

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

**Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей**

«До захисту допущено»

ВО завідувача кафедри

_____ Галина СОЗОННИК

«___» _____ 20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

**на тему: «Застосування технології Інтернету речей при реалізації захисту
“Розумного будинку”»**

Виконав:

студент IV курсу, групи ТС-01

Борисенко Ігор Костянтинович

Керівник:

Доцент, к.т.н., доцент

Максимов В.В

Рецензент:

Доцент каф. ІТТ, к.т.н., доцент

Правило В.В.

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів без
відповідних посилань.

Студент _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та інтернету речей»

ЗАТВЕРДЖУЮ

ВО завідувача кафедри

_____ Галина СОЗОННИК

«___» _____ 20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Борисенку Ігорю Костянтиновичу

1. Тема роботи «Застосування технології Інтернету речей при реалізації захисту «Розумного будинку»», керівник Максимов Володимир Васильович, затверджені наказом по університету від «22» травня 2024 р. №2064-с

2. Термін подання студентом роботи 07.06.2024

3. Вихідні дані до роботи

Пулеко І. В. Єфіменко А. А. Архітектура та технології Інтернету речей: навч. посіб. / І.В. Пулеко, А.А. Єфіменко. – Електронні дані. – Житомир: Державний університет «Житомирська політехніка», 2022. – 234 с.

Заїка В.Ф., Варфоломеева О.Г., Домрачева К.О., Гринкевич Г.О. ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ НАСТУПНОГО ПОКОЛІННЯ. -Київ – 2019. -315 с.

4. Зміст роботи

1. ІоТ. розгляд систем розумного будинку на основі технологій інтернету речей
2. Архітектура розумного будинку

3. Захист розумного будинку на основі технологій інтернету речей

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) Електронна презентація PowerPoint (в обсязі 10 слайдів):

1. Титульний слайд
2. Мета роботи та Зміст дослідження
3. Актуальність роботи
4. Ключові концепції Інтернету речей
5. Категоризація сфер Інтернету речей
6. Порівняльна характеристика протоколів
7. Переваги та недоліки протоколів
8. Основні види шифрування
9. Основні компоненти систем управління безпекою
10. Основні аспекти моніторингу та управління загрозами в IoT
11. Рекомендації щодо впровадження моніторингу та управління загрозами
12. Подяка за увагу

6. Дата видачі завдання 06.12.2023

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	06.12.2023	виконано
2	Збір інформації	15.01.2024	виконано
3	Розгляд технології Internet of Things	20.02.2024	виконано
4	Розгляд та аналіз архітектури розумного будинку на основі IoT	17.03.2024	виконано
5	Поглиблене вивчення загроз та вразливостей у системах розумного будинку	13.04.2024	виконано
6	Аналіз методів забезпечення безпеки та вибір відповідних протоколів для IoT	04.05.2024	виконано
7	Дослідження інструментів та технологій для захисту розумного будинку	25.05.2024	виконано
8	Оформлення дипломної роботи	01.06.2024	виконано
9	Отримання допуску до захисту		

Студент

Ігор БОРИСЕНКО

Керівник роботи

Володимир МАКСИМОВ

РЕФЕРАТ

Дипломна робота «Застосування технології Інтернету речей при реалізації захисту «Розумного будинку»» складається з переліку умовних скорочень, вступу, основної частини, що містить три розділи, висновків та списку використаних джерел. Загальний обсяг роботи складає 77 сторінок. Робота містить 29 рисунків 3 таблиці та 45 джерел.

У дипломній роботі проведено детальне дослідження та аналіз сучасних технологій Інтернету речей (IoT), спрямованих на забезпечення безпеки розумного будинку. Розглянуто архітектуру розумних будинків, включаючи сенсори, актуатори, контролери, хаби та інтерфейси користувача. Особливу увагу приділено вивченню різних архітектурних моделей розумного будинку: децентралізованої, централізованої та гібридної.

Також було проаналізовано різні протоколи зв'язку, такі як Zigbee, Z-Wave, Wi-Fi, Bluetooth, і проведено їх порівняльний аналіз для визначення оптимальних рішень з точки зору безпеки та ефективності. Досліджено типи загроз та вразливостей систем розумного будинку, включаючи фізичні та кібернетичні загрози, а також потенційні наслідки атак.

Особлива увага приділена методам забезпечення безпеки в IoT-системах, зокрема, аутентифікації та авторизації, шифруванню даних, виявленню та запобіганню вторгнень. Розглянуто сучасні інструменти та технології для захисту розумного будинку, такі як системи управління безпекою та використання блокчейну для безпеки IoT.

Крім того, у роботі представлені рекомендації щодо вибору протоколів зв'язку для конкретних потреб та заходи для підвищення рівня безпеки розумного будинку.

ІНТЕРНЕТ РЕЧЕЙ, ІОТ, РОЗУМНИЙ БУДИНОК, SMART HOUSE,
БЕЗПЕКА, КІБЕРБЕЗПЕКА, ШИФРУВАННЯ

ABSTRACT

The thesis "Application of Internet of Things Technology for Smart Home Security" consists of a list of abbreviations, an introduction, a main part containing three chapters, conclusions, and a list of references. The total volume of the work is 77 pages. The work includes 29 figures and 3 tables.

This thesis presents a detailed study and analysis of modern Internet of Things (IoT) technologies aimed at ensuring the security of smart homes. The architecture of smart homes is considered, including sensors, actuators, controllers, hubs, and user interfaces. Special attention is given to the study of different architectural models of smart homes: decentralized, centralized, and hybrid.

Various communication protocols such as Zigbee, Z-Wave, Wi-Fi, and Bluetooth are analyzed, and a comparative analysis is conducted to determine the optimal solutions in terms of security and efficiency. The types of threats and vulnerabilities in smart home systems, including physical and cyber threats, as well as the potential consequences of attacks, are examined.

Particular attention is given to security measures in IoT systems, specifically authentication and authorization, data encryption, and intrusion detection and prevention. Modern tools and technologies for smart home security, such as security management systems and the use of blockchain for IoT security, are reviewed.

Additionally, the thesis presents recommendations for choosing communication protocols for specific needs and measures to enhance the security level of smart homes.

INTERNET OF THINGS, IOT, SMART HOME, SMART HOUSE, SECURITY, CYBERSECURITY, ENCRYPTION

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ	8
ВСТУП.....	9
1 ІОТ. РОЗГЛЯД СИСТЕМ РОЗУМНОГО БУДИНКУ НА ОСНОВІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ.....	11
1.1 Сучасна ситуація в області інтернету речей (IoT)	11
1.2 Еволюція в Інтернеті Речей (IoT).....	13
1.3 Сфери застосування IoT	17
1.4 Висновки до розділу 1	22
2 АРХІТЕКТУРА РОЗУМНОГО БУДИНКУ	24
2.1 Основні компоненти розумного будинку	24
2.1.1 Сенсори та актуатори	24
2.1.2 Контролери та хаби.....	27
2.1.3 Інтерфейси користувача	30
2.2 Архітектурні моделі розумного будинку	33
2.2.1 Децентралізована архітектура	34
2.2.2 Централізована архітектура	36
2.2.3 Гібридна архітектура	39
2.3 Протоколи зв'язку в системах розумного будинку	42
2.3.1 Zigbee, Z-Wave, Wi-Fi, Bluetooth	42
2.3.2 Порівняльний аналіз протоколів	46
2.3.3 Вибір протоколу для конкретних потреб	47
2.4 Висновки по розділу 2	48
3 ЗАХИСТ РОЗУМНОГО БУДИНКУ НА ОСНОВІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ	50
3.1 Загрози та вразливості в системах розумного будинку	50

					НТУУ2064-с-24.01ТС-01.2024.ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата	Застосування технології Інтернету речей при реалізації захисту «Розумного будинку»		
Розроб.		Борисенко І.К.					
Перевір.		Максимов В.В.					
Реценз.		Правило В.В.					
Н. Контр.		Новіков В.І.					
Затверд.		Созонник Г.Д.			Літ. Арк. Акрушів		
					6 77		
					КПІ ім. Ігоря Сікорського НН ІТС		

3.1.1 Типи загроз (фізичні, кібернетичні).....	50
3.1.2 Вразливості пристроїв IoT	51
3.1.3 Потенційні наслідки атак	52
3.2 Методи забезпечення безпеки в IoT.....	53
3.2.1 Аутентифікація та авторизація	53
3.2.2 Шифрування даних	54
3.2.3 Виявлення та запобігання вторгненням.....	56
3.3 Інструменти та технології для захисту розумного будинку	63
3.3.1 Системи управління безпекою	63
3.3.2 Використання блокчейну для безпеки IoT	65
3.3.3 Моніторинг та управління загрозами	69
3.4 Висновки до розділу 3	71
ВИСНОВКИ.....	72
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	74

					НТУУ2064-с-24.01ТС-01.2024.ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		7

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

- IoT – Інтернет речей
- IIoT – Промисловий Інтернет речей
- SIoT – Соціальний Інтернет речей
- WE – Wearable Electronics (переносні пристрої)
- IDS – Intrusion Detection System (система виявлення вторгнень)
- IPS – Intrusion Prevention System (система запобігання вторгненням)
- SIEM – Security Information and Event Management (інформаційна безпека та управління подіями)
- QRadar – IBM QRadar (платформа управління інформаційною безпекою)
- AI – Artificial Intelligence (штучний інтелект)
- ML – Machine Learning (машинне навчання)
- VPN – Virtual Private Network (віртуальна приватна мережа)

ВСТУП

Тема:

"Застосування технології Інтернету речей при реалізації захисту «Розумного будинку» "

Актуальність:

Тема дослідження є надзвичайно актуальною через стрімкий розвиток технологій Інтернету речей (IoT) та їхній вплив на повсякденне життя. Розумні будинки стають все більш популярними, пропонуючи зручність, ефективність та безпеку для мешканців. Однак зростання кількості підключених пристроїв та їх інтеграція в єдину мережу створює нові виклики у сфері кібербезпеки. Вразливості в системах IoT можуть бути використані для атак, що ставить під загрозу конфіденційність та безпеку користувачів. Тому дослідження методів забезпечення безпеки для розумних будинків є вкрай важливим для захисту приватного життя та майна громадян.

Огляд питань, що будуть розглянуті:

У рамках цього дослідження буде проведено комплексний аналіз архітектури та безпеки розумних будинків на основі IoT-технологій. Спочатку будуть розглянуті основні компоненти розумного будинку, включаючи сенсори, актуатори, контролери, хаби та інтерфейси користувача. Далі буде досліджено різні архітектурні моделі розумного будинку: децентралізовану, централізовану та гібридну. Особлива увага буде приділена протоколам зв'язку, таким як Zigbee, Z-Wave, Wi-Fi, Bluetooth, а також їх порівняльному аналізу для визначення оптимальних рішень. Крім того, будуть розглянуті загрози та вразливості систем розумного будинку, методи забезпечення безпеки, такі як аутентифікація, авторизація, шифрування даних та виявлення вторгнень. Також буде проаналізовано сучасні інструменти та технології для захисту розумного будинку, включаючи системи управління безпекою та використання блокчейну.

Мета дослідження:

Основна мета дослідження полягає в комплексному вивченні та аналізі методів забезпечення безпеки розумних будинків на основі технологій Інтернету речей. Це включає вивчення архітектури розумних будинків, протоколів зв'язку, типів загроз та вразливостей, а також методів їх запобігання. Особливу увагу буде приділено розробці рекомендацій та стратегій для підвищення безпеки та надійності IoT-систем у розумних будинках.

Об'єкт дослідження:

Безпека розумних будинків, що використовують технології Інтернету речей. Це включає різноманітні компоненти, технології та методи, які забезпечують захист системи від загроз та атак.

Предмет дослідження:

Конкретні технологічні рішення, методи, протоколи та інструменти, які використовуються для забезпечення безпеки розумних будинків на основі IoT. Дослідження охоплює аналіз архітектурних моделей, протоколів зв'язку, методів виявлення та запобігання загрозам, а також оцінку їхньої ефективності та надійності.

1 ІОТ. РОЗГЛЯД СИСТЕМ РОЗУМНОГО БУДИНКУ НА ОСНОВІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Сучасна ситуація в області інтернету речей (IoT)

Інтернет речей (Internet of Things, IoT) є однією з найбільш інноваційних і динамічних галузей сучасної технології. IoT включає в себе мережу фізичних об'єктів, обладнаних сенсорами, програмним забезпеченням та іншими технологіями для зв'язку та обміну даними з іншими пристроями та системами через інтернет.

Глобальний ринок IoT

Станом на 2024 рік, ринок IoT продовжує швидко зростати. Аналітики прогнозують, що до 2025 року кількість підключених IoT-пристроїв перевищить 75 мільярдів. Це зростання зумовлене як розвитком технологій, так і збільшенням попиту на автоматизацію та підвищення ефективності в різних галузях промисловості.

Основні сегменти IoT

IoT можна поділити на кілька основних сегментів:

1. *Промисловий IoT (IIoT):* Застосування IoT в промисловості для оптимізації виробничих процесів, підвищення безпеки та ефективності, зменшення витрат. Приклади включають предиктивне обслуговування обладнання, розумні ланцюги постачання, автоматизацію виробництва.

2. *Розумний дім:* IoT пристрої, що використовуються в побуті, такі як розумні термостати, освітлення, системи безпеки, побутова техніка. Ці системи дозволяють автоматизувати і управляти різними аспектами життя вдома за допомогою мобільних додатків або голосових асистентів.

3. *Розумне місто:* Інтеграція IoT технологій для покращення міської інфраструктури, включаючи управління трафіком, моніторинг якості повітря, смарт-парковки, управління енергією.

4. *Здоров'я (IoT Health):* Використання IoT для моніторингу здоров'я пацієнтів, управління медичними даними, забезпечення віддаленого медичного

обслуговування. Приклади включають носимі пристрої для моніторингу життєво важливих показників, розумні медичні прилади.

5. *Роздрібна торгівля:* IoT застосування в роздрібній торгівлі для покращення досвіду покупців, управління запасами, персоналізації маркетингу. Наприклад, розумні полиці, які автоматично відстежують рівень запасів та інформують про необхідність поповнення.

Технологічні тенденції

Кілька ключових технологічних тенденцій формують розвиток IoT:

1. *5G:* Впровадження 5G забезпечує значно швидші і надійніші з'єднання, що є критичним для масового впровадження IoT-пристроїв, особливо в реальному часі.

2. *Штучний інтелект (AI) і машинне навчання (ML):* Інтеграція AI та ML з IoT дозволяє обробляти і аналізувати великі обсяги даних, що генеруються IoT-пристроями, для отримання інсайтів та автоматизації процесів.

3. *Безпека та конфіденційність:* Зі збільшенням кількості IoT-пристроїв зростає і кількість потенційних кіберзагроз. Важливими є розробка і впровадження безпечних протоколів та стандартів для захисту даних і забезпечення конфіденційності користувачів.

4. *Хмарні обчислення та Edge Computing:* Хмарні платформи дозволяють зберігати та обробляти великі обсяги даних, тоді як edge computing дозволяє обробляти дані ближче до джерела їх виникнення, зменшуючи затримки та підвищуючи швидкість реакції систем.

Виклики та перспективи

Хоча IoT має величезний потенціал, він також стикається з кількома викликами:

1. *Інтероперабельність:* Різноманітність пристроїв і протоколів створює проблеми з сумісністю і інтеграцією різних систем.

2. *Безпека:* Кібербезпека залишається критично важливою, оскільки багато IoT-пристроїв мають обмежені можливості для захисту від атак.

3. *Масштабованість*: Зі збільшенням кількості пристроїв виникають питання щодо ефективного управління та масштабування мереж.

Незважаючи на ці виклики, IoT продовжує розвиватися і змінювати різні аспекти нашого життя та промисловості. З подальшим розвитком технологій та впровадженням інновацій, IoT має всі шанси стати фундаментом для майбутніх розумних систем і середовищ.

1.2 Еволюція в Інтернеті Речей (IoT)

Початковий етап розвитку

Еволюція Інтернету речей (IoT) почалася з концепту, коли ідея підключення пристроїв до мережі тільки зароджувалася. В кінці 20-го століття технологічний прогрес, включаючи розвиток мікроконтролерів та сенсорів, заклав основу для IoT. Перші комерційні IoT-проекти зосереджувалися на індустріальних застосуваннях, таких як автоматизація та моніторинг обладнання.

Основні етапи еволюції IoT

1. Рання стадія (1990-ті роки)

- Відправні точки: Перші концепції IoT з'явилися у 1982 році, коли було підключено до мережі модифікований напоївний автомат в Університеті Карнегі-Меллона, що дозволяв перевіряти запаси напоїв та температуру.
- Технологічні розробки: Перші RFID (радіочастотна ідентифікація) та сенсорні технології почали використовуватися для ідентифікації та моніторингу об'єктів.

2. Поява терміну "IoT" (2000-ті роки)

- Визначення IoT: У 1999 році Кевін Ештон, співзасновник Auto-ID Center в MIT, ввів термін "Інтернет речей". Це підкреслювало ідею про те, що об'єкти можуть бути підключені до інтернету для обміну даними.
- Перші впровадження: Початкові проекти включали інтеграцію сенсорів та мереж для логістики та ланцюгів постачання. IoT почав

застосовуватися для моніторингу умов зберігання, відстеження руху товарів та оптимізації процесів.

3. Експоненційне зростання (2010-ті роки)

- Розвиток технологій: Поява хмарних обчислень, дешевих сенсорів, покращення мережевих технологій (Wi-Fi, 4G/5G), і збільшення потужності обробки даних на пристроях (edge computing).

- Споживчі пристрої: Вихід на ринок розумних пристроїв для споживачів, таких як розумні термостати (наприклад, Nest), освітлення (Philips Hue), та голосові асистенти (Amazon Echo, Google Home).

Індустріальний IoT (IIoT): Широке впровадження IoT в промисловості для моніторингу і управління виробництвом, енергетичними системами, транспортом та іншими критичними інфраструктурами.

4. Сучасний етап (2020-ті роки)

- Масове впровадження: Значне зростання кількості підключених пристроїв, які використовуються як у споживчому, так і в промисловому секторах.

- Технологічна інтеграція: Інтеграція IoT з іншими передовими технологіями, такими як штучний інтелект (AI), машинне навчання (ML), великі дані (Big Data) та блокчейн, для підвищення ефективності і безпеки.

- Розумні міста: Застосування IoT для створення розумних міських інфраструктур, що включають управління трафіком, екологічний моніторинг, розумне освітлення та енергетичні системи.

Виклики та можливості

Еволюція IoT супроводжувалася численними викликами, такими як питання безпеки, конфіденційності даних, стандартів та інтероперабельності. Однак, незважаючи на ці проблеми, потенціал IoT продовжує розширюватися завдяки інноваціям та новим застосуванням:

1. Безпека: Забезпечення захисту даних та пристроїв від кіберзагроз.
2. Стандартизація: Розробка єдиних стандартів для забезпечення сумісності різних IoT-пристроїв та систем.

3. Енергоефективність: Розробка енергоефективних рішень для підключених пристроїв.

4. Етичні аспекти: Вирішення питань конфіденційності та етичного використання даних, зібраних IoT-пристроями.

Майбутнє IoT

З подальшим розвитком технологій та зростанням числа підключених пристроїв, IoT продовжуватиме трансформувати різні галузі та аспекти нашого життя. Основні напрямки розвитку включають:

1. Підвищення інтеграції AI та ML: Використання штучного інтелекту та машинного навчання для автоматизації процесів та прийняття рішень на основі аналізу даних, зібраних IoT-пристроями.

2. Розширення застосувань в розумних містах та інфраструктурах: Подальший розвиток розумних міст з інтеграцією IoT для покращення управління міськими ресурсами та інфраструктурою.

3. Розвиток нових інтерфейсів та взаємодій: Інновації у взаємодії з IoT-пристроями, включаючи голосові асистенти, доповнену та віртуальну реальність.

4. Посилення кібербезпеки: Розробка нових рішень та стандартів для захисту IoT-систем від кіберзагроз та забезпечення конфіденційності даних.

Подібно до Інтернету, IoT також має свою еволюцію, яка є результатом конвергенції різних концепцій, таких як орієнтація на речі, Інтернет та семантику. За визначенням, наведеним у [5], IoT дозволяє людям і пристроям бути підключеними в будь-який час і в будь-якому місці, з будь-якими об'єктами та суб'єктами, використовуючи будь-який шлях або мережу та будь-які сервіси.

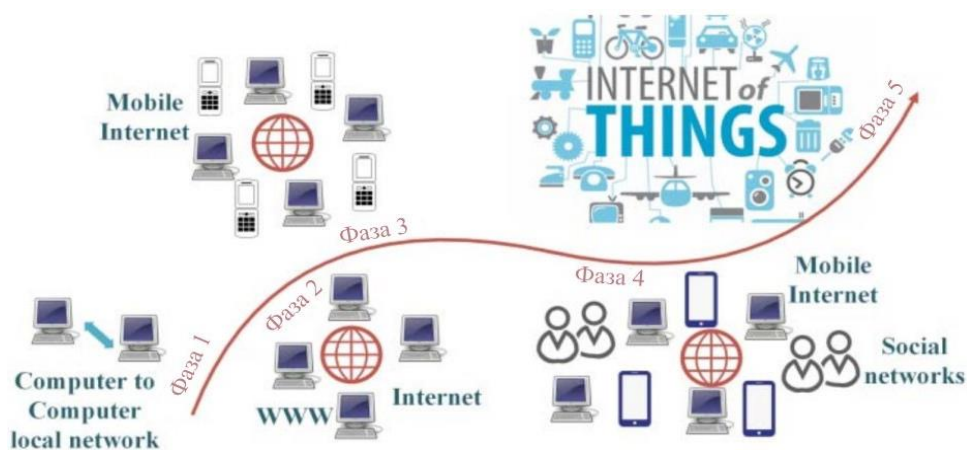


Рисунок 1.1 - Еволюція в IoT

Наукові дослідження показують, що велика кількість людей, об'єднаних у соціальній мережі, може давати більш точні відповіді на складні проблеми, ніж окрема особа або невелика група, навіть якщо вони дуже обізнані. Цей принцип широко використовується в різних сферах, пов'язаних з Інтернетом, і нещодавно досліджувався для впровадження систем IoT. Очікується, що IoT інтегрує багато технологій і об'єднає десятки мільярдів об'єктів за короткий час.

Соціальний Інтернет речей (SIoT) визначається як IoT, де речі можуть автономно встановлювати соціальні відносини з іншими об'єктами. Це створює соціальну мережу об'єктів. Прийняття парадигми SIoT має кілька переваг:

- Структура соціальної мережі речей може бути сформована відповідно до вимог, що забезпечує ефективну навігацію мережею для виявлення об'єктів та послуг, а також гарантує масштабованість, як у соціальних мережах людей.
- Рівень надійності можна встановити для підвищення взаємодії між об'єктами, які є "друзями".
- Моделі, розроблені для вивчення соціальних мереж, можуть бути використані для вирішення проблем, пов'язаних з IoT, які включають розгалужені мережі взаємопов'язаних об'єктів.

Іншим важливим аспектом IoT є Промисловий Інтернет речей (IIoT), який має на меті перетворити існуючу систему промислового виробництва та обслуговування в інтелектуальну систему автоматизації підприємства з вищим рівнем інтелекту та когнітивних обчислень. Це досягається через безпечне

підключення промислових активів через Інтернет і використання відповідних технологій, таких як хмарні обчислення, що забезпечує точний нагляд у промислових середовищах і збільшує прибуток від інвестицій.

1.3 Сфери застосування IoT

Інтернет речей (IoT) відкриває численні можливості для різних галузей, завдяки здатності підключати фізичні об'єкти до мережі та забезпечувати обмін даними між ними.

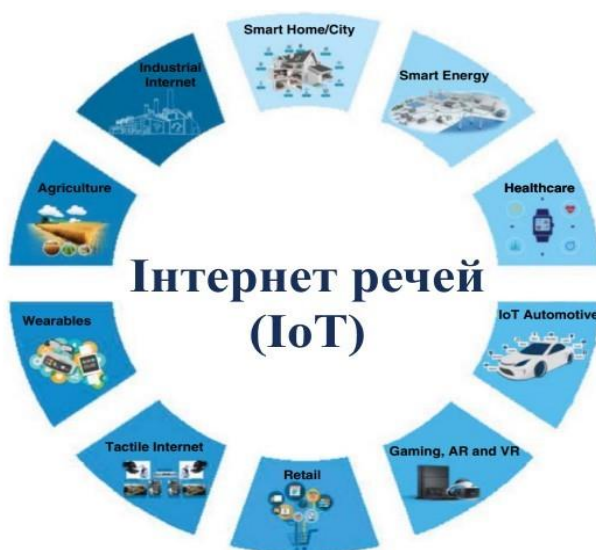


Рисунок 1.2 - Класифікація IoT сфер

Послуги, що стосуються ідентифікації, відображають кожен фізичний об'єкт у мережевому просторі (тим самим надаючи їм адресу), а також реалізують сервіси дозволу мережі. Подібні сервіси характерні для будь-якої сфери, де може бути використаний Інтернет речей. Потім, сервіси, які ефективно збирають агреговані дані від різноманітних об'єктів для подальшої обробки, відносяться до категорії сервісів агрегування інформації.

На основі зібраних агрегованих даних, сервіси, що підтримують спільну роботу, приймають рішення, і відповідно реагують/координують дії до моменту їх виконання. У кінцевому підсумку, універсальні сервіси забезпечують поширену присутність в мережі та доступність базових функцій, що підтримують спільну

роботу, у будь-який час. Сфери Інтернету речей, які розроблені з метою досягнення рівня всепроникної обслуговуючої мережі, принесуть найбільшу користь. Проте для досягнення цієї мети потрібна плавна інтеграція технологій, протоколів і стандартів.

Таблиця 1.1 - Категоризація різних сфер Інтернету речей

IoT сфера	Категорія відповідно до [6]	Категорія відповідно до [7]	Категорія відповідно до [8]
Smart Home	Співпрацюючий свідомий	Масовий IoT	Індивідуальний рівень
Smart City	Співпрацюючий свідомий	Масовий IoT	Інфраструктурний рівень
Smart Energy	Агрегація інформації	Масовий IoT	Інфраструктурний рівень
IoT Automotive	Агрегація інформації	Критичний IoT	Універсальний рівень
Healthcare	Агрегація інформації	Масовий IoT	Універсальний рівень
Gaming, AR, VR	Агрегація інформації	Масовий IoT	Індивідуальний рівень
Retail	Співпрацюючий свідомий	Масовий IoT	Організаційний рівень
Wearable	Агрегація інформації	Масовий IoT	Індивідуальний рівень
Smart Agriculture	Співпрацюючий свідомий	Масовий IoT	Організаційний рівень
Industrial Internet	Співпрацюючий свідомий	Критичний IoT	Організаційний рівень

В залежності від ступеня використання та адаптації конкретної сфери Інтернету речей, їх можна розділити на чотири рівні застосувань:

- Інфраструктурний рівень;
- Організаційний рівень;
- Індивідуальний рівень;
- Комплексний рівень.

На рівні інфраструктури розміщуються такі сфери, як розумні міста, розумна енергетика, розумний туризм та інші, де вони можуть сприяти створенню нового рівня екосистеми. Промисловий Інтернет, інтелектуальне сільське господарство, роздрібна торгівля та інші відносяться до організаційного рівня, оскільки такі програми призначені для автоматизації роботи організацій. Очевидно, що додатки, які належать до категорії індивідуального рівня, включають розумний будинок, ігри, переносні пристрої та інше. Однак існують

деякі сфери, які охоплюють всі рівні і можуть включати такі галузі, як медицина та охорона здоров'я, автомобілебудування, освіта та інші. Таблиця 1.1 демонструє односторонню категоризацію різних сфер Інтернету речей, тоді як таблиця 1.2 наводить характеристики цих сфер.

Таблиця 1.2 - Характеристики різноманітних сфер IoT

IoT сфера	Тип даних	Зворотний зв'язок	Очікувана затримка
Smart Home	Потокові / Історичні дані	Реальний час	1 мс - 1000 с
Smart City	Потокові / Масивні дані	Реальний час	≤ 1 мс
Smart Energy	Потокові / Масивні дані	Реальний час / Переривчастий	1 мс - 10 хв
IoT Automotive	Потокові / Масивні дані	Реальний час	≤ 1 мс
Remote surgery	Потокові дані	Реальний час	≤ 200 мс
Remote consultancy	Потокові дані	Реальний час	1 мс - 100 с
Gaming, AR, VR	Потокові / Масивні дані	Реальний час	≤ 1 мс
Retail	Потокові / Історичні дані	Реальний час / Переривчастий	≤ 1 мс
Wearable	Потокові дані	Переривчастий	Кілька годин
Smart Agriculture	Історичні дані	Переривчастий	Кілька годин

Нижче наведено основні сфери застосування IoT та їхні переваги.

Розумний дім (Smart Home) - основні аспекти:

- *Автоматизація:* Управління освітленням, опаленням, кондиціонуванням повітря, та побутовою технікою для підвищення комфорту і енергоефективності.

- *Безпека:* Інтегровані системи безпеки, включаючи відеоспостереження, сигналізацію та датчики руху, що забезпечують захист житла.

- *Голосові асистенти:* Пристрої, такі як Amazon Echo та Google Home, дозволяють керувати різними аспектами дому за допомогою голосових команд.

Приклад: Nest Learning Thermostat: Автоматично регулює температуру в домі на основі поведінки користувачів, що дозволяє заощаджувати енергію.

Розумні міста (Smart Cities) - основні аспекти:

- *Управління трафіком:* Інтелектуальні системи управління трафіком та паркування для зменшення заторів та покращення транспортної інфраструктури.

- *Моніторинг навколишнього середовища:* Системи для відстеження якості повітря, рівня шуму та інших екологічних параметрів для покращення якості життя.
- *Енергетичні системи:* Розумне управління енергоспоживанням та розподілом ресурсів для підвищення енергоефективності.



Рисунок 1.3 - Використання Інтернету речей в розумних містах

Приклад: Kyiv Smart City: Впровадження інтелектуальних рішень для управління транспортом, освітленням, сміттям та водопостачанням у Києві.

Промисловий Інтернет речей (IIoT) - основні аспекти:

- *Моніторинг обладнання:* Використання сенсорів для постійного відстеження стану обладнання, що дозволяє запобігати поломкам та зменшувати час простою.
- *Автоматизація виробництва:* Інтеграція робототехніки та автоматизованих систем для підвищення ефективності виробництва.
- *Управління ланцюгом постачання:* Оптимізація логістики та управління запасами на основі даних з IoT-пристроїв.

Приклад: General Electric Predix Platform: Хмарна платформа для аналізу даних з промислових пристроїв, що допомагає підвищувати ефективність виробництва.

Охорона здоров'я (Healthcare) - основні аспекти:

- *Віддалений моніторинг пацієнтів:* Використання носимих пристроїв для моніторингу життєво важливих показників пацієнтів в реальному часі.
- *Управління медичними даними:* Збирання та аналіз даних про пацієнтів для покращення діагностики та лікування.
- *Інтелектуальні медичні пристрої:* Використання IoT для створення розумних медичних приладів, таких як інсулінові помпи та інгалятори.



Рисунок 1.4 - Роль IoT у розумній охороні здоров'я

Приклад: Fitbit: Носимий пристрій для моніторингу фізичної активності, сну та інших показників здоров'я.

Сільське господарство (Agriculture) - основні аспекти:

- *Прецизійне землеробство:* Використання сенсорів для моніторингу умов ґрунту, вологості, температури та інших параметрів для оптимізації врожаїв.
- *Автоматизація обладнання:* Інтеграція автоматизованих систем для управління поливом, внесенням добрив та збором врожаю.
- *Моніторинг тварин:* Відстеження стану здоров'я та поведінки тварин за допомогою носимих пристроїв.

Приклад: John Deere Field Connect: Система для моніторингу ґрунтових умов та автоматизації зрошення.

Логістика та транспорт (Logistics and Transportation) - основні аспекти:

- *Відстеження вантажів:* Використання GPS та сенсорів для відстеження місцезнаходження та стану вантажів в реальному часі.
- *Інтелектуальні транспортні системи:* Оптимізація маршрутів та управління автопарком для підвищення ефективності транспорту.
- *Автономні транспортні засоби:* Інтеграція IoT для розробки безпілотних автомобілів та дронів.

Приклад: UPS Orion: Система для оптимізації маршрутів доставки, що дозволяє зменшувати витрати на паливо та покращувати обслуговування клієнтів.

Споживчі товари та роздрібна торгівля (Consumer Goods and Retail) - основні аспекти:

- *Розумні полиці:* Використання сенсорів для моніторингу запасів товарів та автоматичного поповнення.
- *Персоналізований маркетинг:* Збирання даних про поведінку покупців для створення індивідуальних маркетингових кампаній.
- *Автоматизація покупок:* Інтеграція розумних кошиків та касових систем для спрощення процесу покупок.

Приклад: Amazon Go: Магазини без касирів, де покупки можуть здійснювати покупки, використовуючи тільки мобільний додаток.

Ці приклади ілюструють, як IoT трансформує різні сфери, підвищуючи ефективність, безпеку та комфорт. Технологія продовжує розвиватися, відкриваючи нові можливості для інтеграції та інновацій у багатьох галузях.

1.4 Висновки до розділу 1

У цьому розділі було розглянуто основні концепції Інтернету речей (IoT) та його застосування у розумних будинках. Описано базові компоненти IoT, включаючи сенсори, актуатори, контролери та хаби, а також інтерфейси

користувача. Детально проаналізовано архітектурні моделі розумного будинку: децентралізована, централізована та гібридна. Показано, як ці архітектури сприяють автоматизації та підвищенню ефективності управління будинком, забезпечуючи зручність для користувачів.

2 АРХІТЕКТУРА РОЗУМНОГО БУДИНКУ

2.1 Основні компоненти розумного будинку

Архітектура розумного будинку складається з кількох основних компонентів, які забезпечують інтеграцію та автоматизацію різних систем і пристроїв. До основних компонентів відносяться сенсори та актуатори, які відіграють ключову роль у зборі даних та виконанні відповідних дій.

2.1.1 Сенсори та актуатори

Сенсори – це пристрої, які сприймають різні фізичні параметри (температуру, вологість, світло, рух тощо) і перетворюють їх на електричні сигнали, що можуть бути оброблені системою розумного будинку.

Актуатори – це пристрої, які виконують певні дії у відповідь на команди від системи. Вони можуть керувати різними пристроями, такими як освітлення, опалення, вентиляція, побутова техніка та інше.

Приклади сенсорів та актуаторів:

1. Сенсори руху:

Використовуються для виявлення присутності або руху в приміщенні.

Приклад: Philips Hue Motion Sensor[1]



Рисунок 2.1 - Motion sensor

2. Сенсори температури та вологості:

Вимірюють температуру та вологість повітря, забезпечуючи комфортні умови в приміщенні.

Приклад: Xiaomi Mi Temperature and Humidity Sensor[2]



Рисунок 2.2 - Temperature and Humidity Sensor

3. Сенсори освітленості:

Вимірюють рівень освітленості в приміщенні і можуть автоматично керувати освітленням.

Приклад: Bosch Smart Home Light Sensor[3]



Рисунок 2.3 - Bosch Smart Home Light Sensor

4. Сенсори диму та газу:

Виявляють дим або витік газу, забезпечуючи безпеку в будинку.

Приклад: Nest Protect Smoke and CO Alarm[4]

5. Актуатори для керування освітленням:

Автоматично включають або вимикають освітлення залежно від умов.

Приклад: Lutron Caseta Wireless Smart Lighting Dimmer Switch[5]



Рисунок 2.4 - Lutron Caseta Wireless Smart Lighting Dimmer

6. Актуатори для управління опаленням:

Регулюють роботу системи опалення для підтримання заданої температури.

Приклад: Honeywell Home T9 Smart Thermostat [6]



Рисунок 2.5 - Smart Thermostat

Сенсори та актуатори є невід'ємною частиною розумного будинку, забезпечуючи збирання інформації про навколишнє середовище та виконання автоматизованих дій для створення комфортного, безпечного та енергоефективного житлового простору.

2.1.2 Контролери та хаби

Контролери та хаби є центральними компонентами системи розумного будинку, що забезпечують зв'язок між сенсорами, актуаторами та іншими пристроями. Вони дозволяють користувачам керувати всіма аспектами розумного будинку через одну інтегровану платформу.

Контролери – це пристрої, які управляють сенсорами та актуаторами, обробляють дані, що надходять від них, і виконують задані дії.

Хаби – це центральні пристрої або платформи, які об'єднують усі розумні пристрої в одну мережу, забезпечуючи їхню взаємодію та спільну роботу.

Приклади контролерів та хабів:

1. *Samsung SmartThings Hub*:

Відноситься до універсальних хабів, сумісний з різними протоколами (Zigbee, Z-Wave, Wi-Fi).

Дозволяє керувати різноманітними розумними пристроями через одну платформу.

Детальніше: Samsung SmartThings Hub [7]



Рисунок 2.6 - SmartThings Hub

2. Amazon Echo Plus:

Смарт-динамік з вбудованим хабом для управління розумним будинком.

Підтримує управління пристроями через голосові команди за допомогою Alexa.

Детальніше: Amazon Echo Plus [8]



Рисунок 2.7 - Amazon Echo Plus

3. Google Nest Hub:

Інтерактивний дисплей з функціями керування розумним будинком.

Підтримує управління пристроями через голосові команди за допомогою Google Assistant.

Детальніше: Google Nest Hub [9]

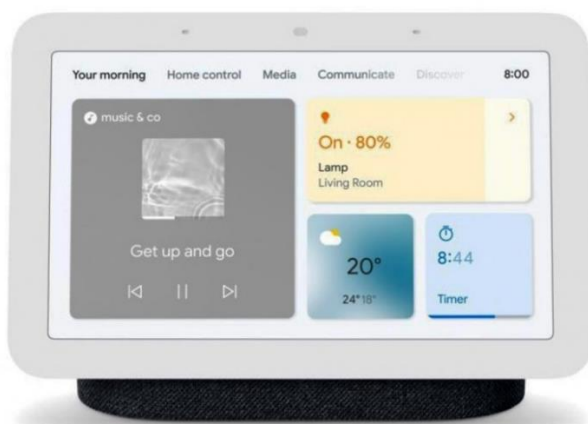


Рисунок 2.8 - Google Nest Hub

4. *Apple HomePod Mini:*

Смарт-динамік з функціями хаба для керування розумним будинком.

Підтримує управління пристроями через голосові команди за допомогою Siri.

Детальніше: Apple HomePod Mini [10]



Рисунок 2.9 - Apple HomePod Mini

5. *Fibaro Home Center 3:*

Потужний контролер для управління розумним будинком, підтримує протоколи Z-Wave та Zigbee.

Забезпечує розширені функції автоматизації та сценаріїв.

Детальніше: Fibaro Home Center 3 [11]

6. *Hubitat Elevation:*

Хаб для локального управління розумним будинком, підтримує Zigbee та Z-Wave.

Забезпечує високий рівень конфіденційності та безпеки даних.

Детальніше: Hubitat Elevation[12]



Рисунок 2.10 - Hubitat Elevation

Контролери та хаби забезпечують центральне управління розумним будинком, дозволяючи інтегрувати різні пристрої та системи в єдину екосистему. Вони відіграють ключову роль у забезпеченні автоматизації, безпеки та зручності використання розумного будинку.

2.1.3 Інтерфейси користувача

Інтерфейси користувача (UI) є важливою складовою систем розумного будинку, оскільки вони забезпечують взаємодію користувачів з різними пристроями та системами. Інтерфейси користувача можуть бути представлені у різних формах, таких як мобільні додатки, веб-інтерфейси, голосові асистенти та панелі управління.

Приклади інтерфейсів користувача:

1. Мобільні додатки:

Забезпечують дистанційне керування всіма аспектами розумного будинку через смартфон або планшет.

Мають інтуїтивно зрозумілий інтерфейс для налаштування та моніторингу систем.

Приклад: Samsung SmartThings App [13]

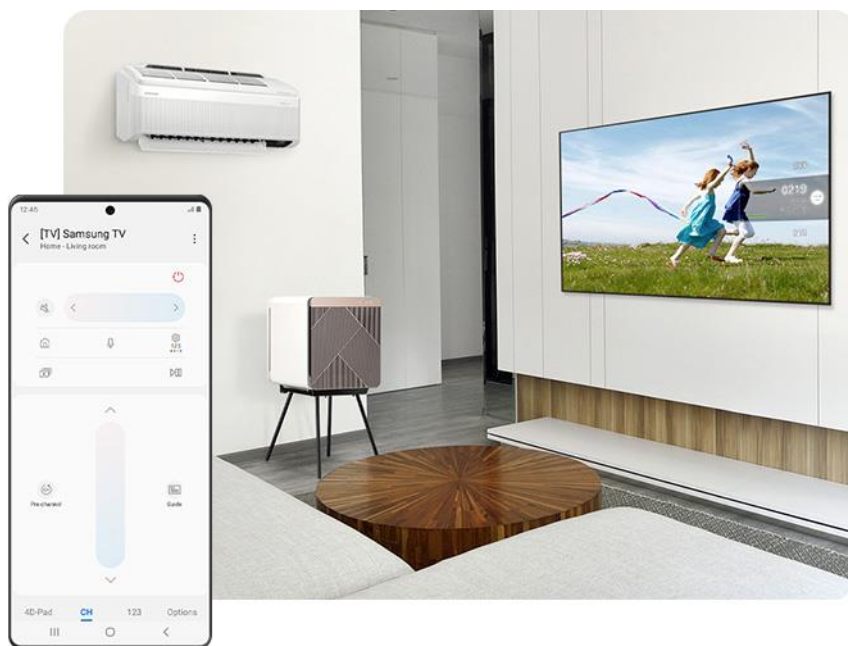


Рисунок 2.11 - Samsung SmartThings App

2. Веб-інтерфейси:

Доступні через браузер і дозволяють керувати розумним будинком з будь-якого пристрою з доступом до Інтернету.

- Забезпечують детальний контроль та аналіз даних про стан систем.

- Приклад: Fibaro Home Center Web Interface [14]



Рисунок 2.12 - Fibaro Home Center Web Interface

3. Голосові асистенти:

Дозволяють керувати розумним будинком за допомогою голосових команд.

Інтегровані з такими платформами, як Amazon Alexa, Google Assistant, Apple Siri.

Приклад: Google Assistant [15]



Рисунок 2.13 - Google Assistant

4. Панелі управління:

Стаціонарні пристрої, встановлені в будинку для локального керування системами.

Можуть бути інтерактивними екранами або простими кнопками для швидкого доступу до функцій.

Приклад: Control4 Smart Home Panel [16]

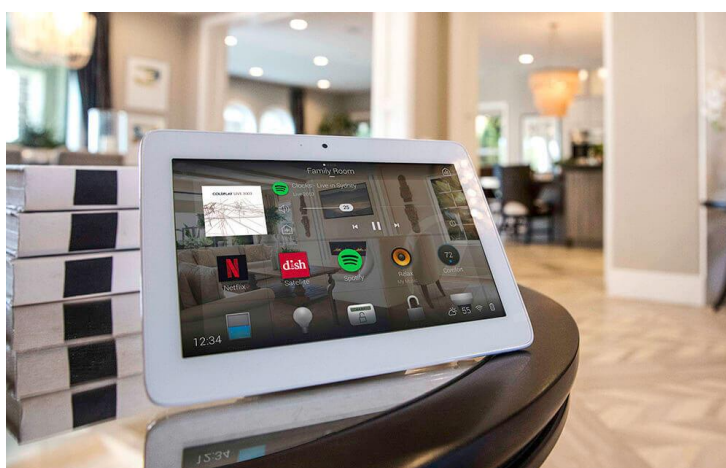


Рисунок 2.14 - Control4 Smart Home Panel

5. Портативні пульты:

Забезпечують керування системами розумного будинку з будь-якої точки приміщення.

Зазвичай використовуються для управління розвагами, освітленням, клімат-контролем.

Приклад: Logitech Harmony Elite Remote [17]



Рисунок 2.15 Logitech Harmony Elite Remote

Інтерфейси користувача забезпечують зручний доступ до функцій розумного будинку та дозволяють користувачам ефективно керувати своїм житловим простором. Вибір інтерфейсу залежить від потреб користувачів та типу систем, що встановлені в будинку.

2.2 Архітектурні моделі розумного будинку

Архітектура розумного будинку визначає, як компоненти системи взаємодіють між собою та з користувачем. Однією з моделей є децентралізована архітектура, яка має свої особливості та переваги.

2.2.1 Децентралізована архітектура

Децентралізована архітектура розумного будинку базується на розподіленому підході, де кожен пристрій або підсистема має автономність і здатність взаємодіяти з іншими пристроями без необхідності в центральному контролері або хабі. Цей підхід забезпечує більшу гнучкість і надійність системи.

Основні особливості децентралізованої архітектури:

1. Автономність пристроїв:

Кожен пристрій (сенсор, актуатор) має власний процесор і програмне забезпечення для обробки даних та виконання завдань.

Пристрої можуть функціонувати незалежно один від одного.

2. Пряме спілкування між пристроями:

Пристрої можуть обмінюватися даними напряму, без необхідності проходження через центральний хаб.

Використання протоколів, таких як Zigbee, Z-Wave, Bluetooth та Wi-Fi.

3. Масштабованість:

- Додавання нових пристроїв до системи не вимагає значних змін в існуючій інфраструктурі.

Система легко розширюється, що робить її придатною для великих будинків або комплексів.

4. Висока надійність і стійкість до збоїв:

Відсутність єдиної точки відмови (central point of failure), оскільки кожен пристрій може продовжувати працювати незалежно.

Зменшення ризику втрати функціональності у випадку виходу з ладу окремого компонента.

Приклади децентралізованої архітектури:

1. Philips Hue:

Розумна система освітлення, де кожна лампа та перемикач можуть спілкуватися напряму за допомогою протоколу Zigbee.

Детальніше: Philips Hue [18]



Рисунок 2.16 - Philips Hue

2. Lutron Caseta Wireless:

Система керування освітленням, де перемикачі та димери можуть взаємодіяти напряду через протокол Clear Connect.

Детальніше: Lutron Caseta Wireless [19]



Рисунок 2.17 - Lutron Caseta Wireless

3. Sonos:

Бездротова аудіосистема, де кожен динамік може працювати незалежно та обмінюватися даними з іншими динаміками у мережі.

Детальніше: Sonos [20]



Рисунок 2.18 - Sonos

Переваги децентралізованої архітектури:

- Гнучкість: Легко адаптується до змін і розширення.
- Надійність: Стійка до збоїв окремих компонентів.
- Сумісність: Може інтегрувати різні пристрої від різних виробників.
- Приватність: Місцеве оброблення даних може підвищити конфіденційність.

Децентралізована архітектура розумного будинку є привабливим варіантом для тих, хто цінує гнучкість, надійність та можливість масштабування системи з мінімальними зусиллями.

2.2.2 Централізована архітектура

Централізована архітектура розумного будинку передбачає наявність центрального хабу або контролера, який виступає як основний координаційний вузол для всіх пристроїв у системі. У цій архітектурі всі сенсори, актуатори та інші пристрої підключаються до центрального хабу, який управляє їхньою роботою, обробляє дані та виконує команди користувача.

Основні особливості централізованої архітектури:

1. Центральний контролер:

Головний елемент системи, який відповідає за обробку даних, управління пристроями та забезпечення взаємодії між ними.

Центральний контролер може бути окремим пристроєм або сервером, який виконує функції хабу.

2. Єдина точка управління:

Усі команди та налаштування здійснюються через центральний хаб, що забезпечує зручність у користуванні.

Централізований контроль дозволяє легко інтегрувати нові пристрої та керувати всіма компонентами системи з одного інтерфейсу.

3. Взаємодія між пристроями:

Пристрої можуть обмінюватися даними через центральний хаб, що дозволяє координувати їхні дії.

Хаб може підтримувати різні протоколи зв'язку, такі як Zigbee, Z-Wave, Wi-Fi, Bluetooth, що забезпечує сумісність з широким спектром пристроїв.

4. Управління автоматизацією:

Центральний контролер може налаштовувати сценарії автоматизації, які виконуються при певних умовах (наприклад, вмикання освітлення при виявленні руху).

Це дозволяє створювати складні сценарії взаємодії між пристроями для підвищення комфорту та безпеки.

Приклади централізованої архітектури:

1. Samsung SmartThings Hub:

Центральний хаб, який підтримує різні протоколи (Zigbee, Z-Wave, Wi-Fi) і дозволяє керувати розумними пристроями через одну платформу.

Детальніше: Samsung SmartThings [7]

2. Apple HomeKit:

Платформа, що використовує центральний контролер (наприклад, Apple TV або HomePod) для керування розумними пристроями через додаток Home.

Детальніше: Apple HomeKit [21]



Рисунок 2.19 – HomeKit

3. Google Nest Hub:

Центральний пристрій з дисплеєм, який дозволяє керувати розумними пристроями, використовувати голосові команди через Google Assistant і створювати сценарії автоматизації.

Детальніше: Google Nest Hub [9]

4. Amazon Echo Plus:

Смарт-динамік з вбудованим хабом, який підтримує управління розумними пристроями через голосові команди за допомогою Alexa.

Детальніше: Amazon Echo Plus [9]

Переваги централізованої архітектури:

- *Уніфіковане управління:* Зручність управління всіма пристроями через єдину платформу.
- *Інтеграція:* Легкість інтеграції нових пристроїв та створення складних сценаріїв автоматизації.

- *Безпека:* Центральний контролер може забезпечувати додатковий рівень безпеки та шифрування даних.

Недоліки централізованої архітектури:

- *Єдина точка відмови:* Вихід з ладу центрального контролера може призвести до втрати функціональності всієї системи.

- *Витрати:* Центральний контролер може бути дорогим компонентом системи.

- *Залежність від інтернету:* У деяких випадках для роботи системи необхідне постійне підключення до інтернету.

Централізована архітектура є популярним вибором для створення розумних будинків, оскільки забезпечує зручність управління та широкі можливості автоматизації, проте потребує надійного центрального контролера для стабільної роботи системи.

2.2.3 Гібридна архітектура

Гібридна архітектура розумного будинку поєднує елементи як централізованої, так і децентралізованої архітектур, створюючи систему, яка має переваги обох підходів. В такій архітектурі використовуються центральний хаб або контролер для координації і управління, але також дозволяється автономність і взаємодія між окремими пристроями без обов'язкового проходження через центральний вузол.

Основні особливості гібридної архітектури:

1. Комбінація автономності та централізованого управління:

Пристрої можуть працювати незалежно один від одного та спілкуватися напряму.

Центральний хаб використовується для загального управління, моніторингу і координації роботи всієї системи.

2. Гнучкість і масштабованість:

Легко додавати нові пристрої та розширювати систему без значних змін в існуючій інфраструктурі.

Можливість адаптуватися до змінних умов і вимог користувача.

3. Підвищена надійність і стійкість до збоїв:

Пристрої можуть продовжувати працювати незалежно у випадку виходу з ладу центрального контролера.

Відсутність єдиної точки відмови зменшує ризик повного відключення системи.

4. Оптимізація продуктивності:

Завдання можуть бути розподілені між центральним контролером і автономними пристроями для оптимізації використання ресурсів.

Централізований контроль для складних сценаріїв та аналітики, а автономність для простих, повторюваних завдань.

Приклади гібридної архітектури:

1. Google Nest Ecosystem:

Використовує центральні пристрої (наприклад, Nest Hub) для управління і координації, але окремі пристрої (наприклад, термостати, датчики) можуть працювати автономно та обмінюватися даними напрямку.

Детальніше: Google Nest [9]

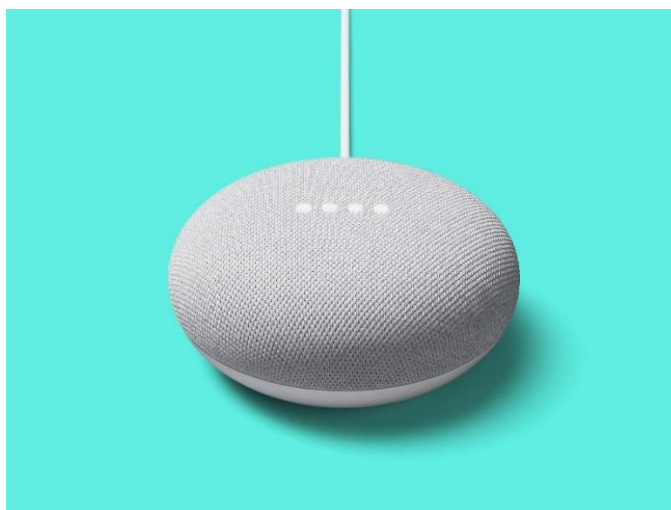


Рисунок 2.21 - Google Nest Hub

2. Samsung SmartThings:

Центральний хаб використовується для координації пристроїв, але багато з них (наприклад, світильники, розетки) можуть працювати автономно і взаємодіяти напрямку.

Детальніше: Samsung SmartThings [7]

3. Home Assistant:

Відкрита платформа, яка може працювати як центральний контролер, але також дозволяє автономність пристроїв і використання локальних мереж для прямого обміну даними.

Детальніше: Home Assistant [21]

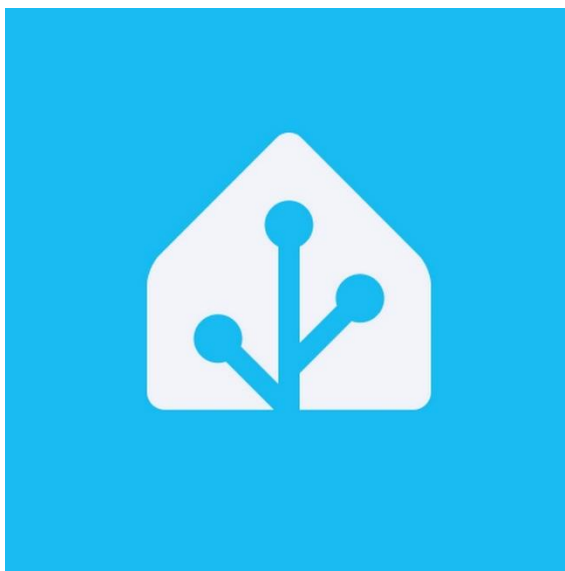


Рисунок 2.22 - Home Assistant

Переваги гібридної архітектури:

- *Гнучкість:* Можливість адаптуватися до різних вимог і умов експлуатації.
- *Надійність:* Висока стійкість до збоїв завдяки поєднанню централізованого і децентралізованого підходів.
- *Масштабованість:* Легке розширення системи з мінімальними зусиллями.

- *Оптимізація*: Баланс між централізованим контролем і автономністю пристроїв дозволяє оптимізувати продуктивність.

Недоліки гібридної архітектури:

- *Складність налаштування*: Може вимагати більше часу і зусиль для початкового налаштування і конфігурації.

- *Витрати*: Можливі вищі початкові витрати на придбання центрального контролера та автономних пристроїв.

- *Сумісність*: Потреба забезпечення сумісності між різними пристроями і протоколами.

Гібридна архітектура розумного будинку є оптимальним варіантом для тих, хто прагне поєднати переваги централізованого управління і автономності пристроїв, забезпечуючи високу гнучкість, надійність та масштабованість системи.

2.3 Протоколи зв'язку в системах розумного будинку

Протоколи зв'язку є основою для забезпечення ефективної взаємодії між пристроями в системах розумного будинку. Вони визначають, як пристрої обмінюються даними, і впливають на надійність, енергоефективність, безпеку та масштабованість системи. Розглянемо найпоширеніші протоколи зв'язку в системах розумного будинку: Zigbee, Z-Wave, Wi-Fi та Bluetooth.

2.3.1 Zigbee, Z-Wave, Wi-Fi, Bluetooth

Zigbee

Огляд:

Zigbee – це бездротовий протокол зв'язку, створений спеціально для додатків з низьким енергоспоживанням, що вимагають тривалої роботи пристроїв

на батареях. Використовується переважно в системах автоматизації будинків, охоронних системах, моніторингу здоров'я та управлінні освітленням.

Основні характеристики:

- Частота: 2.4 GHz (глобально), 868 MHz (Європа), 915 MHz (США).
- Швидкість передачі даних: До 250 kbps.
- Дальність: До 100 м (залежить від умов середовища).
- Топологія мережі: Зірка, дерево, mesh (мережа з вузлами).
- Енергоспоживання: Дуже низьке.
- Підтримка пристроїв: До 65 000 в мережі.
- Застосування: Розумні лампи (Philips Hue), системи безпеки, розумні вимикачі.

Детальніше: Zigbee Alliance [22]

Z-Wave

Огляд:

Z-Wave – це ще один бездротовий протокол зв'язку, розроблений спеціально для розумних будинків і автоматизації будівель. Він забезпечує надійну і безпечну комунікацію між пристроями з низьким енергоспоживанням.

Основні характеристики:

- Частота: 908.42 MHz (США), 868.42 MHz (Європа), різні частоти в інших регіонах.
- Швидкість передачі даних: До 100 kbps.
- Дальність: До 30 м в приміщенні, до 100 м на відкритому просторі.
- Топологія мережі: Mesh.
- Енергоспоживання: Дуже низьке.
- Підтримка пристроїв: До 232 в мережі.
- Застосування: Розумні замки, сенсори руху, розумні термостати.

Детальніше: Z-Wave Alliance [23]

Wi-Fi

Огляд:

Wi-Fi – один з найпоширеніших протоколів бездротового зв'язку, який забезпечує високу швидкість передачі даних і великий радіус дії. Використовується в широкому спектрі пристроїв, включаючи розумні будинки, побутову електроніку, комп'ютери та смартфони.

Основні характеристики:

- Частота: 2.4 GHz і 5 GHz.
- Швидкість передачі даних: До 9.6 Gbps (Wi-Fi 6).
- Дальність: До 100 м (залежить від умов середовища і стандарту).
- Топологія мережі: Зірка.
- Енергоспоживання: Високе (порівняно з Zigbee і Z-Wave).
- Підтримка пристроїв: Теоретично необмежено.
- Застосування: Відеокамери, смарт-телевізори, розумні розетки.

Детальніше: Wi-Fi Alliance [24]

Bluetooth

Огляд:

Bluetooth – бездротовий протокол зв'язку, призначений для короткодістанційного обміну даними між пристроями. Використовується в різноманітних пристроях, від навушників і колонок до фітнес-трекерів і розумних годинників.

Основні характеристики:

Частота: 2.4 GHz.

Швидкість передачі даних: До 3 Mbps (Bluetooth 4.2), до 2 Mbps (Bluetooth 5.0).

Дальність: До 100 м (Bluetooth 5.0).

Топологія мережі: Зірка, точка-точка, mesh (з Bluetooth 5.0).

Енергоспоживання: Низьке (особливо з Bluetooth Low Energy).

Підтримка пристроїв: До 7 активних з'єднань одночасно.

Застосування: Смарт-годинники, навушники, фітнес-трекери, розумні дверні замки.

Детальніше: Bluetooth SIG [25]

Переваги та недоліки протоколів

Zigbee:

- Переваги: Низьке енергоспоживання, висока масштабованість, mesh-топологія.
- Недоліки: Відносно невелика дальність дії, потребує спеціального хабу.

Z-Wave:

- Переваги: Низьке енергоспоживання, надійність, mesh-топологія.
- Недоліки: Обмежена кількість пристроїв у мережі, потребує спеціального хабу.

Wi-Fi:

- Переваги: Висока швидкість передачі даних, велика дальність дії, широка підтримка пристроїв.
- Недоліки: Високе енергоспоживання, потенційні проблеми з перевантаженням мережі.

Bluetooth:

- Переваги: Низьке енергоспоживання (Bluetooth LE), простота використання, широкий спектр пристроїв.
- Недоліки: Обмежена дальність дії, обмежена кількість з'єднань.

Розуміння характеристик і особливостей різних протоколів зв'язку допомагає вибрати найкращий варіант для конкретних додатків в системах розумного будинку, забезпечуючи оптимальну продуктивність, надійність і енергоефективність.

2.3.2 Порівняльний аналіз протоколів

Порівняємо основні характеристики та переваги протоколів Zigbee, Z-Wave, Wi-Fi та Bluetooth, що використовуються в системах розумного будинку:

Таблиця 2.1 - Порівняльна характеристика протоколів Zigbee, Z-Wave, Wi-Fi та Bluetooth

Характеристика	Zigbee	Z-Wave	Wi-Fi	Bluetooth
Частота	2.4 GHz, 868MHz, 915MHz	868.42 MHz (Європа), різні частоти	2.4 GHz, 5GHz	2.4 GHz
Швидкість передачі даних	До 250 kbps	До 100 kbps	До 9.6 Gbps (Wi-Fi 6)	До 3 Mbps (Bluetooth 4.2), До 2 Mbps (Bluetooth 5.0)
Дальність	До 100 м (залежить від умов середовища)	До 30 м (в приміщенні), до 100 м (на відкритому просторі)	До 100 м (залежить від умов середовища і стандарту)	До 100 м (Bluetooth 5.0)
Топологія мережі	Зірка, дерево, mesh	Mesh	Зірка	Зірка, точка-точка, mesh
Енергоспоживання	Дуже низьке	Дуже низьке	Високе	Низьке (особливо з Bluetooth LE)
Підтримка пристроїв	До 65 000 в мережі	До 232 в мережі	Теоретично необмежено	До 7 активних з'єднань одночасно
Застосування	Розумні лампи (Philips Hue), системи безпеки, розумні вимикачі	Розумні замки, сенсори руху, розумні термостати	Відеокамери, смарт-телевізори, розумні розетки	Смарт-годинники, навушники, фітнес-трекери, розумні дверні замки

Підсумуємо:

- Zigbee та Z-Wave - це протоколи з низьким енергоспоживанням, які ідеально підходять для великої кількості розумних пристроїв в будинку. Вони гарантують надійну комунікацію і можуть працювати в мережі типу mesh, що робить їх особливо ефективними в великих будівлях або будинках зі складною конфігурацією.

- Wi-Fi - це протокол з високою швидкістю передачі даних, що підходить для вимогливих додатків, таких як відеоспостереження або стрімінг відео. Однак він має високе енергоспоживання, що може бути неефективним для батарейних пристроїв.

- Bluetooth - це універсальний протокол, який забезпечує низьке енергоспоживання та просту інтеграцію зі смартфонами та іншими персональними пристроями. Він ідеально підходить для переносних розумних пристроїв, таких як фітнес-трекери чи навушники.

При виборі протоколу для системи розумного будинку важливо враховувати конкретні потреби, вимоги до енергоефективності та масштабованості, а також можливості інтеграції з існуючими пристроями та платформами.

2.3.3 Вибір протоколу для конкретних потреб

При виборі протоколу для системи розумного будинку необхідно враховувати конкретні потреби, вимоги та характеристики пристроїв, які будуть використовуватися. Нижче наведено загальні вказівки для вибору протоколу зв'язку в залежності від конкретних потреб:

1. Кількість пристроїв: Якщо вам потрібно підключити велику кількість розумних пристроїв, таких як сенсори, розумні лампи, термостати тощо, протоколи з мережевою топологією типу mesh, такі як Zigbee або Z-Wave, можуть бути кращим варіантом, оскільки вони забезпечують стабільну та надійну комунікацію великої кількості пристроїв.

2. Енергоефективність: Якщо вам потрібно підключити батарейні пристрої або пристрої з обмеженим живленням, такі як датчики руху або дверей, розгляньте протоколи з низьким енергоспоживанням, такі як Zigbee або Bluetooth LE (Low Energy).

3. Швидкість передачі даних: Якщо вам потрібна висока швидкість передачі даних для відеоспостереження або стрімінгу великого обсягу даних, Wi-Fi може бути найкращим варіантом, оскільки він забезпечує високу пропускну здатність.

4. Дальність передачі: Якщо вам потрібна велика дальність передачі сигналу, особливо у великих будинках або на великих ділянках землі, врахуйте, що Zigbee та Z-Wave зазвичай мають кращу проникливість у стіни порівняно з Wi-Fi або Bluetooth.

5. Інтеграція з існуючими пристроями: Переконайтеся, що вибраний протокол підтримує інтеграцію з існуючими розумними пристроями або системами автоматизації, які ви вже використовуєте в своєму будинку.

6. Вартість: Розгляньте вартість як пристроїв, підтримуваних обраною технологією, так і самого обладнання. Деякі протоколи можуть виявитися дорожчими для встановлення та підтримки, ніж інші.

Ретельне вивчення цих факторів допоможе зробити найкращий вибір протоколу для ваших конкретних потреб у системі розумного будинку.

2.4 Висновки по розділу 2

У цьому розділі було розглянуто різні протоколи зв'язку, що використовуються у системах розумного будинку, включаючи Zigbee, Z-Wave, Wi-Fi та Bluetooth. Проведено порівняльний аналіз цих протоколів за основними характеристиками, такими як енергоспоживання, радіус дії, швидкість передачі даних та здатність підтримувати велику кількість підключених пристроїв. Розглянуто питання вибору протоколу для конкретних потреб та сценаріїв

використання, що дозволяє оптимально інтегрувати IoT-рішення в інфраструктуру розумного будинку.

3 ЗАХИСТ РОЗУМНОГО БУДИНКУ НА ОСНОВІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

3.1 Загрози та вразливості в системах розумного будинку

3.1.1 Типи загроз (фізичні, кібернетичні)

У системах розумного будинку існують різні типи загроз, які можуть ставити під загрозу безпеку та приватність власників. Ці загрози можна розділити на фізичні та кібернетичні, кожен з яких має свої характеристики та наслідки.

Фізичні загрози:

1. Неупередженість: Це може включати в себе фізичний доступ до розумного будинку шляхом зламу дверей або вікон.

2. Крадіжка розумних пристроїв: Розумні пристрої можуть стати об'єктом крадіжки, особливо якщо вони не захищені або не зареєстровані в системі безпеки.

3. Фізичні пошкодження: Атакувальники можуть намагатися фізично пошкодити розумні пристрої або інфраструктуру мережі.

Кібернетичні загрози:

1. Віруси та шкідливі програми: Розумні пристрої можуть стати мішенню для вірусів та шкідливих програм, які можуть перешкоджати їхній нормальній роботі або навіть зламувати їх.

2. Несанкціонований доступ до мережі: Атакувальники можуть намагатися здійснити несанкціонований доступ до мережі розумного будинку для отримання конфіденційної інформації або керування пристроями.

3. Перехоплення даних: Несанкціоновані користувачі можуть намагатися перехопити передавані дані між розумними пристроями та хакерськими серверами для використання цих даних у злочинних цілях.

Розуміння цих типів загроз допоможе власникам розумних будинків виявляти потенційні проблеми та приймати заходи для їх запобігання.

3.1.2 Вразливості пристроїв IoT

Пристрої Інтернету речей (IoT) можуть бути підвержені різноманітним вразливостям через їхню специфіку та особливості використання. Ось деякі з найпоширеніших вразливостей:

1. Недостатня аутентифікація та авторизація: Деякі пристрої IoT можуть бути піддаються атакам через недостатньо сильну аутентифікацію користувача або недостатні обмеження доступу.
2. Незахищені мережеві з'єднання: Вразливості у протоколах зв'язку, таких як Wi-Fi або Bluetooth, можуть призвести до несанкціонованого доступу до пристроїв або перехоплення даних.
3. Недостатнє оновлення програмного забезпечення: Відсутність регулярних оновлень програмного забезпечення може залишати пристрої вразливими до вже відомих атак.
4. Збереження конфіденційної інформації: Просте збереження конфіденційних даних на пристроях IoT без захисту може призвести до їхнього витоку в результаті атаки.
5. Недостатнє керування доступом: Недостатні обмеження на доступ до функцій пристроїв можуть призвести до несанкціонованого використання або зламу.
6. Фізичні вразливості: Просте фізичне доступ до пристроїв може дозволити атакувальникам отримати доступ до них та виконати різноманітні атаки.

Розуміння цих вразливостей допомагає власникам пристроїв IoT приймати необхідні заходи для забезпечення безпеки їхнього розумного будинку.

3.1.3 Потенційні наслідки атак

Атаки на системи розумного будинку можуть мати серйозні наслідки як для безпеки, так і для приватності власників. Деякі з потенційних наслідків атак включають:

1. Фізична шкода: Атаки на системи розумного будинку можуть призвести до фізичної шкоди для будівельних конструкцій або пристроїв, зокрема шляхом перекривання електрики або переведення в режим, який може призвести до пожежі.

2. Крадіжка конфіденційних даних: Зламани пристрої можуть бути використані для крадіжки конфіденційної інформації, такої як особисті дані користувачів, плани будинку або графіки руху мешканців.

3. Спостереження за приватним життям: Інтимні дані про поведінку або звички мешканців можуть бути збережені або використані для шантажу або іншої зловживання в результаті атак на розумний будинок.

4. Відмова в обслуговуванні: Атаки можуть призвести до відмови в обслуговуванні розумних пристроїв або систем управління, що може призвести до недоступності деяких функцій або послуг.

5. Віддалене керування системами: Зламани системи можуть бути використані для віддаленого керування системами управління, такими як система опалення або кондиціонування повітря, що може призвести до несподіваних змін у внутрішньому середовищі будинку.

6. Крадіжка або розграбування: Зламани системи безпеки можуть бути використані для відкриття дверей або вікон, що може призвести до крадіжок або розграбувань.

Розуміння цих потенційних наслідків допомагає власникам розумних будинків усвідомлювати загрози та приймати заходи для їх запобігання.

3.2 Методи забезпечення безпеки в IoT

3.2.1 Аутентифікація та авторизація

Аутентифікація та авторизація є критично важливими методами забезпечення безпеки в системах Інтернету речей (IoT). Ці методи дозволяють контролювати доступ до пристроїв та даних, забезпечуючи захист від несанкціонованого доступу.

Аутентифікація — це процес перевірки особи або пристрою, що намагається отримати доступ до системи. Основні методи аутентифікації в IoT включають:

- Паролі: Використання сильних, унікальних паролів для кожного пристрою.
- Біометрія: Використання відбитків пальців, розпізнавання обличчя або голосу.
- Двофакторна аутентифікація (2FA): Використання додаткового рівня перевірки, наприклад, коду, надісланого на мобільний телефон.

Авторизація — це процес визначення прав доступу користувача або пристрою після успішної аутентифікації. Це забезпечує, що користувач або пристрій має лише той рівень доступу, який їм необхідний для виконання своїх функцій.

Приклади методів аутентифікації та авторизації:

1. OAuth: Протокол, що дозволяє стороннім сервісам доступ до ресурсів без передачі пароля. Детальніше про OAuth можна дізнатися на українській сторінці Вікіпедії про OAuth [26]



Рисунок 3.1 - OAuth

2. JWT (JSON Web Tokens): Стандарт, що використовується для передачі інформації між сторонами у безпечний спосіб за допомогою підписаних токенів. Більше інформації на jwt.io [27].

3. SSL/TLS: Використання протоколів безпеки для захисту передачі даних між пристроями. Інформацію про SSL/TLS можна знайти на ssl.com [28].

4. Механізми управління доступом на основі ролей (RBAC): Визначення прав доступу на основі ролей користувачів. Детальніше можна дізнатися на українській сторінці Вікіпедії про RBAC [29].

Впровадження надійних методів аутентифікації та авторизації є важливим кроком для забезпечення безпеки в IoT-системах. Це допомагає захистити пристрої від несанкціонованого доступу та зберегти конфіденційність даних.

3.2.2 Шифрування даних

Шифрування даних є одним із найважливіших методів забезпечення безпеки в системах Інтернету речей (IoT). Воно забезпечує конфіденційність та цілісність даних, переданих між пристроями, зберігаючи їх у зашифрованому вигляді та роблячи їх недоступними для несанкціонованих користувачів.

Основні види шифрування:

1. *Шифрування симетричним ключем:* Використовує один і той самий ключ для шифрування і дешифрування даних. Прикладом є алгоритм AES (Advanced

Encryption Standard). Це швидкий і ефективний метод, але вимагає безпечного зберігання та передачі ключа.

- Переваги: Висока швидкість, ефективність.
- Недоліки: Необхідність безпечної передачі ключа.

2. *Асиметричне шифрування*: Використовує пару ключів – публічний та приватний. Публічний ключ використовується для шифрування, а приватний – для дешифрування. Прикладом є алгоритм RSA.

- Переваги: Високий рівень безпеки, немає потреби в передачі приватного ключа.
- Недоліки: Повільніший процес шифрування та дешифрування порівняно з симетричним шифруванням.

3. *Гібридне шифрування*: Комбінація симетричного та асиметричного шифрування. Симетричний ключ використовується для шифрування даних, а асиметричний ключ – для шифрування симетричного ключа. Це поєднує швидкість симетричного шифрування з безпекою асиметричного.

- Переваги: Баланс між швидкістю та безпекою.
- Недоліки: Ускладнена реалізація.

Протоколи шифрування даних:

1. *TLS (Transport Layer Security)*: Протокол, що забезпечує шифрування даних під час їхньої передачі в Інтернеті. TLS широко використовується для захисту даних у веб-браузерах, електронній пошті, миттєвих повідомленнях та інших протоколах передачі.

Детальніше про TLS можна дізнатися на MDN [30].

2. *IPsec (Internet Protocol Security)*: Протокол, що забезпечує шифрування та автентифікацію на рівні IP для забезпечення безпечного обміну даними в мережі.

Детальніше про IPsec можна дізнатися на Twingate: It's time to ditch your VPN [31].

Рекомендації для шифрування даних в IoT:

- Використовувати сучасні стандарти шифрування (наприклад, AES-256, RSA-2048).

- Забезпечувати регулярне оновлення ключів шифрування.
- Використовувати протоколи безпеки для захисту даних під час передачі.
- Забезпечувати безпечне зберігання ключів шифрування.

Шифрування даних допомагає забезпечити захист конфіденційної інформації в системах IoT, знижуючи ризик перехоплення та несанкціонованого доступу до даних.

3.2.3 Виявлення та запобігання вторгненням

Виявлення та запобігання вторгненням є критично важливими аспектами захисту систем Інтернету речей (IoT). Ці методи допомагають виявити та запобігти несанкціонованим спробам доступу, атак та іншим шкідливим діям.

Системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS) забезпечують моніторинг, аналіз і реагування на підозрілі активності в мережі.

Основні види IDS та IPS:

1. Мережева IDS/IPS (NIDS/NIPS): Моніторять трафік мережі на наявність підозрілих активностей.

NIDS: Виявляє підозрілі активності, аналізуючи мережевий трафік.

NIPS: Активно блокує або запобігає виявленим загрозам.

2. Хостова IDS/IPS (HIDS/HIPS): Встановлюються на окремих пристроях і контролюють їх активність.

HIDS: Виявляє підозрілу активність на конкретному хості.

HIPS: Запобігає атакам на конкретному хості, захищаючи його ресурси.

Методи виявлення вторгнень:

1. Підписне виявлення (Signature-based detection): Використовує базу даних відомих підписів атак для виявлення підозрілої активності.

Переваги: Висока точність виявлення відомих атак.

Недоліки: Неможливість виявлення нових, невідомих атак.

2. Аномалійне виявлення (Anomaly-based detection): Створює модель нормальної поведінки системи і виявляє аномалії, що відхиляються від цієї моделі.

Переваги: Можливість виявлення нових, невідомих атак.

Недоліки: Можливість хибних спрацьовувань (false positives).

3. Гібридне виявлення (Hybrid detection): Поєднує підписне та аномалійне виявлення для більш точного та ефективного виявлення атак.

Переваги: Збалансований підхід, що поєднує переваги обох методів.

Недоліки: Ускладнена реалізація та більша потреба в обчислювальних ресурсах.

Інструменти та ресурси для виявлення та запобігання вторгненням:

1. Snort: Відкрита система виявлення та запобігання вторгненням, що використовує підписне виявлення. Докладніше на сайті CrowdStrike. [32].



Рисунок 3.2 - Snort

2. Suricata: Високопродуктивна система виявлення вторгнень та запобігання з відкритим вихідним кодом, яка підтримує як підписне, так і аномалійне виявлення. Детальніше можна дізнатися на українській сторінці Вікіпедії про Suricata [33].

Приклад захисту розумного будинку з використанням Suricata:

Suricata — це потужний інструмент для виявлення вторгнень та аналізу мережевого трафіку. Ось приклад налаштування Suricata для захисту розумного будинку.

Кроки:

1. Встановлюємо Suricata:

```
``python
import os
# Оновлюємо системні репозиторії

os.system("sudo apt update")

# Встановлюємо Suricata

os.system("sudo apt install suricata -y")
```
```

### 2. Налаштовуємо Suricata:

Створимо простий конфігураційний файл для Suricata, щоб він міг моніторити мережу розумного будинку.

```
``python
suricata_config = """
vars:
 address-groups:
 HOME_NET: "[192.168.1.0/24]" # Локальна мережа розумного будинку
outputs:
 - fast:
 enabled: yes
 filename: /var/log/suricata/fast.log
 append: yes

af-packet:
 - interface: eth0
```

```

threads: auto
defrag: yes
cluster-id: 99
cluster-type: cluster_flow
copy-mode: ips
checksum-checks: auto
"""

Записуємо конфігурацію до файлу suricata.yaml
with open("/etc/suricata/suricata.yaml", "w") as file:
 file.write(suricata_config)

Перезапускаємо Suricata для застосування нових налаштувань
os.system("sudo systemctl restart suricata")

```

### 3. Аналізуємо логи Suricata:

Створимо базовий скрипт на Python для аналізу логів Suricata, щоб виявляти підозрілу активність у мережі розумного будинку.

```

``python
log_file = "/var/log/suricata/fast.log"

def analyze_log(file):
 with open(file, 'r') as f:
 for line in f:
 # Аналізуємо лог для виявлення підозрілої активності
 if "ET SCAN" in line:
 print(f"Підозрілий скан виявлено: {line}")
 elif "ET POLICY" in line:
 print(f"Порушення політики виявлено: {line}")
analyze_log(log_file)

```

...

Цей приклад показує основні кроки для встановлення та налаштування Suricata, а також базовий аналіз логів для виявлення підозрілої активності. Suricata може бути налаштована для більш складних сценаріїв та інтеграції з іншими системами моніторингу та аналізу безпеки.

3. OSSEC: Відкрита хостова система виявлення вторгнень, яка забезпечує моніторинг та аналіз активностей на хості. Докладніше на офіційному сайті OSSEC [34].

4. Zeek (раніше відомий як Bro): Потужна платформа для мережевого аналізу, яка також використовується для виявлення вторгнень. Детальніше можна дізнатися на українській сторінці Вікіпедії про Zeek [35].



Рисунок 3.3 – Zeek

*Приклад захисту розумного будинку з використанням Zeek:*

Для захисту розумного будинку можна використовувати Zeek для моніторингу мережевого трафіку і виявлення підозрілої активності. Ось приклад сценарію на Python, який допоможе встановити Zeek і налаштувати його для збору даних з розумного будинку.

*Кроки:*

1. Додаємо репозиторій Zeek:

```
``python
import os
```

```
Додаємо репозиторій Zeek до файлу sources.list
os.system("echo'deb
http://download.opensuse.org/repositories/security:/zeek/xUbuntu_20.04/ /" | sudo tee
/etc/apt/sources.list.d/security:zeek.list")

Завантажуємо та додаємо ключ репозиторію
os.system("curl-fsSL
https://download.opensuse.org/repositories/security:zeek/xUbuntu_20.04/Release.key |
gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/security_zeek.gpg > /dev/null")
Оновлюємо системні репозиторії
os.system("sudo apt update")
...

```

## 2. Встановлюємо Zeek:

```
``python
Встановлюємо Zeek
os.system("sudo apt install zeek -y")
Додаємо шлях до Zeek у PATH
os.system("echo 'export PATH=$PATH:/opt/zeek/bin' >> ~/.bashrc")
os.system("source ~/.bashrc")
...

```

## 3. Налаштовуємо Zeek для моніторингу мережі розумного будинку:

Створимо простий скрипт для налаштування Zeek. Ми визначимо локальну мережу розумного будинку і активуємо необхідні модулі.

```
``python
Створюємо файл для налаштувань локальної мережі
local_net = ""
redef Site::local_nets += {

```

```

192.168.1.0/24, # Приклад локальної мережі розумного будинку
};
"""

Записуємо налаштування до файлу local.zeeb
with open("/opt/zeek/share/zeek/site/local.zeeb", "a") as file:
 file.write(local_net)

Запускаємо Zeek
os.system("sudo zeekctl deploy")
'''

```

#### 4. Створюємо базовий скрипт на Python для аналізу логів Zeek:

```

``python
import json

Шлях до логу
log_file = "/opt/zeek/logs/current/conn.log"
def analyze_log(file):
 with open(file, 'r') as f:
 for line in f:
 if line.startswith('#'):
 continue
 log_entry = json.loads(line)
 # Аналізуємо лог для виявлення підозрілої активності
 if log_entry.get("id.resp_p") == 22 and log_entry.get("proto") == "tcp":
 print(f"Підозрілий доступ до SSH: {log_entry}")
analyze_log(log_file)

```

...

Цей простий приклад допоможе налаштувати та використовувати Zeek для моніторингу мережевого трафіку в розумному будинку. Звичайно, реальні сценарії можуть вимагати більш складних налаштувань і аналізу, але цей приклад показує основні кроки для початку роботи.

*Рекомендації для виявлення та запобігання вторгненням в IoT:*

- Впроваджувати IDS та IPS для постійного моніторингу мережевого трафіку та активностей пристроїв.
- Регулярно оновлювати бази даних підписів атак для підвищення ефективності підписного виявлення.
- Використовувати аномалійне виявлення для ідентифікації нових та невідомих загроз.
- Інтегрувати системи виявлення та запобігання вторгненням з іншими засобами кібербезпеки для комплексного захисту.

Виявлення та запобігання вторгненням є важливими складовими безпеки IoT-систем, які допомагають забезпечити захист від несанкціонованих доступів та атак, зберігаючи цілісність та конфіденційність даних.

### 3.3 Інструменти та технології для захисту розумного будинку

#### 3.3.1 Системи управління безпекою

Системи управління безпекою є ключовим елементом для забезпечення комплексного захисту розумного будинку. Вони інтегрують різні компоненти безпеки, такі як камери спостереження, датчики руху, дверні замки та інші пристрої, забезпечуючи координацію та управління їхньою роботою через єдину платформу.

*Основні компоненти систем управління безпекою:*

1. *Центральний контролер (хаб):* Центральний пристрій, який керує всіма іншими компонентами системи безпеки, забезпечуючи їхню взаємодію та обробку даних.

Приклад: Samsung SmartThings [7]

2. *Камери спостереження:* Відеокамери, які забезпечують моніторинг території навколо будинку та всередині приміщень. Вони можуть мати функції запису, розпізнавання обличчя та передачі відео в реальному часі.

Приклад: Nest Cam [36]

3. *Датчики руху та відкриття дверей/вікон:* Пристрої, які виявляють рух або відкриття дверей та вікон, передаючи сигнал про можливе вторгнення до центрального контролера.

Приклад: Philips Hue Motion Sensor [1]

4. *Розумні замки:* Електронні замки, які можна відкривати та закривати дистанційно за допомогою смартфона або іншого пристрою, забезпечуючи контроль доступу до будинку.

5. *Сигналізаційні системи:* Аудіо- та візуальні сигнали, які спрацьовують у разі виявлення загрози, попереджаючи мешканців будинку та сусідів про потенційну небезпеку.

Приклад: Ring Alarm [38]

*Функції систем управління безпекою:*

1. *Моніторинг в реальному часі:* Системи управління безпекою надають можливість спостерігати за подіями в реальному часі через мобільні додатки або веб-інтерфейси.

2. *Автоматичні сповіщення:* У разі виявлення підозрілої активності система надсилає сповіщення на смартфон або інші пристрої користувача.

3. *Інтеграція з іншими системами розумного будинку:* Системи управління безпекою можуть інтегруватися з іншими пристроями, такими як розумне освітлення, термостати та інші сенсори, для автоматичного реагування на загрози.

4. Віддалений доступ та управління: Користувачі можуть віддалено керувати своїми системами безпеки через інтернет, що дозволяє оперативно реагувати на загрози навіть за межами будинку.

5. Запис та зберігання даних: Камери спостереження та інші пристрої можуть записувати відео та інші дані, зберігаючи їх для подальшого аналізу та доказів у разі інциденту.

Системи управління безпекою є невід'ємною частиною сучасних розумних будинків, забезпечуючи захист мешканців та їхнього майна від різних загроз.

### 3.3.2 Використання блокчейну для безпеки IoT

Блокчейн є перспективною технологією для підвищення безпеки в системах Інтернету речей (IoT). Вона забезпечує децентралізований, незмінний і прозорий спосіб зберігання та передачі даних, що робить її ідеальним рішенням для захисту мереж IoT від різних загроз.

*Основні переваги використання блокчейну для безпеки IoT:*

1. *Децентралізація:* Блокчейн усуває потребу в центральному контролері, розподіляючи управління мережею між всіма учасниками. Це знижує ризик атак на центральний вузол і підвищує загальну стійкість системи.

Decentralized Network [39]



Рисунок 3.4 - Decentralized Network

2. *Незмінність*: Дані, записані в блокчейні, не можуть бути змінені або видалені. Це забезпечує високий рівень захисту від несанкціонованого втручання і маніпуляцій з даними.

3. *Прозорість та відстежуваність*: Усі транзакції в блокчейні прозорі та можуть бути перевірені будь-яким учасником мережі. Це сприяє підвищенню довіри між учасниками та забезпечує можливість відстеження кожної транзакції.

4. *Безпека*: Блокчейн використовує криптографічні методи для захисту даних, що забезпечує високий рівень безпеки проти різних типів атак, включаючи підробку даних і несанкціонований доступ.

#### *Застосування блокчейну для захисту IoT:*

1. *Автентифікація та управління доступом*: Блокчейн може використовуватися для автентифікації пристроїв і управління доступом у мережі IoT. Кожен пристрій має унікальний криптографічний ключ, який зберігається в блокчейні, забезпечуючи надійну автентифікацію.

2. *Автентифікація в блокчейні здійснюється за допомогою криптографії, забезпечуючи безпеку та надійність верифікації пристроїв. Ось як цей процес зазвичай працює:*

#### *1. Криптографічні ключі*

- *Приватний ключ*: Це секретний ключ, який використовується для підписання транзакцій або повідомлень. Він повинен зберігатися в таємниці і не бути доступним іншим особам.

- *Публічний ключ*: Це відкритий ключ, який використовується для перевірки підписів, зроблених приватним ключем. Публічний ключ може бути доступний всім.

#### *2. Процес автентифікації*

##### *1. Створення ключів:*

Кожен пристрій генерує пару криптографічних ключів (приватний і публічний ключ).

##### *2. Зберігання ключів:*

Публічний ключ зберігається в блокчейні, де він доступний для всіх учасників мережі.

Приватний ключ зберігається на пристрої і використовується для підписання транзакцій.

### 3. Підписання транзакцій:

Коли пристрій хоче виконати певну дію або комунікувати з іншим пристроєм, він підписує транзакцію або повідомлення своїм приватним ключем.

### 4. Перевірка підпису:

Інші учасники мережі використовують публічний ключ, збережений у блокчейні, для перевірки підпису. Це дозволяє їм переконатися, що транзакція або повідомлення дійсно походить від власника приватного ключа.

### 5. Запис у блокчейн:

Після успішної перевірки транзакція записується в блокчейн, створюючи незмінний запис автентифікованої дії.

### *Переваги автентифікації за допомогою блокчейну*

Децентралізація: Блокчейн не потребує централізованого серверу для управління ключами, що зменшує ризик єдиної точки відмови.

Безпека: Використання криптографічних ключів забезпечує високий рівень безпеки автентифікації.

Прозорість: Усі транзакції та їх перевірки зберігаються у блокчейні, що дозволяє легко аудіювати та перевіряти автентичність дій.

Автентифікація на основі блокчейну є потужним інструментом для забезпечення безпеки в мережах IoT, особливо коли необхідно забезпечити надійну ідентифікацію та верифікацію великої кількості пристроїв.

2. *Захист даних та конфіденційність*: Дані, зібрані з пристроїв IoT, можуть бути зашифровані та зберігатися в блокчейні. Це забезпечує високий рівень захисту конфіденційності даних і гарантує, що дані не можуть бути змінені або видалені.

3. *Управління оновленнями програмного забезпечення*: Блокчейн може використовуватися для безпечного управління оновленнями програмного

забезпечення пристроїв IoT. Кожне оновлення записується в блокчейн, що забезпечує прозорість і безпеку процесу оновлення.

4. *Контроль цілісності даних:* Блокчейн дозволяє перевіряти цілісність даних, забезпечуючи захист від маніпуляцій і підробки. Це особливо важливо для критичних додатків IoT, таких як розумні міста та промислові системи.

*Приклади використання блокчейну для захисту IoT:*

Одним із прикладів використання блокчейну для захисту Інтернету речей (IoT) є проект, реалізований IBM та корейською компанією Hyundai. Вони спільно розробили блокчейн-платформу для підвищення безпеки автомобілів, які підключені до інтернету.

Ця платформа використовує блокчейн для автентифікації та управління доступом до автомобілів, що дозволяє захищати транспортні засоби від несанкціонованого доступу. Кожен автомобіль має унікальний криптографічний ключ, який зберігається в блокчейні. Це забезпечує надійну автентифікацію та підтвердження справжності кожного автомобіля, підключеного до системи.

Блокчейн також використовується для запису всіх транзакцій та дій, що виконуються автомобілем, на незмінний цифровий реєстр. Це дозволяє створити прозору історію всіх подій, пов'язаних з транспортним засобом, включаючи технічне обслуговування, ремонт та використання послуг.

Цей підхід забезпечує підвищений рівень безпеки та прозорості, знижуючи ризик кібератак та шахрайства. Він також дозволяє автоматизувати та спростити процеси взаємодії між автомобілем та іншими сервісами, такими як зарядні станції для електромобілів, паркувальні місця та платні дороги.

Такий приклад використання блокчейну в IoT демонструє, як ці технології можуть бути інтегровані для підвищення безпеки та ефективності систем розумних пристроїв.

*Рекомендації щодо впровадження блокчейну в IoT-системи:*

- Вибирайте блокчейн-платформи, що забезпечують високу масштабованість і продуктивність.

- Забезпечуйте інтеграцію блокчейну з існуючими IoT-системами та протоколами.
- Використовуйте криптографічні методи для захисту даних і автентифікації пристроїв.
- Регулярно оновлюйте блокчейн-мережу для захисту від нових загроз і вразливостей.
- Забезпечуйте прозорість і контроль доступу до блокчейну для всіх учасників мережі.

Використання блокчейну для безпеки IoT дозволяє значно підвищити захист даних і пристроїв, забезпечуючи надійну та прозору мережу для сучасних розумних будинків і інших систем IoT.

### 3.3.3 Моніторинг та управління загрозами

Моніторинг та управління загрозами є критично важливими компонентами для забезпечення безпеки систем розумного будинку на основі технологій Інтернету речей (IoT). Ефективне виявлення, реагування та усунення загроз допомагає запобігти потенційним атакам та мінімізувати їхні наслідки.

*Основні аспекти моніторингу та управління загрозами в IoT:*

1. *Моніторинг мережі в реальному часі:* Постійний моніторинг мережевого трафіку допомагає виявляти підозрілі активності та аномалії, які можуть свідчити про спроби несанкціонованого доступу або атаки на систему.

Приклад: Splunk [40]

2. *Використання систем виявлення та запобігання вторгненням (IDS/IPS):* IDS/IPS системи аналізують мережевий трафік та події на наявність відомих загроз і аномалій, що допомагає оперативно реагувати на потенційні атаки.

Приклад: Snort [32]

3. *Аналіз поведінки пристроїв:* Використання алгоритмів машинного навчання для аналізу поведінки пристроїв IoT дозволяє виявляти відхилення від нормального функціонування, які можуть свідчити про компрометацію пристрою.

Приклад: Darktrace [41]

4. *Інформаційна безпека та управління подіями (SIEM)*: SIEM платформи збирають, аналізують та корелюють дані з різних джерел для виявлення та реагування на загрози в режимі реального часу.

Приклад: IBM QRadar [42]

5. *Використання Threat Intelligence*: Інформація про нові загрози та вразливості, отримана з різних джерел, дозволяє швидко адаптувати захисні заходи та підвищити ефективність моніторингу загроз.

Приклад: FireEye Threat Intelligence [43]

*Рекомендації щодо впровадження моніторингу та управління загрозами:*

1. *Інтеграція багаторівневого захисту*: Використовуйте комбінацію різних засобів захисту, таких як IDS/IPS, SIEM, та системи аналізу поведінки, для забезпечення багаторівневого захисту.

2. *Автоматизація процесів*: Використовуйте автоматизовані системи для збору, аналізу та реагування на загрози. Це допоможе швидко виявляти та нейтралізувати загрози з мінімальним втручанням людини.

3. *Постійне оновлення системи*: Регулярно оновлюйте програмне забезпечення та бази даних загроз для забезпечення актуальності захисних механізмів.

4. *Тестування та оцінка безпеки*: Проводьте регулярні аудити безпеки, пенетраційні тестування та оцінки вразливостей для виявлення слабких місць у системі.

5. *Підготовка та навчання персоналу*: Забезпечте належну підготовку та навчання персоналу щодо методів виявлення та реагування на загрози. Підвищення обізнаності користувачів про потенційні загрози є ключовим аспектом забезпечення безпеки.

6. *Інформаційна взаємодія*: Співпрацюйте з іншими організаціями та обмінюйтеся інформацією про загрози для покращення колективного захисту

*Приклади реалізації:*

1. *Cisco Talos*: Cisco Talos надає інформацію про загрози та допомагає у виявленні та нейтралізації атак на мережі IoT.

Cisco Talos [44]

2. *Armis*: Armis пропонує комплексні рішення для захисту пристроїв IoT, включаючи моніторинг, виявлення та реагування на загрози.

Armis [45]

Моніторинг та управління загрозами є важливою складовою захисту розумних будинків, забезпечуючи надійний захист від сучасних кіберзагроз і знижуючи ризики компрометації систем IoT.

### 3.4 Висновки до розділу 3

Цей розділ присвячено питанням безпеки в системах розумного будинку, побудованих на основі технологій IoT. Розглянуто типи загроз та вразливостей, що можуть виникати, а також їх потенційні наслідки. Представлено сучасні інструменти та технології для захисту розумного будинку, включаючи системи управління безпекою та використання блокчейну. Показано, як ці методи сприяють захисту даних і підвищенню загальної безпеки IoT-систем.

## ВИСНОВКИ

### *Основні висновки роботи*

Були проаналізовані сучасні підходи до захисту розумних будинків на основі технологій Інтернету речей (IoT). В результаті дослідження було визначено основні компоненти розумного будинку, архітектурні моделі, протоколи зв'язку та методи забезпечення безпеки. Особлива увага була приділена виявленню загроз та вразливостей IoT пристроїв, а також методам їх захисту.

### *Узагальнення отриманих результатів дослідження*

Було виявлено, що розумні будинки стикаються з широким спектром загроз, як фізичних, так і кібернетичних. Вразливості пристроїв IoT можуть мати серйозні наслідки, включаючи компрометацію конфіденційних даних і порушення роботи систем. Проте, впровадження методів аутентифікації, шифрування даних, виявлення та запобігання вторгненням значно підвищує рівень безпеки.

### *Висновки щодо ефективності застосування технологій IoT для захисту розумного будинку*

Застосування технологій IoT в розумних будинках є ефективним для підвищення комфорту, енергоефективності та безпеки. Використання блокчейну, систем моніторингу та управління загрозами дозволяє значно знизити ризики несанкціонованого доступу та кібератак. Проте, необхідно забезпечити постійне оновлення та вдосконалення захисних механізмів для підтримання високого рівня безпеки.

### *Внесок в науку і практику та значення проведеного дослідження для теорії та практики*

Проведене дослідження робить вагомий внесок у розуміння архітектури та безпеки розумних будинків на основі IoT. Теоретичні знання про вразливості та методи захисту можуть бути використані для подальшого розвитку технологій безпеки. Практичні рекомендації щодо впровадження захисних механізмів можуть бути використані при розробці та експлуатації розумних будинків.

*Можливість використання отриманих результатів у реальних умовах*

Отримані результати можуть бути застосовані для підвищення безпеки розумних будинків в реальних умовах. Рекомендації щодо використання блокчейну, систем моніторингу та управління загрозами можуть бути впроваджені для захисту приватних і комерційних розумних будинків.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Motion sensor [Електронний ресурс] URL: <https://www.philips-hue.com/en-us/p/hue-motion-sensor/046677570972> (дата звернення: 07.06.2024)
2. Бездротовий датчик температури і вологості Xiaomi Mijia Temperature [Електронний ресурс] URL: <https://homehub.com.ua/datchiki-temperature/xiaomi-mijia-temperature-and-humidity-ytc4018cn.html> (дата звернення: 07.06.2024)
3. Smart Home light control [Електронний ресурс] URL: <https://www.bosch-smarthome.com/uk/en/products/devices/light-control/> (дата звернення: 07.06.2024)
4. Nest Protect [Електронний ресурс] URL: [https://store.google.com/gb/product/nest\\_protect\\_2nd\\_gen?hl=en-GB](https://store.google.com/gb/product/nest_protect_2nd_gen?hl=en-GB) (дата звернення: 07.06.2024)
5. Caséta by Lutron [Електронний ресурс] URL: <https://www.casetawireless.com/us/en> (дата звернення: 07.06.2024)
6. HoneywellHome [Електронний ресурс] URL: <https://www.honeywellhome.com/us/en/products/air/thermostats/wifi-thermostats/t9-smart-thermostat-with-sensor-rcht9610wfs2003-u/> (дата звернення: 07.06.2024)
7. Samsung Unveils SmartThings Station [Електронний ресурс] URL: <https://news.samsung.com/global/samsung-unveils-smarthings-station-at-ces-2023-making-smarter-homes-accessible-for-all> (дата звернення: 07.06.2024)
8. Amazon Echo Plus [Електронний ресурс] URL: <https://www.techradar.com/reviews/amazon-echo-plus-review> (дата звернення: 07.06.2024)
9. Nest Hub [Електронний ресурс] URL: [https://store.google.com/us/product/google\\_nest\\_hub](https://store.google.com/us/product/google_nest_hub) (дата звернення: 07.06.2024)
10. HomePod mini [Електронний ресурс] URL: <https://www.apple.com/homepod-mini/> (дата звернення: 07.06.2024)
11. Home center 3 [Електронний ресурс] URL: <https://www.fibaro.com/en/products/home-center-3/> (дата звернення: 07.06.2024)

12. Hubitat Elevation Model C-8 Pro [Електронний ресурс] URL: <https://hubitat.com/> (дата звернення: 07.06.2024)
13. Smarter life with SmartThings [Електронний ресурс] URL: <https://www.samsung.com/global/galaxy/apps/smarthings/> (дата звернення: 07.06.2024)
14. Home Center 3 [Електронний ресурс] URL: <https://manuals.fibaro.com/home-center-3/> (дата звернення: 07.06.2024)
15. Дізнайтеся, що таке Google Assistant [Електронний ресурс] URL: <https://assistant.google.com/> (дата звернення: 07.06.2024)
16. Control4 [Електронний ресурс] URL: <https://www.control4.com/> (дата звернення: 07.06.2024)
17. ПОЧАТОК РОБОТИ З HARMONY ELITE [Електронний ресурс] URL: <https://www.logitech.com/en-us/product/harmony-elite> (дата звернення: 07.06.2024)
18. Розумне освітлення Philips Hue [Електронний ресурс] URL: <https://www.philips-hue.com/en-us> (дата звернення: 07.06.2024)
19. Caséta by Lutron [Електронний ресурс] URL: <https://www.casetawireless.com/> (дата звернення: 07.06.2024)
20. Sonos [Електронний ресурс] URL: <https://www.sonos.com/> (дата звернення: 07.06.2024)
21. Домашній помічник [Електронний ресурс] URL: <https://www.home-assistant.io/> (дата звернення: 07.06.2024)
22. Створення основи та майбутнього IoT [Електронний ресурс] URL: <https://zigbeealliance.org/> (дата звернення: 07.06.2024)
23. Дізнайтеся про технологію Z-Wave [Електронний ресурс] URL: <https://z-wavealliance.org/> (дата звернення: 07.06.2024)
24. Інформація про Wi-Fi [Електронний ресурс] URL: <https://www.wi-fi.org/> (дата звернення: 07.06.2024)
25. Інформація про Bluetooth [Електронний ресурс] URL: <https://www.bluetooth.com/> (дата звернення: 07.06.2024)

26. Що таке Open Authorization [Електронний ресурс] URL: <https://foxminded.ua/oauth-shcho-tse/> (дата звернення: 07.06.2024)
27. Вступ до веб-токенів JSON [Електронний ресурс] URL: <https://jwt.io/introduction> (дата звернення: 07.06.2024)
28. Що таке рукоштовування SSL/TLS? [Електронний ресурс] URL: <https://ssl.com.ua/blog/ukr/what-is-ssl-tls-handshake/> (дата звернення: 07.06.2024)
29. Wikipedia RBAC [Електронний ресурс] URL: [https://uk.wikipedia.org/wiki/Керування\\_доступом\\_на\\_основі\\_ролей](https://uk.wikipedia.org/wiki/Керування_доступом_на_основі_ролей) (дата звернення: 07.06.2024)
30. Безпека транспортного рівня [Електронний ресурс] URL: [https://developer.mozilla.org/en-US/docs/Web/Security/Transport\\_Layer\\_Security](https://developer.mozilla.org/en-US/docs/Web/Security/Transport_Layer_Security) (дата звернення: 07.06.2024)
31. Пес: повний посібник про те, як це працює та як ним користуватися [Електронний ресурс] URL: <https://www.twingate.com/blog/ipsec> (дата звернення: 07.06.2024)
32. ПОЯСНЕННЯ ПРАВИЛ ХРИПАННЯ ТА ХРИПАННЯ [Електронний ресурс] URL: <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/snort-rules/> (дата звернення: 07.06.2024)
33. Wikipedia Suricata [Електронний ресурс] URL: [https://uk.wikipedia.org/wiki/Suricata\\_\(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0\)](https://uk.wikipedia.org/wiki/Suricata_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0)) (дата звернення: 07.06.2024)
34. Atomic OSSEC для розширеного виявлення та реагування (XDR) [Електронний ресурс] URL: <https://www.ossec.net/get-atomic-ossec-for-enterprise/> (дата звернення: 07.06.2024)
35. Wikipedia Zeek [Електронний ресурс] URL: <https://uk.wikipedia.org/wiki/ZeeK> (дата звернення: 07.06.2024)
36. Nest Cam [Електронний ресурс] URL: [https://store.google.com/us/product/nest\\_cam\\_indoor](https://store.google.com/us/product/nest_cam_indoor) (дата звернення: 07.06.2024)

37. August Wi-Fi Smart Lock [Електронний ресурс] URL: <https://august.com/products/august-smart-lock-pro-connect> (дата звернення: 07.06.2024)

38. Домашні системи безпеки [Електронний ресурс] URL: <https://ring.com/alarm> (дата звернення: 07.06.2024)

39. Що таке децентралізована мережа? [Електронний ресурс] URL: <https://www.fool.com/terms/d/decentralized-network/#:~:text=A%20decentralized%20network%20distributes%20information,all%20computing%20for%20a%20network>. (дата звернення: 07.06.2024)

40. Splunk [Електронний ресурс] URL: <https://www.splunk.com/> (дата звернення: 07.06.2024)

41. Перше в галузі комплексне рішення для управління ризиками ОТ [Електронний ресурс] URL: <https://www.darktrace.com/en/products/industrial/> (дата звернення: 07.06.2024)

42. Security intelligence [Електронний ресурс] URL: <https://www.ibm.com/security/security-intelligence/qradar> (дата звернення: 07.06.2024)

43. FireEye NX - захист від загроз нового покоління вступників по Web [Електронний ресурс] URL: <https://bakotech.ua/product/134/> (дата звернення: 07.06.2024)

44. Всередині кампанії крадіжки даних LilacSquid [Електронний ресурс] URL: <https://www.talosintelligence.com/> (дата звернення: 07.06.2024)

45. ARMIS — ЛІДЕР У СФЕРІ ІОТ SECURITY [Електронний ресурс] URL: <https://softprom.com/ua/vendor/armis> (дата звернення: 07.06.2024)