати небажану інформацію. Вони використовують програмне забезпечення, таке як сніффер пакетів, який відстежує пакети, що входять та виходять з мережі. Вони використовують цей метод не для того, щоб завдати шкоди системі, а для того, щоб отримати інформацію без ідентифікації. Хакери атакують електронні листи, телефонні дзвінки, перегляд веб-сторінок тощо;

– програми-вимагачі запобігають належному та повноцінному функціонуванню кінцевого пристрою користувача, доки не буде сплачено певну плату. Деякі видають себе за різні організації, такі як правоохоронні органи, щоб «попередити» бізнес про речі, які можуть загрожувати їхньому бізнесу. Це може включати закінчення терміну дії ліцензії або проблеми з інвентаризацією. Після того, як зловмисники захопили системи в заручники, вони вимагають викуп в обмін на розшифрування. Якщо викуп не сплачено, зловмисники можуть продати інформацію або викрити компанію;

– крипто-шкідливе програмне забезпечення – це ще одна форма вимагання грошей. Цей тип шкідливого програмного забезпечення ув'язнює користувачів і шифрує всі файли на пристрої, щоб жоден з них не можна було відкрити. Вартість розблокування Кількість криптошкідливих програм зростає щогодини або щодня. Деякі форми криптошкідливих програм можуть шифрувати всі файли в мережі. Під час шифрування файли «змішуються», щоб їх було неможливо прочитати. Для відновлення потрібен ключ розшифрування. Криптозловмисне програмне забезпечення або програмне забезпечення-вимагач можна знайти

через файли або посилання, через електронні листи, повідомлення тощо. Їх можна завантажити через інші загрози, такі як троянський кінь або інші пристрої експлуатації («Крипто-програми-вимагачі», н.д.);

– вірус – існує два типи вірусів: файловий вірус та безфайловий вірус. Файловий вірус — це шкідливий код, який прикріплюється до файлу та може відтворюватися без взаємодії. Ці віруси мають потужні засоби запобігання виявленню, такі як розділене зараження та мутація. Він вивантажує корисне навантаження (частину переданих даних, яка є фактичним передбачуваним повідомленням) для виконання атаки, і вірус реплікується, вставляючи код в інші файли. Існує два типи файлових вірусів, включаючи віруси прямої дії та резидентні віруси. Безфайловий вірус не прикріплюється до файлу та використовує служби та процеси в операційній системі для... уникати виявлення та здійснювати атаки. Код завантажується безпосередньо в оперативну пам'ять (оперативну пам'ять). Він також може використовувати програми для виконання шкідливого коду. Існує кілька переваг (для зловмисників), які дозволяють вибрати безфайловий вірус порівняно з файловим, зокрема: легкість зараження пристрою, широкий контроль, стійкість, важко виявити та перемогти вірус;

– черв’як – це шкідлива програма, яка використовує комп’ютерну мережу для розмноження. Вона призначена для проникнення в комп’ютер через мережу та використання вразливості в програмі або операційній системі на пристрої. Деякі з них залишають після себе корисне навантаження, яке може заразити та завдати шкоди. Черв’яки можуть виконувати такі дії, як видалення файлів або дозвіл зловмиснику контролювати комп’ютер;

– ботнет – цей тип вразливості дозволяє мережі заражених пристроїв потрапити під контроль зловмисника для здійснення атак. Зловмисник відомий як «пастух ботів». «Пастух ботів» керує ботами для автоматизації масових атак, включаючи крадіжку даних, збої серверів та розповсюдження шкідливого програмного забезпечення. Ця загроза дозволяє пристроям обманювати інших та спричиняти збої без його згоди. Мотивом більшості цих атак є просто бажання вкрасти щось цінне або спричинити проблеми;

– шпигунське програмне забезпечення – це програмне забезпечення для відстеження, яке розгортається без згоди користувача. Ця діяльність робить користувачів вразливими до порушень даних та зловживає приватними даними. Воно також уповільнює діяльність користувача. Шпигунське програмне забезпечення може збирати такі дані, як облікові дані для входу, PIN-коди облікових записів, номери кредитних карток, звички перегляду тощо. Різні форми шпигунського програмного забезпечення включають троянські програми, рекламне програмне забезпечення, відстеження файлів *cookie* та моніторинг системи для збору конфіденційних даних;

– потенційно небажана програма – це програмне забезпечення, яке користувачі не хочуть бачити на своєму комп’ютері. Це може включати рекламу, панелі інструментів та спливаючі вікна, які завантажуються разом із встановленим програмним забезпеченням;

– комп’ютерний троянець – це програма, замаскована під легітимне програмне забезпечення, яка також виконує шкідливі дії. Користувачів обманом змушують запустити трояна на своїх пристроях за допомогою соціальної інженерії. Після встановлення троянець може шпигувати за вами, красти інформацію та отримувати прихований доступ до ваших пристроїв;

– троянець віддаленого доступу – має ідентичні функції, як і троянець, але відрізняється тим, що надає загрозі несанкціонований віддалений доступ до комп’ютера жертви за допомогою налаштованих протоколів зв’язку. Це дозволяє отримати доступ до комп’ютера жертви та надати загрозі необмежений доступ;

– бекдор – ця загроза надає доступ до комп'ютера, програми або служби, яка обходить будь-які звичайні засоби захисту та отримує високий рівень доступу користувача. Бекдори можуть бути використані для крадіжки особистої та фінансової інформації, встановлення шкідливого програмного забезпечення та захоплення пристроїв;

– логічна бомба – це комп'ютерний код, який додається до легітимної програми, але залишається в стані спокою та уникає виявлення, доки певна подія

не спрацює. Вона активується в гарячій мережі та повинна відповідати певним умовам для атаки;

– руткіт – це атака, яка може приховати свою присутність та присутність іншого шкідливого програмного забезпечення на комп'ютері. Він отримує доступ до нижнього рівня операційної системи, щоб вносити зміни. Це дозволяє комусь отримати контроль над пристроєм без відома користувача. Після встановлення руткіт може виконувати файли та змінювати конфігурацію пристрою на хості. Він також може реєструвати файли та шпигувати за використанням користувача;

– *SQL*-ін'єкція – атака з використанням *SQL*-ін'єкції (*Structured Query Language*) вставляє оператор для маніпулювання сервером бази даних. Одна з найпоширеніших атак типу ін'єкція (SQL-ін'єкція) вставляє оператори для маніпулювання сервером бази даних. Успішна атака може зчитувати конфіденційні дані з бази даних та змінювати інформацію;

– атака переповнення буфера відбувається, коли процес намагається зберегти інформацію в оперативній пам'яті (*RAM*) за межами буфера фіксованої довжини. Додаткові дані переповнюються в області пам'яті, що прилягають до оперативної пам'яті. Зловмисник може скористатися цією загрозою, перезаписавши пам'ять програми, що змінює шлях виконання програми та пошкоджує файли або розкриває інформацію.

Отже, розмах та розмаїття нападів на *IoT*-пристрої вказують на серйозну небезпеку. Їхні наслідки можуть коливатися від простої втрати зв’язку до повної компрометації особистих даних, або навіть загрози життю у надважливих сферах, як-от медицина чи промисловість.

Серед основних наслідків реалізації атак слід виділити:

1. Зловмисне проникнення через слабку автентифікацію. Чимало *IoT*-пристроїв постачаються з типовими логінами та паролями (на кшталт *admin/admin*), які користувачі часто не змінюють. Через це зловмисники можуть без зусиль під'єднатися до пристрою та здобути цілковитий контроль. Особливо небезпечно, коли йдеться про системи відеонагляду, "розумні" двері чи медичне

обладнання. Деякі пристрої навіть не мають функціоналу для зміни облікових даних, що робить їх вразливими на фундаментальному рівні. Атаки *brute force* або *credential stuffing* широко використовуються у подібних випадках [34].

2. Використання *IoT*-пристроїв у ботнетах. *IoT*-пристрої, уражені шкідливим ПЗ, можуть бути застосовані у ботнетах для проведення масштабних атак. Один з найбільш відомих прикладів — ботнет *Mirai*, який у 2016 році вивів з ладу великі частини інтернету, атакуючи DNS-провайдера Dyn. Зловмисники сканували мережу на предмет пристроїв з відкритими портами та ненадійними паролями, після чого заражали їх. Після інфікування пристрої отримували команди з централізованого серверу управління. Згодом з'явились модифікації — *Dark Mirai*, *Mozi*, які значно ускладнили виявлення ботів.

3. Витік секретної інформації. *IoT*-системи збирають відомості про користувачів, як-от температуру у помешканні, показники здоров'я або пересування. Коли ці дані не зашифровані чи зберігаються на серверах з невисоким рівнем безпеки, їх можуть перехопити або викрасти. Приклад: у 2018 році компанія *Strava* випадково оприлюднила місця розташування військових баз через відкриті геолокаційні дані фітнес-браслетів, що стало причиною міжнародного скандалу. Такі випадки показують, що навіть без злих намірів дані можуть бути використані небезпечно.

4. Найбільшу загрозу становлять напади, націлені на конфіденційність даних. Системи інтернету речей (*IoT*) нерідко оперують медичними відомостями, інформацією про приватне життя чи геолокаційними даними, що мають суто персональний характер. Якщо їх скомпрометують, це може призвести до юридичних проблем для компаній та особистих ризиків для користувачів.

5. Також важливо пам'ятати про фізичні загрози. Значна частина пристроїв Інтернету речей розміщена у відкритому просторі, де зловмисник може фізично взаємодіяти з обладнанням, наприклад, перепрошити його, вилучити ключі шифрування або інші важливі дані. Це відкриває шлях для подальшого проникнення в мережу.

3 АНАЛІЗ РІШЕННЬ БЕЗПЕКИ СИСТЕМ ІНТЕРНЕТ РЕЧЕЙ

3.1 Організаційні рішення

Забезпечення безпеки систем Інтернету речей вимагає комплексного підходу, що охоплює як технічні аспекти, так і надійну організаційну структуру, управління доступом, політику захисту даних та чітке інституційне регулювання. Саме організаційні заходи є фундаментом для побудови безпечного середовища функціонування *IoT*, відіграючи ключову роль у реалізації всебічного підходу до кіберзахисту [20].

Насамперед, надзвичайно важливо розробити внутрішню політику безпеки, що регламентує використання *IoT*-пристроїв, процедури обробки даних, автентифікації, шифрування, ведення журналів подій та управління інцидентами. Успішні організації формулюють конкретні вимоги до впровадження *IoT*-рішень, включаючи обов'язкові сертифікаційні процедури для пристроїв, забезпечення своєчасного оновлення прошивки та ізоляцію критичних компонентів в мережевій інфраструктурі.

Керування життєвим циклом *IoT*-пристроїв – ще один наріжний камінь для організації. Цей процес не обмежується лише закупівлею та введенням в експлуатацію пристроїв, а й передбачає їхню інвентаризацію, контроль за конфігураціями, регулярну оцінку безпеки, а також відповідне вилучення або оновлення пристроїв після закінчення терміну служби. Ігнорування цього етапу часто обертається тим, що застарілі або неактуальні пристрої перетворюються на слабку ланку в обороні всієї системи.

Необхідно також розробити систему розподілу пристроїв та інформації за категоріями. Це дозволить виокремити критично важливі ресурси Інтернету речей від тих, що мають менше значення, а отже, правильно встановити рівень захисту для кожної категорії. Критичні пристрої, наприклад, медичне устаткування чи енергетичні системи, слід розміщувати в ізольованих сегментах мережі з використанням багатошарового контролю доступу.

Іншим важливим аспектом організаційного рівня є підготовка персоналу. Співробітники, які працюють з системами Інтернету речей, повинні мати базові знання з кібербезпеки, володіти інформацією про порядок дій при виявленні інцидентів, процедури оновлення пристроїв та правил роботи з конфіденційною інформацією. У багатьох випадках саме людський фактор стає причиною серйозних витоків чи порушень, яких можна було б уникнути, якби персонал мав необхідні знання.

Вагоме значення має і безпековий аудит, котрий варто проводити як періодично, так і в процесі інтеграції нових *IoT*-платформ. Це дає змогу знаходити слабкі місця ще до їх можливого використання зловмисником. Аудит може виконуватися як внутрішніми командами з безпеки, так і сторонніми сертифікаційними організаціями.

Особливої уваги потребує формалізація взаємодії з зовнішніми постачальниками, які постачають *IoT*-пристрої або суміжні послуги. В організаційних договорах необхідно чітко визначити вимоги до безпеки, обов'язковість оновлень, забезпечення захисту каналу передачі даних та можливість проведення перевірок.

На міжнародному рівні організаційні аспекти безпеки *IoT* регулюються відповідними стандартами, зокрема *ISO/IEC* 27001 (система управління інформаційною безпекою) та *ISO/IEC* 30141 (еталонна архітектура *IoT*), що задають структуру для створення політик безпеки, оцінювання ризиків і безперервного вдосконалення систем захисту.

3.2 Технічні рішення

Технічні засоби у галузі охорони систем Інтернету речей відіграють визначальну роль у гарантуванні таємності, цілісності й доступності даних. Враховуючи велику кількість пристроїв, обмеженість їхніх обчислювальних можливостей, а також високий рівень розподіленості, підхід до захисту *IoT* має бути всебічним і багаторівневим [21].

Одним з ключових технічних напрямків є впровадження інструментів аутентифікації та контролю доступу. Використання слабких або встановлених за замовчуванням паролів є однією з найпоширеніших вразливостей *IoT*. Щоб зменшити ризики, використовуються сучасні методи аутентифікації, зокрема протоколи з двофакторною перевіркою, цифрові сертифікати та механізми авторизації на основі ролей (*RBAC*), які забезпечують контроль за тим, хто саме має доступ до певного пристрою чи сервісу.

Ще одним надзвичайно важливим елементом є безпечна передача даних. Зважаючи на те, що більшість *IoT*-пристроїв взаємодіє через відкриті канали зв'язку (*Wi-Fi, Bluetooth, Zigbee, LoRa* та інші), шифрування трафіку стає вкрай необхідним заходом. Для цього застосовуються полегшені криптографічні протоколи, які пристосовані до обмежених ресурсів пристроїв. Зокрема, це *TLS/DTLS, ECC* (еліптична криптографія), або симетричне шифрування (*AES*-128), що гарантують захист інформації, яка передається, навіть у нестабільних або недостатньо захищених мережевих умовах.

Окрему царину технічних рішень формує реалізація безпечного оновлення програмного забезпечення. Прошивки *IoT*-пристроїв потребують систематичного оновлення задля усунення вразливостей. Ключовим завданням є перевірка цифрових підписів оновлень, аби запобігти впровадженню шкідливого ПЗ. Сучасні системи оновлення базуються на *OTA* (*over-the-air*) технологіях з криптографічною аутентифікацією джерела.

До ключових технічних заходів також варто віднести засоби виявлення вторгнень (*IDS/IPS*), адаптовані до *IoT*. Через специфіку трафіку, незначні обсяги даних та особливу поведінку пристроїв, традиційні *IDS/IPS* можуть виявлятися не надто ефективними. З цієї причини дедалі частіше використовуються системи виявлення аномалій, розроблені на основі машинного навчання, що здатні розпізнавати нетипову активність пристроїв чи спроби їх компрометації у режимі реального часу.

Ще один стратегічний крок – сегментація мережі. *IoT*-системи нерідко інтегруються в загальну інформаційно-технологічну інфраструктуру компанії,

що може становити загрозу для всієї мережі. Для пом'якшення таких ризиків практикується поділ мережі на ізольовані сегменти (наприклад, за допомогою *VLAN*), які обмежують розповсюдження потенційних загроз. Надзвичайно ефективним вважається підхід «нульової довіри», котрий передбачає суворий контроль над усіма пристроями, незалежно від їхнього місця розташування в мережі.

Насамкінець, ключовим є інтегрування *IoT* з хмарними платформами, що дають змогу централізовано контролювати безпеку пристроїв, реєструвати події, створювати резервні копії конфігурацій та гарантувати реагування на інциденти. Водночас хмарні сервіси повинні відповідати міжнародним нормам безпеки даних, як-от *ISO/IEC* 27017 та *ISO/IEC* 27018.

З огляду на комплексну природу *IoT*, ефективний захист можливий винятково за умови комбінування декількох технічних рішень, пристосованих до особливостей кожної системи. Такі рішення мають бути масштабованими, фінансово виправданими та включеними у загальну архітектуру безпеки установи.

3.3 Програмні рішення

Програмні рішення у сфері забезпечення безпеки Інтернету речей мають вирішальне значення, оскільки саме програмний код визначає функціональність пристроїв, принципи їхньої взаємодії та спосіб опрацювання інформації. На відміну від технічних або організаційних підходів, програмні засоби втілюються у прошивках, програмному забезпеченні пристроїв, шлюзів та хмарних платформах, що забезпечує пристосованість, варіативність і здатність до розширення методів кіберзахисту [22].

Одним з ключових аспектів є використання полегшених та спеціалізованих операційних систем для *IoT*, на зразок *Contiki, RIOT* або *TinyOS*, розроблених з урахуванням обмежених можливостей пристроїв. Ці

ОС надають базові інструменти ізоляції процесів, безпечної роботи з пам’яттю та мережевими протоколами. Додатково, вони часто містять попередньо встановлені механізми шифрування, аутентифікації та оновлення прошивки.

Важливу роль відіграють бібліотеки програмного забезпечення, які втілюють у життя захищені протоколи обміну даними. Наприклад, реалізації *MQTT* із захистом *TLS*, бібліотеки для роботи з *CoAP* з підтримкою *DTLS*, а також готові модулі для взаємодії з *JSON Web Tokens* (*JWT*) дозволяють проводити шифрування, автентифікацію та керування доступом без створення надлишкового навантаження на пристрої.

Програмні рішення охоплюють і централізовані системи безпеки, які існують як хмарні сервіси (*PaaS, SaaS*). Платформи на кшталт *AWS IoT Core, Azure IoT Hub* або *Google Cloud IoT* реалізують моніторинг пристроїв, ведення журналів подій, автоматичне оновлення програмного забезпечення, застосування політик доступу та інтеграцію з *SIEM*-системами (*Security Information and Event Management*). Вони також надають можливість масштабовано впроваджувати контроль безпеки на всіх етапах життєвого циклу пристрою — від етапу виробництва до списання.

До того ж, надзвичайно важливою є роль механізмів виявлення та реагування на аномалії, втілених на програмному рівні. Сучасні бібліотеки штучного інтелекту, інтегровані в *IoT*-шлюзи або хмарні платформи, дають змогу автоматично аналізувати трафік, знаходити відхилення у поведінці пристроїв та оперативно реагувати на можливі небезпеки. Скажімо, алгоритми класифікації чи кластеризації можуть виявити спробу проникнення ще до її реалізації, співставляючи її з типовими зразками активності.

Не менш значущим програмним компонентом є система безпечного оновлення прошивки. Зокрема, використовуються криптографічні підписи оновлень, що перевіряють справжність джерела, та контроль хеш-сум для переконання у цілісності даних. Програмна реалізація механізмів *OTA* дає змогу

автоматично оновлювати пристрої в розподіленому середовищі, зводячи до мінімуму вплив людського фактора та гарантуючи актуальний рівень захисту.

Ще одним вагомим класом є відкриті програмні рішення (*open-source*). Вони надають можливість адаптувати безпекові механізми з урахуванням специфіки конкретного оточення. Наприклад, такі проєкти, як *Zephyr*, *Eclipse IoT* та *OpenHAB*, містять у собі модулі безпеки, підтримку протоколів із застосуванням шифрування, інтеграцію з сервісами аутентифікації, а також гнучкий API, котрий дозволяє розширювати функціонал.

Програмне забезпечення, зокрема відкрите, має важливе значення з точки зору прозорості. Це дозволяє фахівцям у сфері кібербезпеки проводити аудит, виявляти вразливості, оперативно виправляти помилки та контролювати процеси шифрування. У закритих комерційних рішеннях така можливість відсутня.

Підсумовуючи, програмні засоби захисту для *IoT* не просто доповнюють апаратні та організаційні заходи. Вони є фундаментом для автоматизованого управління безпекою, своєчасного виявлення загроз та захисту критичної інфраструктури в умовах прискореного розвитку цифрових технологій.

4 МОДЕЛЮВАННЯ ЗАГРОЗ ІНТЕРНЕТУ РЕЧЕЙ

4.1 Основи побудови моделей загроз для Інтернет речей

Моделювання загроз – це процес аналізу та створення віртуальних моделей можливих загроз і ризиків для різних сфер життя. Такий підхід дозволяє оцінювати потенційні небезпеки та розробляти стратегії їх запобігання та управління. Моделювання загроз є важливим для багатьох галузей, включаючи кібербезпеку, екологічну, фінансову та громадську безпеку. Воно дозволяє прогнозувати можливі наслідки небезпеки та вживати відповідних заходів для її управління. Такий підхід вимагає використання спеціалізованих програмних засобів, статистичного аналізу та інших методів, які допомагають створювати точні та надійні моделі загроз. Моделювання загроз є важливим кроком у процесі розробки стратегій безпеки та управління ризиками. Розуміння та запобігання загрозам є критично важливими завданнями для забезпечення безпеки та стійкості в різних сферах діяльності.

Моделювання загроз передбачає використання різних методів і технологій для створення реалістичних сценаріїв подій, які можуть призвести до загрози або негативного впливу. Це дозволяє оцінити ймовірність та наслідки таких подій, що важливо для прийняття раціональних та обґрунтованих рішень. Моделювання загроз також використовується для дослідження різних варіантів реагування на загрози та вибору найкращих стратегій захисту.

Воно допомагає визначити, які заходи можуть бути найефективнішими та економічно вигідними. Одним з важливих аспектів моделювання загроз є оновлення та корекція моделей на основі нової інформації та аналізу змін у середовищі. Завдяки цьому організації можуть підтримувати своє захисне обладнання та процедури в актуальному стані. Загрози у світі Інтернету речей особливо актуальні в сучасному цифровому світі, де все більше пристроїв підключаються до мережі. Моделювання таких загроз допомагає покращити безпеку підключених пристроїв та забезпечити їх захист від потенційних атак.

Тому моделювання загроз є важливим інструментом для запобігання та управління ризиками в різних галузях промисловості та допомагає забезпечити стабільність і безпеку в цифровому світі.

Під час створення моделей загроз для пристроїв Інтернету речей ви, ймовірно, зіткнетеся з низкою поширених проблем. Причина полягає в тому, що світ Інтернету речей складається переважно з систем з низькою обчислювальною потужністю, енергоспоживанням, пам'яттю та дисковим простором, які розгортаються в незахищених мережевих середовищах. Багато виробників обладнання усвідомили, що вони можуть легко перетворити будь-яку недорогу платформу, таку як телефон або планшет *Android*, *Raspberry Pi* або плата *Arduino*, на складний пристрій Інтернету речей.

Так багато пристроїв Інтернету речей насправді працюють під керуванням *Android* або поширених дистрибутивів *Linux* – тих самих операційних систем, які встановлені на мільярдах телефонів, планшетів, годинників і телевізорів. Ці ОС добре відомі та часто надають більше функцій, ніж потрібно пристрою, що збільшує можливості зловмисника. Гірше того, розробники Інтернету речей розширюють операційні системи, впроваджуючи власні програми, яким бракує належних заходів безпеки! Крім того, щоб забезпечити функціонування пристрою, розробникам часто доводиться обходити оригінальні засоби захисту операційної системи. Інші пристрої Інтернету речей, що базуються на операційній системі реального часу (*RTOS*), мінімізують час обробки, відмовляючись від стандартів безпеки більш просунутих платформ.

Крім того, електроніка такого роду зазвичай не оснащена антивірусом або антивірусним програмним забезпеченням. Її мінімалістичний дизайн, відточений для зручності використання, не враховує загальні заходи безпеки, такі як білий список програмного забезпечення, який дозволяє встановлювати на пристрій лише певне програмне забезпечення, або рішення для контролю доступу до мережі *Network Access Control* (*NAC*) для забезпечення дотримання політик безпеки мережі, що регулюють доступ користувачів і пристроїв. Багато постачальників припиняють пропонувати оновлення безпеки невдовзі після

першого випуску продукту. Крім того, деякі компанії укладають контракти з представниками брендів, які беруть на себе розповсюдження продуктів сторонніх виробників, а потім ті самі пристрої виходять на ринок через різні канали під різними брендами та логотипами, що ускладнює оновлення системи безпеки та програмного забезпечення кожного з них.

Ці обмеження змушують багато інтернет-пристроїв використовувати власні або менш відомі протоколи, які не відповідають стандартам безпеки. Це часто перешкоджає використанню складних методів посилення захисту, таких як моніторинг цілісності програмного забезпечення, який виявляє втручання, або атестація пристрою – тестування за допомогою спеціалізованого обладнання, яке гарантує надійність тестованого пристрою.

Найпростіший спосіб моделювання загроз в оцінці безпеки – це використання моделі класифікації загроз *STRIDE*, яка зосереджена на виявленні вразливостей у технологіях, а не на вразливих активах чи потенційних зловмисниках. Розроблена Праріт Гарг та Лорен Конфельдер у *Microsoft*, *STRIDE* є однією з найпопулярніших систем класифікації загроз.

Ця абревіатура означає такі загрози:

– спуфінг (підміна, підміна) – обхід системи контролю доступу шляхом маскування під іншу систему;

– фальсифікація – суб’єкт порушує цілісність системи або даних;

– заперечення (приховування) – користувач може приховати, що він виконав певні дії в системі;

– розкриття інформації (витік інформації) – порушення конфіденційності даних у системі (відбувається витік даних, перехоплення);

– відмова в обслуговуванні (*DoS*, атака «відмова в обслуговуванні») – зловмисник створює умови, за яких легальні користувачі системи не можуть отримати доступ до її ресурсів;

– підвищення привілеїв – користувач, який має лише обмежений доступ до системи, може самостійно розширити можливості доступу.

STRIDE включає три кроки: визначення архітектури, її розбиття на компоненти та виявлення загроз для кожного компонента.

4.2 Опис об’єкту моделювання

4.2.1 Компоненти системи

На рисунку 4.1 показано архітектуру інтелектуальної системи сонячної енергії, підкреслюючи інтеграцію пристроїв Інтернету речей, протоколів зв'язку та хмарних сервісів. Архітектура системи була розділена на чотири рівні, кожен з яких підтримує моніторинг, керування та оптимізацію в режимі реального часу для забезпечення масштабованості та функціональності.

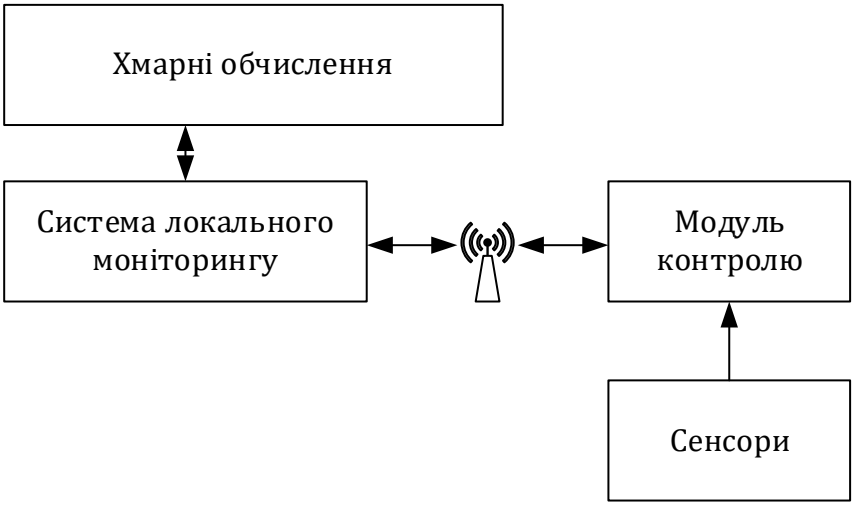

Рисунок 4.1 – Архітектура системи інтелектуальної сонячної енергетики на основі Інтернету речей

Фізичний рівень складається з фотоелектричних модулів та датчиків, які контролюють ключові змінні, такі як температура, вологість та напруга, що генеруються фотоелектричною панеллю;

Рівень вузла Інтернету речей використовує модуль контролю для збору та обробки даних датчиків у режимі реального часу, виконуючи локалізоване

керування для оцінки вироблення енергії на основі умов навколишнього середовища;

Комунікаційний рівень слугує мостом між польовими операціями та хмарною аналітикою. Шлюз Інтернету речей сприяє локальному моніторингу та контролю, одночасно передаючи дані в хмару для подальшого аналізу;

Хмарний рівень обробляє, зберігає та візуалізує дані. Система аналізує дані на наявність аномалій та оптимізації, зберігає їх як у теплому, так і в холодному сховищі, а також надає аналітичні дані через зручні панелі інструментів.

Архітектура системи включає два окремі потоки отримання даних, які разом називаються потоковою передачею, що служать різним цілям та розширюють функціональність системи. Перший потік призначений для аналізу та візуалізації даних у режимі реального часу, що сприяє операційній аналітиці.

Другий потік зосереджений на маршрутизації даних. Окрема група споживачів створюється для керування цим потоком даних, забезпечуючи належну обробку даних, призначених для зберігання — холодного сховища для довгострокового архівування та теплого сховища для прямих запитів *TSI*. *TSI* отримує вхідні дані з системи локального моніторингу та обробляє їх, надаючи детальний огляд продуктивності системи з плином часу.

Щоб краще зрозуміти архітектуру інтелектуальної сонячної енергетики на основі Інтернету речей та її роботу, систему було розділено на ключові функціональні компоненти. Кожен компонент відіграє вирішальну роль у забезпеченні ефективної роботи системи та її цільового призначення. Основні компоненти такі:

– датчики та фотоелектричні модулі: ці пристрої є відправною точкою системи, збираючи важливі дані, такі як напруга, струм, виробництво енергії та фактори навколишнього середовища, такі як температура та сонячне світло. Ця інформація в режимі реального часу є основою для моніторингу та управління продуктивністю сонячної енергетичної системи;

– вузли Інтернету речей (модуль контролю): в основі локальної обробки вузол Інтернету речей збирає та обробляє дані з датчиків. Він дозволяє

здійснювати пряме налаштування системи, таке як точне налаштування операцій, для підтримки оптимальної продуктивності;

– шлюзи Інтернету речей: ці шлюзи діють як міст між локальною системою та хмарою. Вони забезпечують безпечну та безперебійну передачу даних з вузлів Інтернету речей до хмарних сервісів, де їх можна додатково обробляти та зберігати. Крім того, на цьому рівні можна локально контролювати систему;

– хмарні сервіси: хмара слугує мозком системи, займаючись зберіганням даних, аналітикою та візуалізацією. Вона дозволяє отримувати аналітику в режимі реального часу та довгостроковий аналіз тенденцій, допомагаючи зацікавленим сторонам приймати рішення на основі даних щодо роботи та продуктивності системи;

– віддалені інтерфейси користувача: ці інтерфейси є точкою взаємодії для кінцевих користувачів та адміністраторів, надаючи доступ до моніторингу продуктивності системи та видачі команд керування за потреби. Вони надають аналітику в режимі реального часу та корисні дані через інтуїтивно зрозумілі панелі інструментів, тим самим забезпечуючи ефективність та чутливість системи.

Зона локального користувача, зона хмарних сервісів та зона віддаленого користувача взаємопов'язані через безперервний потік даних та команд керування. Дані, що генеруються датчиками та вузлами Інтернету речей у зоні локального користувача, передаються до зони хмарних сервісів для зберігання, аналізу та візуалізації. Потім віддалені користувачі отримують доступ до цих даних через хмарні панелі керування, що дозволяє здійснювати моніторинг та керування в режимі реального часу. Однак ця взаємозалежність створює значні ризики. Наприклад, порушення в зоні хмарних сервісів може дозволити зловмисникам маніпулювати даними, що надсилаються віддаленим користувачам, що призводить до неправильних налаштувань системи або навіть повного вимкнення системи. Аналогічно, скомпрометований пристрій віддаленого користувача може бути використаний для введення шкідливих команд у хмару, які потім можуть поширитися на зону локального користувача,

порушуючи фізичні операції. Розбиття системи на ці компоненти забезпечує чітке та структуроване уявлення про те, як кожен компонент сприяє її функціональності. Це розуміння закладає основу для подальшого аналізу.

4.2.2 Аналіз потоків даних

На початку роботи датчики, підключені до фотоелектричних модулів, збирають робочі дані в режимі реального часу, такі як напруга, струм і температура. Ці дані надсилаються до вузла Інтернету речей (модуль контролю), який обробляє показники та готує їх для подальшого використання. Вузол Інтернету речей також відіграє певну роль у реагуванні на команди керування. Наприклад, локальний користувач може надіслати команду для повторного калібрування датчиків або налаштування параметрів системи для оптимізації енергетичної продуктивності.

Потім дані пересилаються до польового шлюзу Інтернету речей, який служить мостом між локальною системою та хмарою. Польовий шлюз передає оброблені дані до хмарного шлюзу Інтернету речей, що є ключовим компонентом, що забезпечує надійний зв'язок з хмарною інфраструктурою. Цей крок є важливим для передачі даних та підтримки зв'язку між різними частинами системи.

Після розміщення в хмарній інфраструктурі дані зберігаються в хмарному сховищі. Сховища класифікуються наступним чином:

– холодне зберігання: використовується для архівування історичних даних, які пізніше можна проаналізувати на предмет тенденцій або оптимізації системи;

– тепле сховище: дозволяє здійснювати прямі запити та аналіз у режимі реального часу, що забезпечує негайний моніторинг та швидке виявлення несправностей.

Хмарні додатки аналізують дані як у реальному часі, так і в історичних даних, щоб визначити тенденції продуктивності, виявити несправності та створити аналітичні висновки. Результати цього аналізу представлені на інтерактивних інформаційних панелях, що робить інформацію доступною для користувачів для прийняття рішень.

Ці інформаційні панелі дозволяють користувачам ефективно взаємодіяти із системою; віддалений користувач може проаналізувати інформаційну панель та виявити критичну проблему, таку як незвичайна вихідна енергія.

Щоб запобігти подальшим пошкодженням, користувач може надіслати команду через хмару, щоб вимкнути систему або налаштувати робочі параметри. Аналогічно, локальний користувач може отримати доступ до даних про продуктивність у реальному часі та видавати команди керування через польовий шлюз Інтернету речей. Наприклад, користувач може скинути налаштування компонентів або налаштувати енергетичне навантаження, щоб відновити ефективність системи.

Двосторонній потік даних та команд керування забезпечує швидку реакцію, ефективність та адаптивність системи. Дозволяючи як локальним, так і віддаленим користувачам контролювати продуктивність у режимі реального часу, виявляти аномалії та негайно вживати заходів, система досягає високого ступеня гнучкості та надійності.

Систему класифіковано на три зони: зону локального користувача, зону хмарних сервісів та зону віддаленого користувача. Ця класифікація не лише впорядковує потік даних, але й допомагає систематично виявляти потенційні загрози та ризики в кожній зоні. Аналізуючи ці зони окремо, стає легше точно визначити вразливості, характерні для локальних операцій, хмарної інфраструктури та віддаленої взаємодії, забезпечуючи комплексну оцінку ризиків безпеки в усій системі.

4.3 Аналіз загроз та оцінка ризиків для локальних зон використання

4.3.1 . Аналіз загроз та оцінка ризиків локальної зони користувача

Аналіз моделі загроз *STRIDE* (табл. 4.1) визначає критичні ризики безпеки в зоні локального користувача інтелектуальної системи сонячної енергії, що охоплює такі компоненти, як датчики, вузол Інтернету речей, локальні користувачі та польовий шлюз Інтернету речей.

Таблиця 4.1 – Аналіз загроз STRIDE для локальної зони користувача.

Категорія загрози	Потік компонентів/комунікації	Виявлена загроза	Супутній ризик
Спуфінг (*S*)	Датчики до вузла Інтернету речей	Імітація датчика	Неправильні дані призводять до неналежної роботи системи, що може призвести до пошкодження.
Спуфінг (*S*)	Шлюз локального користувача до польового Інтернету речей	Зловмисник видає себе за законного користувача	Несанкціонований доступ може змінити налаштування системи.
Фальсифікація (*T*)	Вузол Інтернету речей до польового шлюзу Інтернету речей	Зміна даних під час передачі	Маніпулювання даними впливає на рішення щодо управління енергією.
Фальсифікація (*T*)	Датчики	Фізичне маніпулювання датчиками	Хибні показники порушують роботу системи.
Заперечення (*R*)	Від локального користувача до вузла Інтернету речей	Заперечення відповідальності за зміни в системі	Відсутність відповідальності перешкоджає вирішенню проблеми.
Розкриття інформації (*I*)	Вузол Інтернету речей	Розкриття конфіденційних системних даних	Витік даних викриває вразливості системи.
Розкриття інформації (*I*)	Датчики до вузла Інтернету речей	Перехоплення даних під час передачі	Скомпрометовані дані розкривають важливу інформацію.
Відмова в обслуговуванні (*D*)	Польовий шлюз Інтернету речей	Перевантаження шлюзу надмірною кількістю запитів	Порушення зв'язку впливає на керування системою.
Підвищення привілеїв (*E*)	Локальний користувач	Несанкціоноване підвищення прав користувача	Несанкціонований доступ дозволяє вносити шкідливі зміни.

Ризики підміни виявляються, коли зловмисники видають себе за легітимних датчиків або користувачів, потенційно вводячи неправдиві дані або вносячи несанкціоновані зміни. Фальсифікація створює загрозу, змінюючи дані під час передачі між вузлом Інтернету речей та польовим шлюзом Інтернету речей, що призводить до неправильної поведінки системи. Ризики відмови виникають через те, що локальні користувачі заперечують відповідальність за зміни в системі, ускладнюючи реагування на інциденти та підзвітність. Вразливості розкриття інформації розкривають конфіденційні операційні дані

під час передачі, тим самим збільшуючи ймовірність подальшого використання. *DoS*-атаки можуть перевантажити критичні компоненти, такі як вузол та шлюз Інтернету речей, порушуючи доступність системи та перешкоджаючи роботі в режимі реального часу. Нарешті, загрози підвищення привілеїв дозволяють неавторизованим користувачам отримати адміністративний доступ, що призводить до шкідливих модифікацій системи.

Для подальшого визначення пріоритетів цих загроз та забезпечення кількісної основи для прийняття рішень було застосовано систему оцінки ризиків *DREAD*. *DREAD* оцінює кожну загрозу на основі п'яти ключових категорій: потенціал пошкодження, відтворюваність, ймовірність використання, уражені користувачі та можливість виявлення. Результати цієї оцінки представлені в таблиці 4.2 .

Таблиця 4.2 – Оцінка ризику для локальної зони користувача.

Категорія загрози	Конкретна загроза	Пошкодження	Відтворюваність	Експлуатаційніс	Постраждалі	Видимість	Оцінка ризику	Рівень ризику
Спуфінг (*S*)	Імітація датчика	3	2	2	3	3	2.6	Високий
Спуфінг (*S*)	Зловмисник видає себе за законного користувача	3	2	2	3	2	2.4	Середній
Фальсифікація (*T*)	Зміна даних під час передачі	3	3	2	3	2	2.6	Високий
Фальсифікація (*T*)	Фізичне маніпулювання датчиками	3	2	2	3	2	2.4	Середній
Заперечення (*R*)	Заперечення відповідальності за зміни	2	2	1	2	2	1.8	Середній
Розкриття інформації (*I*)	Розкриття конфіденційних системних даних	3	2	2	3	3	2.6	Високий
Розкриття інформації (*I*)	Перехоплення даних під час передачі	3	2	2	3	3	2.6	Високий
Відмова в обслуговуванні (*D*)	Перевантаження шлюзу запитами	3	3	3	3	2	2.8	Високий
Підвищення привілеїв (*E*)	Несанкціоноване підвищення прав користувача	3	2	2	3	2	2.4	Середній

Оцінка ризику *DREAD* показує, що кілька загроз у локальній зоні користувача становлять високий ризик, з оцінками ризику від 2,6 до 2,8.

Наприклад, імперсонація датчика отримала оцінку ризику 2,6, що відображає її потенціал завдати значної шкоди через неправильне введення даних, її помірну відтворюваність та високу видимість. Аналогічно, перевантаження шлюзу надмірними запитами (конкретний випадок відмови в обслуговуванні) отримало оцінку 2,8, найвищу оцінку ризику в локальній зоні користувача. Ця загроза створює серйозну загрозу для доступності системи, оскільки може порушити зв'язок між критичними компонентами, зробивши систему невідповідною. Інші загрози високого ризику включають зміну даних під час передачі та розкриття конфіденційних системних даних, обидва показники мають оцінку 2,6.

На противагу цьому, такі загрози, як зловмисник, який видає себе за законного користувача, фізичне маніпулювання датчиками та несанкціоноване підвищення прав користувача, були класифіковані як Середній ризик (оцінка: 2,4), оскільки вони вимагають більше зусиль для використання або мають менший вплив. Відмова від доступу також була класифікована як Середній ризик (оцінка: 1,8), оскільки вона в першу чергу впливає на підзвітність, а не на функціональність системи.

4.3.2 Аналіз загроз та оцінка ризиків зони хмарних сервісів у інтелектуальних системах сонячної енергії

Зона хмарних сервісів є важливою частиною інтелектуальної системи сонячної енергії, яка керує потоком, зберіганням та аналізом даних з пристроїв Інтернету речей у локальній зоні користувача. Ця зона включає важливі компоненти, такі як хмарний шлюз Інтернету речей, хмарне сховище, аналітику потоків та панелі інструментів для взаємодії з користувачем та керування системою. Аналіз загроз на основі STRIDE, наведений у таблиці 4.3, висвітлює ключові вразливості та пов'язані з ними ризики в цій зоні.

Спуфінг становить значний ризик, оскільки зловмисники можуть видавати себе за хмарний шлюз Інтернету речей або віддалених користувачів, вводячи неправдиві дані в хмару. Це може призвести до неправильної аналітики та неправильної конфігурації системи, що зрештою впливає на продуктивність та надійність системи.

Таблиця 4.3 – Аналіз загроз *STRIDE* для зони хмарних сервісів.

Категорія загрози	Потік компонентів/комунікації	Виявлені загрози	Супутній ризик
Спуфінг (*S*)	Від польового шлюзу Інтернету речей до хмарного шлюзу	Зловмисник може видати себе за польовий шлюз Інтернету речей	Неперевірені пристрої можуть надсилати неправдиві дані, що призводить до неточної аналітики або неправильних конфігурацій.
Фальсифікація (*T*)	Потік даних від польового шлюзу Інтернету речей до хмарного шлюзу	Перехоплення або зміна даних під час передачі	Змінені дані можуть призвести до неточних рішень або системних помилок.
Фальсифікація (*T*)	Хмарне сховище	Зміна збережених історичних даних	Зміна збережених даних може призвести до помилкової аналітики та спотворення майбутніх прогнозів.
Розкриття інформації (*I*)	Шлюз польового Інтернету речей до хмарного шлюзу	Розкриття конфіденційних даних під час передачі	Витік даних може виявити слабкі місця системи, що допоможе потенційним зловмисникам.
Розкриття інформації (*I*)	Хмарне сховище	Несанкціонований доступ до даних, що зберігаються в хмарі	Витік даних може бути використаний для запуску більш точних атак.
Відмова в обслуговуванні (*D*)	Аналітика потоку	Перевантаження системи надлишковими даними	Перевантаження може спричинити затримки або збої в аналітиці, що призведе до неефективності системи.
Підвищення привілеїв (*E*)	Доступ до хмарної інформаційної панелі та адміністративного контролю	Зловмисники можуть отримати несанкціонований доступ адміністратора	Отримання вищого рівня доступу може дозволити зловмисникам змінити конфігурації системи або вимикати засоби контролю безпеки.

Втручання під час передачі даних між хмарним шлюзом Інтернету речей та хмарним сховищем є ще однією проблемою, оскільки змінені дані можуть призвести до неправильних рішень, порушуючи як короткострокову роботу, так і довгострокову оптимізацію. Крім того, маніпулювання історичними даними, що зберігаються в хмарі, може поставити під загрозу майбутній системний аналіз та прогнози.

Відмова від відповідальності є ризиком, коли віддалені користувачі отримують доступ до системи через панелі інструментів, оскільки користувачі можуть заперечувати внесення критичних змін без належного відстеження, що ускладнює притягнення їх до відповідальності. Розголошення інформації становить серйозну загрозу, особливо якщо під час передачі відбувається витік конфіденційних операційних даних через погане шифрування, що дає зловмисникам цінну інформацію про вразливості системи.

DoS-атаки, спрямовані на хмарний шлюз Інтернету речей або *Stream Analytics*, можуть перевантажити ці системи, що призведе до затримок або навіть збоїв, що може порушити контроль і моніторинг у режимі реального часу. Нарешті, підвищення прав становить високий ризик, оскільки несанкціонований доступ до адміністративних елементів керування може дозволити зловмисникам вносити шкідливі зміни в систему, ставлячи під загрозу її загальну безпеку та стабільність.

Для подальшої оцінки серйозності цих загроз та оптимізації розподілу ресурсів було використано систему оцінки ризиків. *DREAD* оцінює загрози за п'ятьма ключовими вимірами: потенціал пошкодження, відтворюваність, експлуатаційна спроможність, постраждалі користувачі та можливість виявлення. Результати цієї оцінки зведені в таблиці 4.4.

Таблиця 4.4 Оцінка ризиків для зони хмарних сервісів.

Категорія загрози	Конкретна загроза	Пошкодження	Відтворюваність	Експлуатаційність	Постраждалі	Видимість	Оцінка ризику (середня)	Рівень ризику
Спуфінг (*S*)	Імітація польового шлюзу Інтернету речей	3	2	2	3	3	2.6	Високий
Фальсифікація (*T*)	Перехоплення або зміна даних	3	3	2	3	2	2.6	Високий
Фальсифікація (*T*)	Зміна збережених історичних даних	3	2	2	3	2	2.4	Середній
Розкриття інформації (*I*)	Розкриття конфіденційних даних під час передачі	3	2	2	3	3	2.6	Високий
Розкриття інформації (*I*)	Несанкціонований доступ до даних, що зберігаються в хмарі	3	2	2	3	3	2.6	Високий
Відмова в обслуговуванні (*D*)	Перевантаження системи надлишковими даними	3	3	3	3	2	2.8	Високий
Підвищення привілеїв (*E*)	Несанкціонований доступ адміністратора	3	2	2	3	2	2.4	Середній
Фальсифікація (*T*)	Зміна збережених історичних даних	3	2	2	3	2	2.4	Середній

Результати показують, що більшість загроз у зоні хмарних сервісів відносяться до категорії високого ризику з оцінками від 2,6 до 2,8. Наприклад, загроза уособлення польового шлюзу Інтернету речей отримала оцінку 2,6, що підкреслює її здатність порушувати роботу системи шляхом введення неправдивих даних, її помірну відтворюваність та високу ймовірність бути виявленою зловмисниками. Аналогічно, загроза відмови в обслуговуванні (*DoS*),

спричинена переповненням системи надлишковими даними, мала найвищий бал ризику 2,8, що відображає її потенціал перевантажувати хмарні сервіси, призводячи до затримок або збоїв в обробці даних та загальній функціональності системи. Інші загрози високого ризику включають перехоплення або зміну даних та розкриття конфіденційних даних під час передачі, обидва з яких отримали оцінку 2,6 через їхній значний вплив на цілісність та конфіденційність даних.

І навпаки, такі загрози, як зміна збережених історичних даних та несанкціонований доступ адміністратора, були оцінені як середній ризик, кожна з яких має бал 2,4. Ці загрози все ще становлять значні проблеми безпеки; проте вони вважаються менш критичними, ніж загрози високого ризику, через нижчу ймовірність використання або більш обмежений вплив. Наприклад, зміна історичних даних вимагає доступу до систем зберігання даних, тоді як несанкціонований доступ адміністратора залежить від використання певних вразливостей.

4.3.3 Аналіз загроз та оцінка ризиків у зоні віддаленого користувача

У віддаленій зоні користувача люди використовують персональні копм’ютери та мобільні пристрої для моніторингу та керування інтелектуальними системами сонячної енергії через хмарні сервіси. Однак така конфігурація створює кілька ризиків для безпеки.

Спуфінг: зловмисники можуть видавати себе за законних користувачів, крадучи або вгадуючи облікові дані за допомогою таких методів, як фішинг, шкідливе програмне забезпечення або використання слабких паролів. Це може надати несанкціонований доступ до хмарних панелей інструментів, що дозволить їм змінювати конфігурації системи або красти конфіденційні дані;

Фальсифікація: незахищені канали зв'язку між віддаленими пристроями та хмарними сервісами вразливі до перехоплення та модифікації. Зловмисники можуть маніпулювати пакетами даних, що призводить до неправильних команд або оманливої аналітики. Крім того, скомпрометовані пристрої можуть надсилати несанкціоновані інструкції системі, тим самим впливаючи на її роботу;

Заперечення: без належних систем реєстрації та відстеження користувачі або зловмисники можуть заперечувати свою причетність до критично важливих дій. Така відсутність підзвітності ускладнює відстеження несанкціонованих змін, реагування на інциденти та підриває безпеку системи;

Розкриття інформації: незашифрований зв'язок надає зловмисникам доступ до критично важливих даних, таких як системні налаштування, операційні показники та облікові дані. Якщо пристрої скомпрометовані, вони можуть витікати конфіденційну інформацію, надаючи зловмисникам подальший доступ до системи;

Відмова в обслуговуванні: зловмисники можуть перевантажити хмарні сервіси або віддалені пристрої надмірним трафіком, зробивши їх нефункціональними. Це перешкоджає легітимним користувачам контролювати або моніторити систему, що потенційно може спричинити проблеми з її роботою;

Підвищення прав: використання вразливостей в облікових записах користувачів або пристроях дозволяє зловмисникам отримати несанкціонований доступ. Маючи права адміністратора, вони можуть вносити необмежені зміни, тим самим ставлячи під загрозу стабільність і безпеку системи. У таблиці 4.5 наведено загрози у зоні віддаленого користувача.

Для подальшої оцінки серйозності цих загроз було застосовано систему оцінки ризиків *DREAD*. *DREAD* оцінює загрози за п'ятьма вимірами: потенціал пошкодження, відтворюваність, експлуатаційна спроможність, уражені користувачі та можливість виявлення.

Результати цієї оцінки детально описані в таблиці 4.6. Оцінка *DREAD* показує, що більшість загроз у зоні віддаленого користувача класифікуються як високоризикові, з оцінками від 2,6 до 2,8. Наприклад, зловмисники, які крадуть облікові дані, щоб видавати себе за інших користувачів, отримали 2,8 бала, що є найвищим балом ризику в цій зоні.

Таблиця 4.5 – Аналіз загроз STRIDE для зони віддаленого користувача.

Категорія загрози (*STRIDE*)	Потік компонентів/комунікації	Виявлена загроза	Супутні ризики
Спуфінг (*S*)	Пристрої віддалених користувачів (ПК/мобільні пристрої)	Зловмисники крадуть облікові дані, щоб видавати себе за інших користувачів	Несанкціонований доступ призводить до зловмисних дій або витоків даних.
Спуфінг (*S*)	Передача даних між пристроями користувача та хмарою	Перехоплення та маніпулювання даними	Змінені дані призводять до збоїв у роботі системи або неточної аналітики.
Фальсифікація (*T*)	Пристрої віддалених користувачів	Зловмисне програмне забезпечення змінює програми або системні налаштування	Можуть статися несанкціоновані команди або витік даних.
Заперечення (*R*)	Дії користувача на хмарній інформаційній панелі	Користувачі заперечують виконання ключових дій через відсутність реєстрації	Низька підзвітність ускладнює аудит та реагування на інциденти.
Розкриття інформації (*I*)	Нешифровані канали зв'язку	Дані розкриваються під час передачі	Зловмисники можуть отримати доступ до конфіденційних системних даних або облікових даних.
Розкриття інформації (*I*)	Пристрої віддалених користувачів	Скомпрометовані пристрої розкривають облікові дані або дані	Витік інформації уможливлює подальші атаки на систему.
Відмова в обслуговуванні (*D*)	Послуги віддаленого доступу	Зловмисники затопили хмарні сервіси, що використовуються віддаленими користувачами	Законні користувачі втрачають доступ, порушуючи контроль над системою.
Відмова в обслуговуванні (*D*)	Пристрої віддалених користувачів (ПК/мобільні пристрої)	DoS-атаки призводять до непрацездатності пристроїв	Користувачі не можуть дистанційно контролювати або керувати системою.
Підвищення привілеїв (*E*)	Облікові записи віддалених користувачів	Зловмисники використовують вразливості для отримання вищих привілеїв	Повний адміністративний доступ дозволяє контролювати всю систему.

Ця загроза становить серйозну небезпеку, оскільки дозволяє зловмисникам отримати несанкціонований доступ, що потенційно може призвести до зловмисних дій або витоків даних. Аналогічно, перевантаження хмарних сервісів надмірними запитами (загроза відмови в обслуговуванні) також отримало 2,8 бала, що підкреслює його потенціал для порушення доступу до системи для законних користувачів та компрометації контролю над системою. Інші загрози

високого ризику включають перехоплення та маніпулювання даними, а також розкриття конфіденційних даних під час передачі, обидва з яких мають оцінку 2,6 через їхній серйозний вплив на цілісність та конфіденційність даних.

Таблиця 4.6 – Оцінка ризику для зони віддаленого користувача.

Категорія загрози	Конкретна загроза	Пошкодження	Відтворюваність	Експлуатаційність	Постраждалі користувачі	Видимість	Оцінка ризику (середня)	Рівень ризику
Спуфінг (*S*)	Зловмисники крадуть облікові дані, щоб видавати себе за інших користувачів	3	3	2	3	3	2.8	Високий
Спуфінг (*S*)	Перехоплення та маніпулювання даними	3	2	2	3	3	2.6	Високий
Фальсифікація (*T*)	Зловмисне програмне забезпечення змінює програми або системні налаштування	3	2	2	3	2	2.4	Середній
Заперечення (*R*)	Користувачі заперечують виконання ключових дій через відсутність реєстрації	2	2	1	2	2	1.8	Середній
Розкриття інформації (*I*)	Дані розкриваються під час передачі	3	2	2	3	3	2.6	Високий
Розкриття інформації (*I*)	Скомпрометовані пристрої розкривають облікові дані або дані	3	2	2	3	3	2.6	Високий

Продовження 4.6

Відмова в обслуговуванні (*D*)	Зловмисники затопили хмарні сервіси, що використовуються віддаленими користувачами	3	3	3	3	2	2.8	Високий
Відмова в обслуговуванні (*D*)	*DoS*-атаки призводять до непрацездатності пристроїв	3	2	2	3	2	2.4	Середній
Підвищення привілеїв (*E*)	Зловмисники використовують вразливості для отримання вищих привілеїв	3	2	2	3	2	2.4	Середній

Натомість, такі загрози, як зміна програм або системних налаштувань за допомогою шкідливого програмного забезпечення, атаки типу «відмова в обслуговуванні», що призводять до непрацездатності пристроїв, та використання вразливостей для отримання вищих привілеїв, були оцінені як середній ризик (бали: 2,4). Незважаючи на те, що ці загрози все ще становлять значні ризики, вони є менш терміновими, ніж загрози з високим рівнем ризику, через їхню нижчу ймовірність експлуатації або обмеженіший масштаб впливу. Наприклад, атаки шкідливого програмного забезпечення вимагають встановлення шкідливого програмного забезпечення, а *DoS*-атаки на окремі пристрої впливають лише на певну підгрупу користувачів. Примітно, що жодна із загроз у зоні віддаленого користувача не була класифікована як низькоризикова (1,0–1,5), що свідчить про те, що всі виявлені загрози потребують певного рівня уваги. Ці висновки підкреслюють важливість впровадження надійних заходів безпеки для вирішення виявлених ризиків.

Інтеграція моделювання загроз *STRIDE* та систем оцінки ризиків *DREAD* у зоні локального користувача, зоні хмарних сервісів та зоні віддаленого користувача забезпечила систематичну пріоритезацію ризиків кібербезпеки в інтелектуальних системах сонячної енергії на базі Інтернету речей. Аналіз показав, що більшість загроз належать до категорії високого ризику з оцінками від 2,6 до 2,8, хоча менша підмножина була класифікована як середній ризик з

оцінками від 1,8 до 2,4. Примітно, що жодної загрози не було визначено як низькоризикову, що підкреслює критичну необхідність комплексних заходів безпеки.

Взаємозалежність між локальною зоною користувача, зоною хмарних сервісів та зоною віддаленого користувача створює складний ландшафт ризиків, де вразливості в одній зоні можуть каскадно поширюватися на інші. Наприклад, якщо зловмисник успішно підміняє датчик у локальній зоні користувача, він може впровадити неправдиві дані в зону хмарних сервісів. Ці неправдиві дані можуть призвести до неправильної аналітики, що призведе до надсилання шкідливих команд керування назад до локальної системи, що потенційно може спричинити фізичну шкоду або збої в роботі. Аналогічно, атака типу «відмова в обслуговуванні» (*DoS*) на зону хмарних сервісів може перешкодити віддаленим користувачам отримати доступ до критично важливих функцій моніторингу та керування, що призведе до неефективності роботи або навіть збоїв системи. Крім того, якщо облікові дані віддаленого користувача скомпрометовані, зловмисники можуть отримати несанкціонований доступ до зони хмарних сервісів, що дозволить їм маніпулювати даними або надсилати шкідливі команди до локальної зони користувача. Ці приклади підкреслюють необхідність багаторівневого підходу до захисту, де заходи безпеки впроваджуються в кожній зоні для зменшення ризику каскадних збоїв.

4.4 Рекомендації щодо контролю безпеки

4.4.1 Системи виявлення та запобігання вторгненням

Системи виявлення вторгнень (*Intrusion Detection System* (*IDS*)) та системи запобігання вторгненням (*Intrusion Prevention System* (*IPS*)) важливі для підтримки цілісності системи. *IDS* контролює операції, поведінку пристроїв та мережевий трафік для виявлення потенційних порушень безпеки, таких як шкідливе програмне забезпечення, несанкціонований доступ та аномальна активність. Вони забезпечують раннє виявлення загроз та генерують журнали

для аналізу після інцидентів. *IDS* може бути заснована на сигнатурах порівнюючи активність з відомими шаблонами, або заснована на аномаліях, яка виявляє відхилення від нормальної поведінки. На противагу цьому, *IDS* на основі аномалій працюють, встановлюючи базову лінію нормальної поведінки мережі, а потім виявляючи відхилення від цієї норми.

Система виявлення інтелектуальних систем виявлення розширює функціональність систем виявлення інтелектуальних систем (*IDS*), не лише виявляючи загрози, але й блокуючи підозрілий трафік та ізолюючи скомпрометовані пристрої. Такий проактивний підхід знижує ризики, але іноді може блокувати законні дії, що вимагає ретельного налаштування та моніторингу. *IDS* та *IPS* мають вирішальне значення для інтелектуальних фотоелектричних систем, де великі потоки даних від датчиків та систем керування вимагають постійного моніторингу порушень. Регулярні оновлення методів виявлення гарантують, що ці системи залишаються ефективними в динамічному ландшафті кібербезпеки. Досягнення в *IDS* включають гібридні системи, які контролюють як фізичні, так і кібермережі, пропонуючи комплексний захист від кіберфізичних атак на розподілені енергетичні ресурси.

Впровадження *IDS/IPS* у сонячних енергетичних системах на базі Інтернету речей є перспективним підходом до підвищення кібербезпеки. Однак, для забезпечення ефективного розгортання цих систем необхідно вирішити кілька проблем. Одна з перешкод полягає в обмеженості ресурсів, властивих пристроям Інтернету речей, таким як датчики та шлюзи. Ці пристрої часто мають обмежену обчислювальну потужність та пам'ять, що ускладнює створення повномасштабних рішень *IDS/IPS*. Легкі фреймворки, спеціально розроблені для таких середовищ, стають важливим аспектом у пом'якшенні цих обмежень.

Ще однією проблемою є складність налаштування рішень *IDS* на основі аномалій. Хоча ці системи ефективні, вони потребують значного налаштування для балансування хибнопозитивних та хибнонегативних результатів. Цей процес вимагає не лише технічних знань, але й постійних зусиль, особливо у високодинамічних та взаємопов'язаних екосистемах Інтернету речей, таких як

інтелектуальні системи сонячної енергії. Крім того, фінансові витрати, пов'язані з розгортанням передових рішень *IDS/IPS*, включаючи апаратне забезпечення, ліцензії на програмне забезпечення та кваліфікований персонал, можуть створювати перешкоди, особливо для менших проектів з обмеженим бюджетом. Інтеграція з існуючою інфраструктурою Інтернету речей ще більше ускладнює впровадження. Багато систем покладаються на застарілі пристрої та протоколи, що вимагає значного налаштування для забезпечення сумісності. Такі зусилля часто подовжують терміни розгортання та вимагають додаткових ресурсів, що підкреслює необхідність стратегічного планування та поступового впровадження.

Незважаючи на ці труднощі, існують життєздатні стратегії для підвищення його доцільності. Легкі рішення *IDS/IPS*, розроблені для середовищ Інтернету речей, можуть зменшити потреби в ресурсах, тоді як поетапний підхід до впровадження надає пріоритет критичним компонентам, таким як шлюзи та хмарні інтерфейси, що дозволяє ефективно керувати розподілом ресурсів. Постійне оновлення алгоритмів виявлення та навчання персоналу є важливими для адаптації до змін у ландшафті загроз та для підтримки стійкості системи. Ретельно орієнтуючись у цих проблемах та впроваджуючи цільові стратегії пом'якшення наслідків, можна реалізувати переваги *IDS/IPS*, сприяючи розвитку безпечних та стійких систем сонячної енергії на базі Інтернету речей.

4.4.2 Контроль доступу та автентифікація користувачів.

Впровадження технології *IoT* в інтелектуальні фотоелектричні системи вимагає суворого контролю доступу та механізмів автентифікації для захисту конфіденційних даних. Контроль доступу обмежує доступ до системи лише уповноваженими особами, а автентифікація користувачів перевіряє їхню особу. Доступ на основі ролей гарантує, що користувачі отримують доступ лише до функцій, необхідних для їхніх ролей, тим самим зменшуючи внутрішні загрози.

Багатофакторна автентифікація (*MFA*), надійні політики паролів та біометрія посилюють автентифікацію користувачів, вимагаючи використання кількох методів перевірки. Ці механізми захищають критично важливі системні

дані та компоненти, а також зменшують ризики, пов'язані з несанкціонованим доступом або зловмисною поведінкою. Правильне планування, обслуговування та оновлення мають вирішальне значення для забезпечення адаптації цих засобів контролю до нових загроз кібербезпеці.

Контроль доступу та автентифікація користувачів є основоположними для безпеки сонячних енергетичних систем на базі Інтернету речей, оскільки вони запобігають несанкціонованому доступу та гарантують, що лише законні користувачі можуть взаємодіяти з критично важливими компонентами системи. Однак реалізація цих механізмів у таких середовищах створює кілька технічних проблем.

Одна з проблем виникає через сумісність зі застарілими пристроями. Багато систем сонячної енергії на базі Інтернету речей містять застаріле обладнання та протоколи, які можуть не підтримувати сучасні механізми автентифікації, такі як біометричні дані або системи на основі токенів. Це обмеження часто вимагає зусиль щодо індивідуальної інтеграції, що може збільшити складність розгортання та вартість. Для пом'якшення цих проблем важливі легкі та масштабовані системи контролю доступу, адаптовані до середовища Інтернету речей. Поєднання контролю доступу на основі ролей з динамічними політиками доступу може адаптувати дозволи в режимі реального часу залежно від пристрою або поведінки користувача. Крім того, рішення *MFA*, оптимізовані для зручності використання, такі як *push*-сповіщення або одноразові паролі на основі часу (*TOTP*), можуть підвищити безпеку без перевантаження користувачів.

Для застарілих систем, рішення проміжного програмного забезпечення, що діють як мости автентифікації, можуть допомогти інтегрувати передові механізми зі старою інфраструктурою. Крім того, впровадження систем безперервної автентифікації, які відстежують активність користувачів на наявність аномалій після першого входу, може забезпечити додатковий рівень захисту. Завдяки впровадженню цих стратегій можна ефективно розгорнути механізми контролю доступу та автентифікації, забезпечуючи цілісність та

безпеку сонячних енергетичних систем на базі Інтернету речей без шкоди для операційної ефективності.

4.4.3 Моніторинг безпеки та реагування на інциденти

Моніторинг безпеки забезпечує постійний моніторинг інтелектуальної фотоелектричної системи шляхом виявлення потенційних загроз у режимі реального часу. До них належать моніторинг мереж, датчиків та інших компонентів системи на наявність вразливостей та аномалій. Реагування на інциденти доповнює моніторинг шляхом стримування загроз, аналізу першопричин, їх усунення та забезпечення дотримання правил.

Ефективне реагування на інциденти мінімізує вплив порушень безпеки, сприяючи швидкому відновленню та впровадженню заходів для запобігання повторенню. Однак складність інтелектуальних фотоелектричних систем з кількома взаємопов'язаними компонентами ускладнює балансування хибнопозитивних та хибнонегативних результатів, вимагаючи складних рішень та значних інвестицій у технології та навчання.

Моніторинг безпеки та реагування на інциденти є критично важливими компонентами комплексної стратегії кібербезпеки для сонячних енергетичних систем на базі Інтернету речей. Ці системи з їхніми взаємопов'язаними пристроями та залежністю від даних у режимі реального часу вимагають надійних механізмів для оперативного виявлення, аналізу та реагування на загрози безпеці. Однак, реалізація цих заходів на практиці пов'язана як з технічними, так і з операційними труднощами. Основною проблемою моніторингу безпеки є балансування обсягу даних, що генеруються пристроями Інтернету речей, з можливістю виявлення значущих аномалій. Абсолютний обсяг потоків даних від датчиків, шлюзів та хмарних систем може перевантажити інструменти моніторингу, особливо коли використовуються традиційні методи. Передові методи, такі як машинне навчання та алгоритми виявлення аномалій, необхідні для фільтрації шуму та виявлення справжніх загроз, але для ефективного впровадження потрібні значні обчислювальні ресурси та досвід.

Реагування на інциденти стикається з власним набором труднощів, зокрема, у координації дій у розподіленій системі. Децентралізований характер сонячних енергетичних систем на базі Інтернету речей, які охоплюють локальні пристрої, хмарні платформи та віддалені користувацькі інтерфейси, ускладнює ізоляцію та стримування загроз. Затримка реагування через недостатній зв'язок між компонентами може погіршити вплив порушень безпеки.

Щоб подолати ці проблеми, моніторинг безпеки повинен використовувати масштабовані та інтелектуальні системи, які можуть адаптуватися до динамічної поведінки середовищ Інтернету речей. Централізовані панелі інструментів, інтегровані з передовими інструментами аналітики, можуть допомогти фахівцям з безпеки візуалізувати загрози в режимі реального часу, що дозволяє швидше приймати рішення. Для реагування на інциденти автоматизовані механізми, такі як сценарії для поширених сценаріїв загроз та попередньо налаштовані протоколи ізоляції для скомпрометованих пристроїв, можуть значно скоротити час реагування. Крім того, інтеграція систем моніторингу та реагування з можливостями реєстрації та аудиту гарантує ефективне управління інцидентами та їх аналіз після події для постійного вдосконалення. Вирішуючи ці проблеми за допомогою адаптивних та інтегрованих рішень, системи сонячної енергії на базі Інтернету речей можуть досягти стійкої та проактивної кібербезпеки.

4.4.4 Шифрування даних та конфіденційність даних

Фотоелектричні системи на базі Інтернету речей генерують значні обсяги даних про виробництво енергії, продуктивність системи та взаємодію з користувачем. Шифрування даних гарантує захист конфіденційної інформації під час передачі, тим самим запобігаючи несанкціонованому доступу. Шифрування є ключем до дотримання правил захисту даних та підтримки довіри користувачів. Тим не менш, балансування безпеки та зручності використання, особливо за допомогою ефективного управління ключами, залишається складним завданням.

Шифрування даних та конфіденційність мають вирішальне значення для захисту величезної кількості конфіденційної інформації, що генерується

системами сонячної енергії на базі Інтернету речей. Ці системи залежать від безперервного обміну даними між датчиками, шлюзами та хмарними платформами, тим самим захищаючи дані під час передачі та в стані спокою. Однак впровадження шифрування та забезпечення конфіденційності в цих середовищах створює певні технічні труднощі. Однією з ключових проблем є накладні витрати на обробку, що виникають через алгоритми шифрування. Пристрої Інтернету речей, особливо ті, що розгортаються в польових умовах, такі як датчики та граничні вузли, часто мають обмежену обчислювальну потужність та пам'ять. Впровадження надійних протоколів шифрування, таких як *AES*, для безпеки даних може навантажувати ці пристрої та потенційно впливати на операції в режимі реального часу. Необхідно оптимізувати схеми шифрування, щоб збалансувати безпеку та продуктивність.

Таким чином, ефективне управління ключами створює значний виклик. У розподілених системах Інтернету речей безпечне керування ключами шифрування на кількох пристроях та кінцевих точках зв'язку стає дедалі складнішим. Скомпрометовані ключі можуть призвести до несанкціонованого доступу, підриваючи загальну безпеку системи. Надійні політики ротації ключів та безпечні механізми зберігання, такі як апаратні модулі безпеки (*HSM*), є важливими для зменшення цих ризиків. Питання конфіденційності даних ще більше ускладнюються нормативними вимогами, такими як *GDPR* або регіональні закони про конфіденційність. Ці правила вимагають суворого дотримання вимог щодо обробки даних користувачів, включаючи забезпечення шифрування, анонімізації та захисту від несанкціонованого доступу. Досягнення відповідності та збереження зручності використання та ефективності системи додає додаткового рівня складності.

Вирішення цих проблем вимагає впровадження легких алгоритмів шифрування, оптимізованих для пристроїв Інтернету речей, разом із методами вибіркового шифрування, які надають пріоритет захисту конфіденційних даних та зменшують споживання ресурсів. Інтеграція автоматизованих рішень для управління ключами може підвищити безпеку, мінімізуючи людські помилки.

Крім того, технології підвищення конфіденційності, такі як маскування даних та диференціальна конфіденційність, можуть допомогти узгодити операції системи з нормативними вимогами без шкоди для функціональності. Досягнення в квантових комунікаційних мережах пропонують перспективні рішення для багатьох проблем безпеки Інтернету речей. До них належать шифрування безпечної передачі, цифрові підписи та надійна автентифікація особи.

Інтеграція цих передових технологій у сонячні енергетичні системи на базі Інтернету речей може усунути вразливості, які традиційні криптографічні методи намагаються зменшити, особливо з огляду на нові загрози квантових обчислень. Хоча поточне дослідження зосереджено на традиційних заходах безпеки, конкретні дослідницькі роботи можуть дослідити можливість включення квантової криптографії для підвищення стійкості інтелектуальних фотоелектричних систем.

4.4.5 Регулярні оновлення програмного забезпечення

Регулярні оновлення програмного забезпечення є критично важливими для усунення вразливостей в програмній екосистемі інтелектуальних фотоелектричних систем. Ці оновлення містять виправлення безпеки, нові функції та покращення продуктивності. Керування виправленнями включає систематичну ідентифікацію, оцінку та застосування цих оновлень для підтримки безпеки та функціональності системи. Ефективне управління виправленнями включає такі кроки:

– визначення пріоритетів виправлень для забезпечення усунення критичних вразливостей;

– тестування та перевірка оновлень у контрольованих середовищах для запобігання проблемам сумісності;

– процедури контролю змін для забезпечення безпечного та задокументованого розгортання патчів;

– план резервного копіювання та відкату для відновлення систем, якщо оновлення спричиняють нестабільність;

– регулярний моніторинг та дотримання вимог забезпечують своєчасне застосування оновлень програмного забезпечення, особливо для систем, які вимагають суворого дотримання галузевих стандартів.

Регулярні оновлення програмного забезпечення та керування виправленнями є життєво важливими для забезпечення безпеки та надійності сонячних енергетичних систем на базі Інтернету речей. Однак необхідно вирішувати такі проблеми, як збої в роботі, сумісність зі застарілими пристроями та вразливості під час процесу оновлення. Збої можуть виникати через необхідність безперебійної роботи системи; однак розпорошені екосистеми можуть перешкоджати впровадженню виправлень у різних компонентах.

Безпечні протоколи оновлення, автоматизовані системи розгортання та попереднє тестування є важливими для зменшення ризиків. Проблеми сумісності можна вирішити за допомогою рішень проміжного програмного забезпечення або співпраці з постачальниками. Крім того, механізми резервного копіювання та відкату забезпечують стабільність системи у разі збоїв. Ці заходи дозволяють сонячним системам на базі Інтернету речей залишатися безпечними та функціональними, мінімізуючи вплив на експлуатацію.

4.4.6 Сегментація мережі

Сегментація мережі підвищує безпеку інтелектуальних фотоелектричних систем, розділяючи мережу на менші, ізольовані сегменти, тим самим обмежуючи горизонтальне переміщення зловмисників. Це зменшує масштаби порушень безпеки, навіть якщо один сегмент скомпрометовано. Сегментація мережі мінімізує вплив подій безпеки, розділяючи компоненти з різними рівнями безпеки. Заходи контролю доступу, такі як брандмауери та політики автентифікації, керують трафіком між сегментами, дотримуючись принципу найменших привілеїв. Безперервний моніторинг виявляє аномальну активність у сегментованій мережі, тим самим дозволяючи своєчасно реагувати на потенційні атаки.

Сегментація мережі підвищує безпеку сонячних енергетичних систем на базі Інтернету речей, ізолюючи компоненти в окремі зони, тим самим

обмежуючи поширення атак. Однак, проблеми включають розробку та підтримку складних політик сегментації, забезпечення безпечного, але безперебійного зв'язку між зонами та масштабування мереж у міру додавання нових пристроїв. Досягнення балансу між безпекою та функціональністю вимагає розширеного моніторингу, динамічного управління трафіком та регулярних аудитів.

Впровадження мікросегментації та централізованого управління політиками може вирішити ці проблеми, забезпечуючи детальний контроль та спрощуючи правозастосування. Ці стратегії підвищують стійкість системи до кіберзагроз, одночасно підтримуючи ефективну та безпечну роботу.

4.4.7 Оцінка безпеки постачальників

Безпека постачальників є критично важливою для фотоелектричних систем на базі Інтернету речей через їхню залежність від компонентів та послуг сторонніх виробників. Датчики, контролери, інвертори та хмарні платформи від різних постачальників створюють ризики для безпеки. Комплексні оцінки безпеки політик постачальників, стратегій безпеки даних та відповідності галузевим стандартам є важливими. Оцінки постачальників зосереджені на шифруванні, контролі доступу, реагуванні на інциденти та безпеці апаратних компонентів. Постійні оцінки гарантують, що заходи безпеки постачальників адаптуються до загроз, що розвиваються, одночасно сприяючи тісній співпраці між системними операторами та постачальниками для підтримки цілісності системи.

Оцінка безпеки постачальника є важливою для захисту систем сонячної енергії на базі Інтернету речей, оскільки ці системи значною мірою залежать від компонентів сторонніх виробників. Проблеми включають обмежену прозорість з боку постачальників, затримки оновлень безпеки та ризики ланцюга поставок, такі як підроблене обладнання. Вирішення цих проблем вимагає від організацій проведення комплексних оцінок постачальників, зосереджуючись на шифруванні, контролі доступу, реагуванні на інциденти та дотриманні таких стандартів, як *ISO/IEC* 27001. Договірні угоди повинні включати вимоги безпеки

та зобов'язання, щоб забезпечити дотримання постачальниками найкращих практик. Періодичні аудити та постійна співпраця з постачальниками можуть допомогти проактивно вирішувати вразливості, тим самим підвищуючи загальну безпеку систем сонячної енергії на базі Інтернету речей.

ВИСНОВКИ

В кваліфікаційній роботі було описано структуру та особливості використання систем Інтернет речей. Основною особливістю даних систем є обмежені розрахункові потужності пристроїв Інтернет речей, що не дають змогу використання потужних захисних механізмів. Безпека в системах Інтернет речей описано лише в загальних нормативних документах, що не завжди відображають специфіку таких систем.

В рамках кваліфікаційної роботи також було розглянуто основні види та причини виникнення загроз інформаційній безпеці систем Інтернет речей, та рекомендації по зменшенню їх вірогідності.

Практична частина роботи присвячена моделюванню загроз систем інформаційної безпеки сонячної електростанції з структурою Інтернет речей та розробці рекомендацій по усуненню вразливостей.

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке *IoT* (інтернет речей) простими словами? URL: https://armadio.net.ua/sho-take-internet-rechei-iz-chogo-vin-skladayetsya/ (дата звернення: 14.03.2025).

2. Інтернет речей: основні складові та їхня роль у сучасному світі. *URL*: https://cyberset.com.ua/hi-tech/iot/ (дата звернення: 17.03.2025).

3. Top-10 застосувань IoT. URL: https://www.imena.ua/blog/top-10-scope-iot/ (дата звернення: 24.03.2025).

4. Стандартизація *IoT*: Виклики та перспективи. *URL*: https://itgovreport.com/iot-standards (дата звернення: 15.05.2025).

5. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту при використанні технології хмарних обчислень та Методичних рекомендацій щодо оцінки відповідності хмарних послуг рівням безпеки (впевненості) : наказ Адміністрації Держспецзв'язку від 14.09.2024 р. № 505. *Офіційний вісник України*. 2024. № 76. С. 48–55.

6. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами : наказ Адміністрації Держспецзв'язку від 29.05.2023 р. № 463. *Офіційний вісник України*. 2023. № 47. С. 38–47

7. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» : нормативний документ. – Київ : Держспецзв'язку України, 1999. [Чинний з 01-07-1999]. 64-65 с.

8. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і формування стандартних функціональних профілів захищеності інформації від несанкціонованого доступу» : нормативний документ. – Київ : Держспецзв'язку України, 1999. [Чинний з 01-07-1999]. 8 с.

9. *ISO / IEC* 20924:2018. Інформаційні технології — Інтернет речей — Словник термінів. (ISO 20924:2016, *IDT*). [Чинний від 2018-05-15]. Вид. офіц. Київ : Держспоживстандарт України, 2018. 45 с.

10. *ISO / IEC* 21823-1:2019. Інтернет речей (*IoT*) — Сумісність для систем Інтернету речей — Частина 1: Фреймворк. (*ISO* 21823-1:2018, *IDT*). [Чинний від 2019-08-20]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2019. 60 с.

11. *ISO / IEC* 30141:2018. Еталонна архітектура Інтернету речей (*IoT* Reference Architecture). (*ISO* 30141:2018, *IDT*). [Чинний від 2019-02-01]. Вид. офіц. Київ : Мінцифра України, 2019. 80 с.

12. ДСТУ *ISO* / *IEC* 29182-3:2014. Інформаційні технології — Сенсорні мережі: Еталонна архітектура сенсорної мережі — Частина 3: Види архітектур. (*ISO* 29182-3:2014, *IDT*). [Чинний від 2015-01-15]. Вид. офіц. Київ : Держспоживстандарт України, 2015. 50 с.

13. *ISO / IEC* 30128:2014. Інформаційні технології — Сенсорні мережі — Загальний інтерфейс застосування для сенсорних мереж. (*ISO* 30128:2014, *IDT*). [Чинний від 2015-03-10]. Вид. офіц. Київ : Держспецзв'язку, 2015. 55 с.

14. *ISO / IEC* 30147:2020. Інформаційні технології — *IoT* — Методологія забезпечення надійності систем *IoT*. (*ISO* 30147:2018, *IDT*). [Чинний від 2021-05-05]. Вид. офіц. Київ : МЕРТ України, 2021. 70 с.

15. *ISO / IEC NP* 30161:2020. Інформаційні технології — *IoT*: Вимоги до платформ обміну даними *IoT*. (*ISO* 30161:2020, *NEQ*). [Чинний від 2022-07-12]. Вид. офіц. Київ : Український інститут науково-технічної експертизи та інформаційних ресурсів, 2022. 65 с.

16. *ISO / IEC* 27001:2016. Інформаційні технології — Методи та засоби забезпечення інформаційної безпеки — Управління інформаційною безпекою (*ISMS*). (*ISO* 27001:2013, *IDT*). [Чинний від 2016-12-22]. Вид. офіц. Київ : ДП «Український інститут стандартів», 2016. 110 с.

17. *ISO / IEC* 29100:2015. Інформаційні технології — Протокол конфіденційності для або на підтримку обробки персональних даних.

(*ISO* 29100:2011, *IDT*). [Чинний від 2016-06-15]. Вид. офіц. Київ : Держспецзв'язку України, 2016. 40 с. (Приватність і захист даних).

18. *Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks*. 2015. 146–164 p.

19. *Conti, M., Dehghantanha, A., Franke, K., & Watson, S. Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems.* 2018. 544–546 p.

20. *Roman, R., Najera, P., & Lopez, J. Securing the Internet of Things. Computer*. 2011. 51–58 p.

21. *Kalkan, K., & Zeadally, S. Securing Internet of Things (IoT) with software-defined networking (SDN). Future Generation Computer Systems.* 2020. 100–111 p.

22. *Williams, R., McMahon, E., Samtani, S., Patton, M., and Chen, H., Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach,"* 2017 *IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing,* 2017, *pp.* 179-181. (дата звернення: 29.04.2025).