Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній рівень ***магістр***
(назва освітнього рівня)

кваліфікація
(код і назва кваліфікації)

на тему: *Удосконалений метод захисту інформації у кіберфізичних системах*

Виконавець: студент *2* **курсу, групи** *КБм-21*

(підпис) *Васько Кирило Вікторович*
(прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	*Лаптєв О. А.*		
Рецензент	*Ахрамович А.М.*		
Нормоконтроль	*Даков С. Ю.*		

Київ
2022

Міністерство освіти і науки України

Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації

_____ Лукова-Чуйко Н.В.

«_____»_____20___року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту *КБм-21* *Ваську Кирилу Вікторовичу*
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи *Удосконалений метод захисту інформації у кіберфізичних системах*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *Методи захисту інформації в кіберфизичних системах*

Предмет досліджень *Процес захисту інформації IoT–системи «розумний дім».*

Мета *Розробка удосконаленого методу захисту інформації у кіберфізичних системах, на прикладі IoT–системи «розумний дім».*

Вихідні дані для проведення роботи *Методи захисту кіберфізичних систем за допомогою технології blockchain.*

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *удосконалений метод захисту інформації у кіберфізичних системах типа «розумний дім», удосконалення досягнуто шляхом впровадження оптимізованої Blockchain–технології для надійної автентифікації, з використанням бази даних загроз.*

Практична цінність *отримання дієвого уніфікованого алгоритму широкого застосування у кіберфізичних системах.*

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Розробка плану для досягнення мети роботи	29.10.2021 – 11.11.2021
Аналіз літературних джерел	12.11.2021 – 14.01.2022
Розробка методу захисту захисту інформації у кіберфізичних системах «розумний дім»	15.01.2022 – 09.05.2022
Оформлення і друк пояснювальної записки	09.05.2022 – 17.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *Зниження збитків через вразливості IoT систем*

Соціальний ефект *Покращення технологій забезпечення захисту інформації в кіберфізичних системах.*

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Удосконалений метод захисту інформації у кіберфізичних системах»: 107 сторінок, 37 рисунків та 9 таблиць. 100 літературних джерел.

Об’єкт дослідження – методи захисту інформації в кіберфизичних системах.

Мета роботи – розробка удосконаленого методу захисту інформації у кіберфізичних системах, на прикладі IoT–системи «розумний дім».

Методи дослідження – збір, аналіз, систематизація та верифікація розрізнених інформаційних даних з формуванням загальної концепції та відповідних рішень в рамках досліджуваного напрямку кібернетичної безпеки.

В процесі роботи розроблено рішення з удосконалення захисту інформації в IoT–системі «розумний дім»; проведено моделювання кібернетичних загроз; розроблено математичний апарат для моделювання кібернетичних загроз; сформовано рішення з удосконалення захисту інформації в IoT–системі «розумний дім» на базі новітніх методів шифрування службового спілкування елементів досліджуваної кіберфізчиної системи.

Наукова новизна дослідження - удосконалений метод захисту інформації у кіберфізичних системах типа «розумний дім», удосконалення досягнуто шляхом впровадження оптимізованої (за ресурсоємністю механізму) Blockchain–технології для надійної автентифікації, з використанням бази даних загроз, отриманих з найсучасніших верифікованих джерел та найуспішнішого досвіду впровадження відповідних безпекових засобів і рішень з формуванням актуальної на поточний час бази даних стосовного досліджуваного напрямку забезпечення цифрової безпеки.

Практичне значення досліджень базується на отриманні дієвого уніфікованого алгоритму широкого застосування, що передбачає формування доцільної та ефективної архітектури системи моніторингу цифрової безпеки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІР – Інформаційний Ресурс

ІК – Інформаційний Конфлікт

ПЗ – Програмне Забезпечення

СІБ – Система Інформаційної Безпеки

ЧАМ – Числово-Аналітичне Моделювання

ДІМ – Диференційно-Ігрова Модель

IoT – Internet of Things

AI – Artificial Intelligence

BC – BlockChain

PoW – Proof of Work

P2P – Peer-to-Peer

ATP – Acceptance Test Procedure

ICT – Information and Communications Technology

SaaS – Software as a Service

MitM – Man-in-the-Middle

DDoS – Distributed Denial-of-Service

IDS – Intrusion Detection System

STRIDE – Spoofing, Tampering, Disclosure, Information Disclosure, Denial of Service, Elevation of Privilege

PASTA – Process of Attack Simulation and Threat Analysis

OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation

IPFS – InterPlanetary File System

EIB – European Installation Bus

BLE – Bluetooth Low Energy

PIR – Passive InfraRed

DFD – Data Flow Diagram

ВСТУП

Удосконалений метод захисту інформації у кіберфізичних системах, на прикладі IoT–системи «розумний дім».

Актуальність дослідження базується на сучасних тенденціях розвитку, цифровізації та всеохоплюючого глибокого проникнення цифрових технологій у всі сфери життєдіяльності сучасної людини. Будь-яка сфера діяльності людини в певній мірі використовує цифровий інструментарій та цифрові мережі, а деякі галузі взагалі мають в своїй основі стандарти застосування цифрових засобів, без яких не виявляється можливим нормального функціонування зазначених сфер. Поряд зі значним розвитком і прогресом для цифрової сфери також генеруються і цифрові загрози, що, внаслідок значної залежності та глибокої інтеграції кібернетичних систем в нормальні функції різних галузей та рядових інженерних систем супроводу життєзабезпечення, являють собою значний виклик цивілізаційному розвитку та потребують формування та розвитку адекватних системно-безпекових рішень у вигляді відповідних програмних, моніторингових, мережевих засобів.

Питання забезпечення цифрової та кібернетичної безпеки останніми роками є вкрай актуальним для України, що підтверджується відповідними законодавчими ініціативами, такими як Закон України від 21.06.2018 № 2469-VIII [1], Закон України від 05.10.2017 № 2163-VIII [2], Закон України від 16.11.2021 № 1882-IX [3], Закон України від 16.12.2020 № 1089-IX [4] та іншими нормативнивно-реглуляторними документами, що визначають механізми реалізації загальнодержавної Стратегії кібербезпеки України [5].

Враховуючи безпекову ситуацію в України, визначений напрямок дослідження є вкрай актуальним та таким, що потребує досконалого вивчення та розробки відповідних дієвих рішень з впровадження одного з найважливіших принципів системи загальнодержавної безпеки – безпеки цифрових мереж та, зокрема, безпеки IoT–систем.

Одною з провідних сучасних кіберфізичних систем є IoT–система «розумний дім». В досліджені [6], за суміжними показниками установлена динаміка розвитку «розумних» технологій для побутового використання у якості будинкових систем інженерного супроводу життєзабезпечення:

– за останнє п’ятиріччя (2015/2020) рівень профільних наукових праць та публікацій у світовому науковому товаристві щодо розвитку технології кіберфізичної системи «розумний» дім зріс в 2,2 рази (2015 – 1017 од. / 2020 – 2355 од.);

– у досліджуваному періоді найбільше публікацій (59 %) було присвячено огляду функціонування діючих систем «розумного» дому, а найбільше наукових праць (37 %) було присвячено розвитку саме кібернетичної частини забезпечення функціонування «розумних» технологій інженерного супроводу життєзабезпечення у приватних житлах;

– серед пов’язаних релевантних запитів у мережі Інтернет, суміжних з вектором дослідження «розумний» дім (у зазначеному періоді), найчастіше застосовувався пошук понять кіберфізичних систем – інтернету речей (IoT–систем).

Таким чином, дослідження [6] формує загальний вектор розвитку «розумних» технологій починаючи з 2000-х рр. від базового поняття «розумний» дім до «розумне» місто. Варто зазначити, що Україна в цьому векторі розвитку має відповідні успіхи, а саме на державному рівні введені в дію складові частини концепції «розумного» міста: найбільш вживані – за категорією «smart» government – сервіс та додаток «Дія» та категорією «smart» healthcare – сервіс та додаток «Helsi», а також багато інших урядових доробків, що перебувають на етапі тестування та поступового впровадження.

Поруч з розвитком кіберфізичних систем існує вектор розвитку, що має негативне забарвлення – розвиток кібернетичних загроз. Так у дослідженні [7], встановлено, що за оцінками суспільної думки найбільшу загрозу з впровадженням побутових «розумних» систем у межах концепції «розумний»

дім є збільшення залежності від технологій та втрата контролю над цими інженерними мережами супроводу життєзабезпечення.

Таким чином, встановлено, що кіберфізична IoT–система «розумний дім» має значний потенціал до впровадження, розвитку та удосконалення, при актуальному адекватному розвитку систем кіберзахисту та убезпечення побутових «розумних» систем інженерного супроводу життєзабезпечення.

Об’єкт дослідження – методи захисту інформації в кіберфизичних системах.

Предмет дослідження – процес захисту інформації IoT–системи «розумний дім».

Мета дослідження – розробка удосконаленого методу захисту інформації у кіберфізичних системах, на прикладі IoT–системи «розумний дім».

Задачі дослідження:

– аналіз функціонування IoT системи (кіберфізичної системи) «розумний дім»: концепція та загальна схема реалізації IoT–системи «розумний дім»; устаткування та прилади; аналіз кібернетичних загроз для IoT–системи «розумний дім»;

– розробка рішень з удосконалення захисту інформації в IoT–системі (кіберфізічній системі) «розумний дім»; моделювання кібернетичних загроз; розробка математичного апарату для моделювання кібернетичних загроз; формування рішення з удосконалення захисту інформації в IoT–системі «розумний дім» на базі новітніх методів шифрування службового спілкування елементів досліджуваної кіберфізчиної системи;

– оцінка ефективності удосконаленого методу захисту інформації в IoT–системі (кіберфізічній системі) «розумний дім»: визначення показників оцінювання; алгоритмування методів визначення ефективних засобів захисту; визначення показників ефективності та розробка пропозицій до впровадження.

Методи дослідження – збір, аналіз, систематизація та верифікація розрізнених інформаційних даних з формуванням загальної концепції та відповідних рішень в рамках досліджуваного напрямку кібернетичної безпеки.

Наукова новизна дослідження - удосконалений метод захисту інформації у кіберфізичних системах типа «розумний дім», удосконалення досягнуто шляхом впровадження оптимізованої (за ресурсоємністю механізму) Blockchain–технології для надійної автентифікації, з використанням бази даних загроз, отриманих з найсучасніших верифікованих джерел та найуспішнішого досвіду впровадження відповідних безпекових засобів і рішень з формуванням актуальної на поточний час бази даних стосовного досліджуваного напрямку забезпечення цифрової безпеки.

Практичне значення досліджень базується на отриманні дієвого уніфікованого алгоритму широкого застосування, що передбачає формування доцільної та ефективної архітектури системи моніторингу цифрової безпеки, що дозволить структурувати та концептуалізувати задіяні у сучасності безпекові засоби, а також провадити передові рішення.

РОЗДІЛ 1

АНАЛІЗ ФУНКЦІОНУВАННЯ IoT–СИСТЕМИ (КІБЕРФІЗИЧНОЇ СИСТЕМИ) «РОЗУМНИЙ ДІМ»

1.1 Концепція та загальна схема реалізації IoT–системи «розумний дім»

За результатам огляду актуальних наукових праць та публікацій [8 – 17], формуємо понятійну концепцію кіберфізичної системи «розумний дім» – це IoT–система контролю складових інженерного супроводу життєзабезпечення приватного житла, яка формує базово-санітарні, комфортні та безпечні умови житлового середовища у повному або частковому автоматичному стані – рис. 1.1.

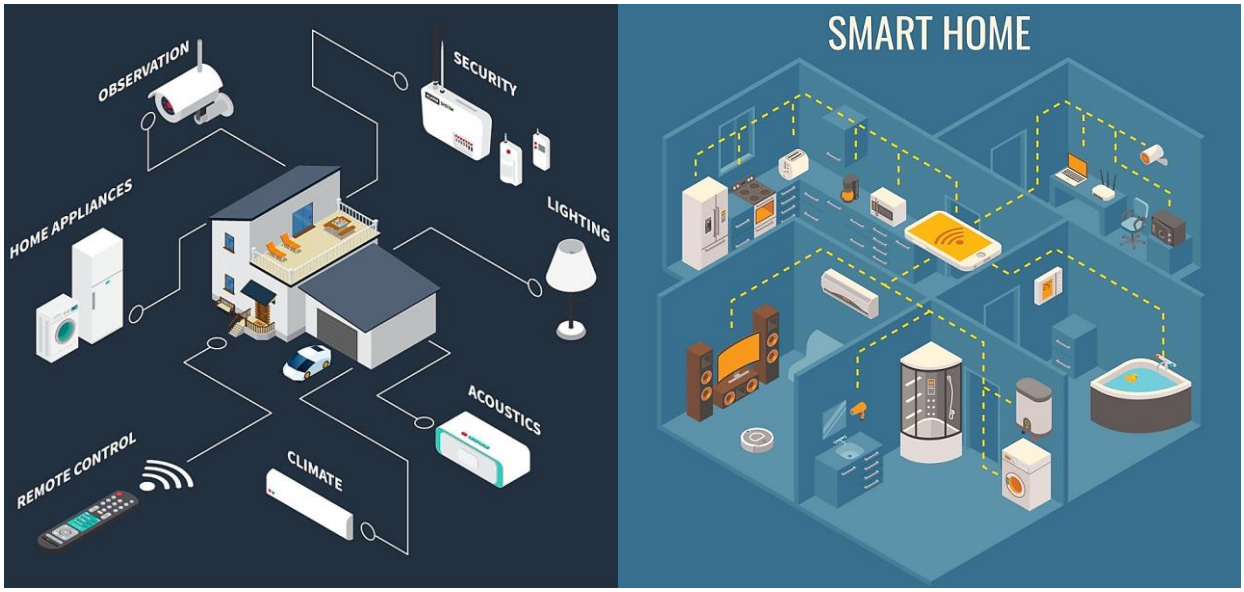

Рисунок 1.1 – Понятійна концепція IoT–системи «розумний дім»

Зазначена на рис. 1.1 концептуальна схема передбачає залучення протоколів та засобів зв’язку IoT–технологій для елементів і складових частин інженерного, мультимедійно-дозвільного, базово-санітарного, комфортного та

безпекового супроводу життєдіяльності мешканців житлового будинку, що мають можливість здійснювати контроль та налаштування параметрів центральної системи керування шляхом виконання маніпуляцій на відповідних приладах, що мають інтуїтивний інтерфейс – рис. 1.2 [8 – 17].

Керовані системи та принципи керування, що реалізуються на базі кіберфізичної системи «розумний дім» зазначені на рис. 1.2 та в табл. 1.1 [8 – 17].

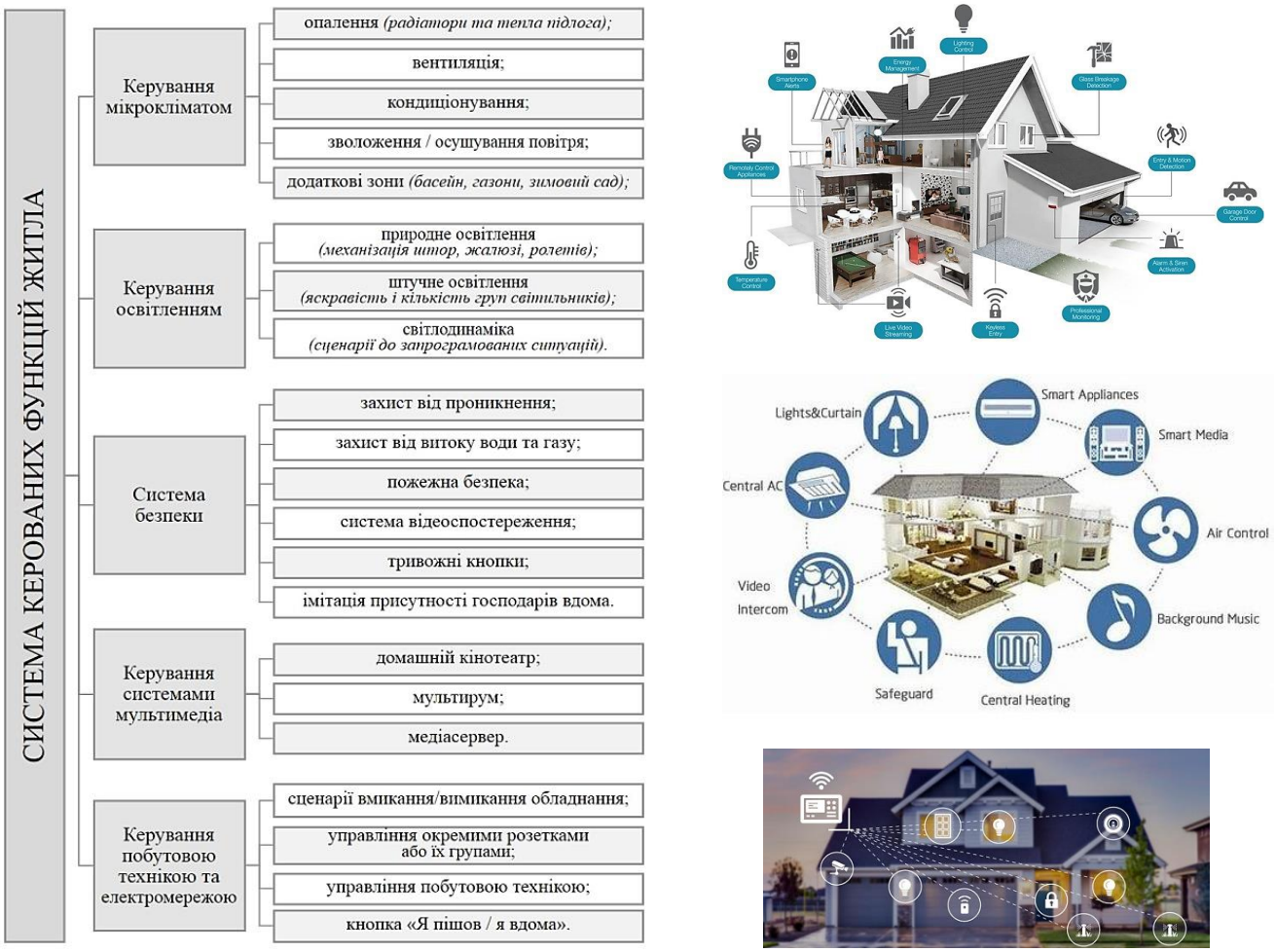

Рисунок 1.2 – Система керованих функцій житлового середовища з допомогою IoT–системи «розумний дім»

Таблиця 1.1

Принципи керування функціями житлового середовища в кіберфізичній системі «розумний дім»

Керована функція житлового середовища	Принцип керування
Мікроклімат	Інтелектуальна система клімат-контролю працює відповідно до закладених у неї алгоритмів, що дозволяють підтримувати параметри середовища і різних кліматичних зон в приміщеннях при мінімальних затратах енергоресурсів. Для автоматичного регулювання систем опалення використовуються спеціальні прилади – терморегулятори. З їх допомогою і за допомогою програмного забезпечення системи можна налаштовувати температурний режим, а також встановити співвідношення між роботою теплої підлоги і радіаторів. Для підтримки оптимальної вологості повітря (40 – 60 %) можуть використовуватися зволожувачі й осушувачі. Система управління кліматом в приміщенні дає можливість встановлювати оптимальний рівень температури, вологості, величину притоку свіжого повітря, управляти роботою системи фільтрації повітря, створювати індивідуальну кліматичну систему для кожного члена сім'ї (наприклад, в дитячій кімнаті постійний приток свіжого повітря за відсутності протягів). У той же час система клімат-контролю, забезпечує економію фінансових коштів і вирішує проблему енергозбереження. Система клімат-контролю «розумного будинку» дозволяє створити здоровий і комфортний мікроклімат для затишного проживання в будинку.
Освітлення	Інтелектуальна система управління джерелами штучного освітлення регулює яскравість і кількість освітлювальних приладів для кожного окремого приміщення чи функціональної зони, в залежності від часу доби, погодних умов, виду діяльності мешканців у конкретний час. Однією з важливих можливостей «розумного будинку» є створення динамічних світлових сценаріїв, коли натискання на одну кнопку вмикає оптимальне освітлення для тієї чи іншої ситуації. Система визначає пріоритетність тих чи інших освітлювальних приладів, за потреби вмикає необхідні світильники і вимикає не використовувані. Крім створення комфорту, застосування таких систем значно подовжує термін служби електроприладів, а також чимало сприяє енергозбереженню.

Продовження табл. 1.1

Керована функція житлового середовища	Принцип керування
Безпека	Система безпеки у «розумному будинку» має кілька напрямів захисту: захист від проникнення;захист від витоку води та газу; пожежна безпека; система відеоспостереження; тривожні кнопки; імітація присутності господарів вдома. Камери відеоспостереження, система сигналізації, датчики руху і об'єму дозволяють відслідковувати появу непрошених гостей. А сенсори температури, вологості, контролю газу та задимленості повідомляють про побутові аварії: протічки в каналізації, пожежонебезпечні ситуації, витоки газу чи води, та передають інформацію до модуля запобігання надзвичайним ситуаціям, господарю і, за необхідності, до відповідних служб швидкого реагування. Додаткова опція «розумного будинку» – можливість встановлення у будинку кнопок тривоги для використання дітьми, людьми похилого віку або особами з фізіологічними обмеженнями.
Мультимедійне дозвілля	Крім функції обслуговування, «розумний будинок» також оснащений внутрішніми системами для розваги господарів будинку та їх гостей. До основних складових системи інтелектуального керування мультимедійними засобами можна віднести: мультирум; медіасервер; домашній кінотеатр. Усі мультимедійні системи «розумного будинку» складають аудіовізуальний комплекс. Інтелектуальна система забезпечує повне управління всіма компонентами комплексу, починаючи від джерел звуку або зображення і закінчуючи підсилювальним устаткуванням і плазмовими екранами. Мультирум – це система багатозонного розподілу аудіо і відео, що дозволяє використовувати апаратуру не лише в тому приміщенні де вона встановлена, а й в усіх передбачених приміщеннях та зонах, навіть на подвір'ї. Будь-які треки або фільми родини зберігається на єдиному медіа сервері, що представляє собою своєрідну домашню бібліотеку всієї, наявної в будинку, аудіо та відео інформації.
Побутова техніка, інженерні мережі	Керування побутовою технікою та інженерними мережами є важливою частиною загального комплексу інтелектуального керування середовищем житла. До неї можна віднести наступні складові: сценарії вмикання / вимикання обладнання; управління окремими розетками або їх групами; управління побутовою технікою. Також частиною системи управління електромережою будинку може стати кнопка «Я пішов / я вдома» біля вхідних дверей, на яку буде запрограмоване при покиданні житла господарем вимкнення певних груп обладнання та переведення в економний режим інших, а також переведення їх в оптимальний режим при поверненні мешканців.

На підставі даних, вказаних на рис. 1.2 та табл. 1.1, доходимо висновку, що IoT–система «розумний дім» являє собою кіберфізичний простір, виконавчі мережі та елементи якого формують комфортне та безпечне житлове середовище, реалізуючи при цьому супутні принципи енерго- та

ресурсоощадності, енергоефективності, а також створює будівельний елемент для інтеграції в більш глобальну концептуальну парадигму «розумне місто», що є наступним кроком на шляху еволюції цифрового середовища суспільства, відповідно до результатів дослідження [6]: виявлено, що впровадження таких цифрових технологій як ICT, AI, IoT дозволяє розширити та підвищити адаптивність керованості та автоматичного реагування (відповідно до запитів користувача) засобів та мереж інженерного супроводу життєзабезпечення – рис. 1.3. Концепція «розумний дім» та більш глобальна парадигма «розумне місто» утворюють засоби для реалізації світових стратегій сталого цивілізаційного розвитку.

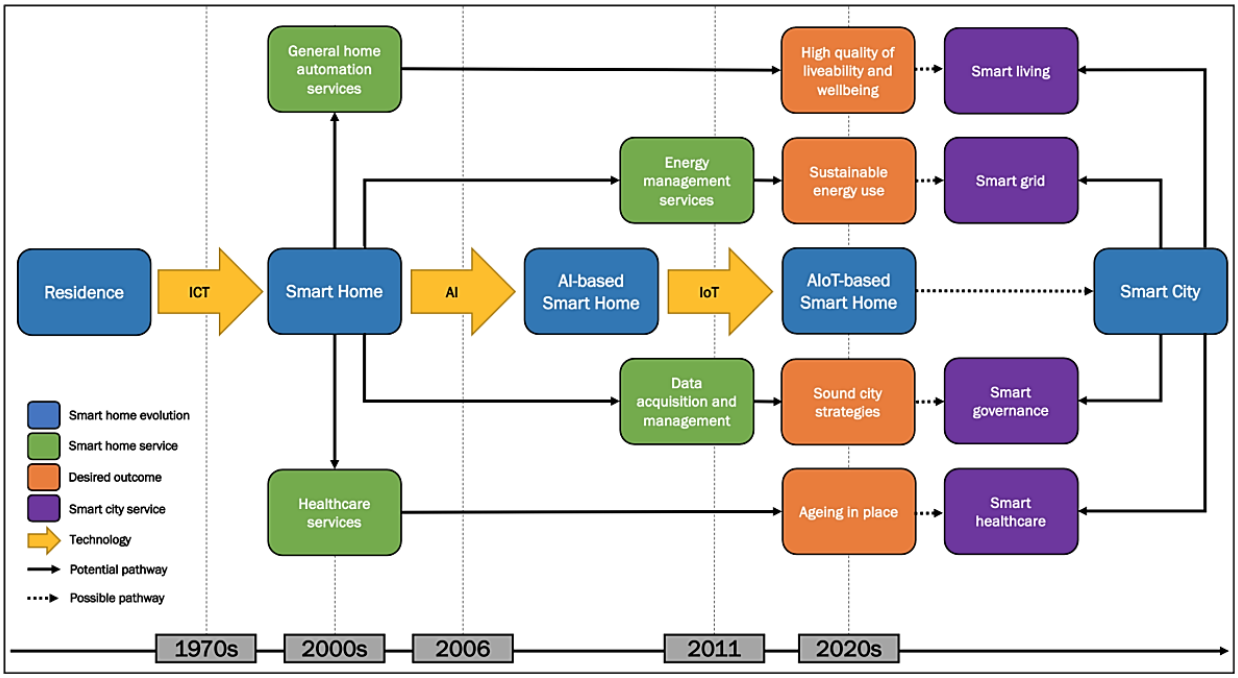

Рисунок 1.3 – Еволюція концепції «розумний дім» в парадигму «розумне місто», що формується на підставі розвитку цифрових технологій: ICT, AI, IoT [6]

Внаслідок результатів понятійного дослідження концепції «розумний дім», доходимо висновку, що досліджувана кіберфізична система є не лише засобом задоволення потреб локальних мешканців «розумного» житлового середовища, а є інструментом раціоналізації і оптимізації ощадного

використання енергії та ресурсів та інтегрується в комплексну систему «розумного» міста.

1.2 Устаткування та прилади

Сучасні прилади, комплекси та системи з маркуванням «розумні», що використовуються в межах досліджуваної IoT–системи мають різноманітні варіації електронно-конструктивного виконання відповідно до проектів профільних виробників, які пропонують в даному секторі ринку окремі та комплексні рішення з улаштування інтелектуальних систем інженерного супроводу життєзабезпечення житлових та цивільних будівель – рис. 1.4 [18 – 35].

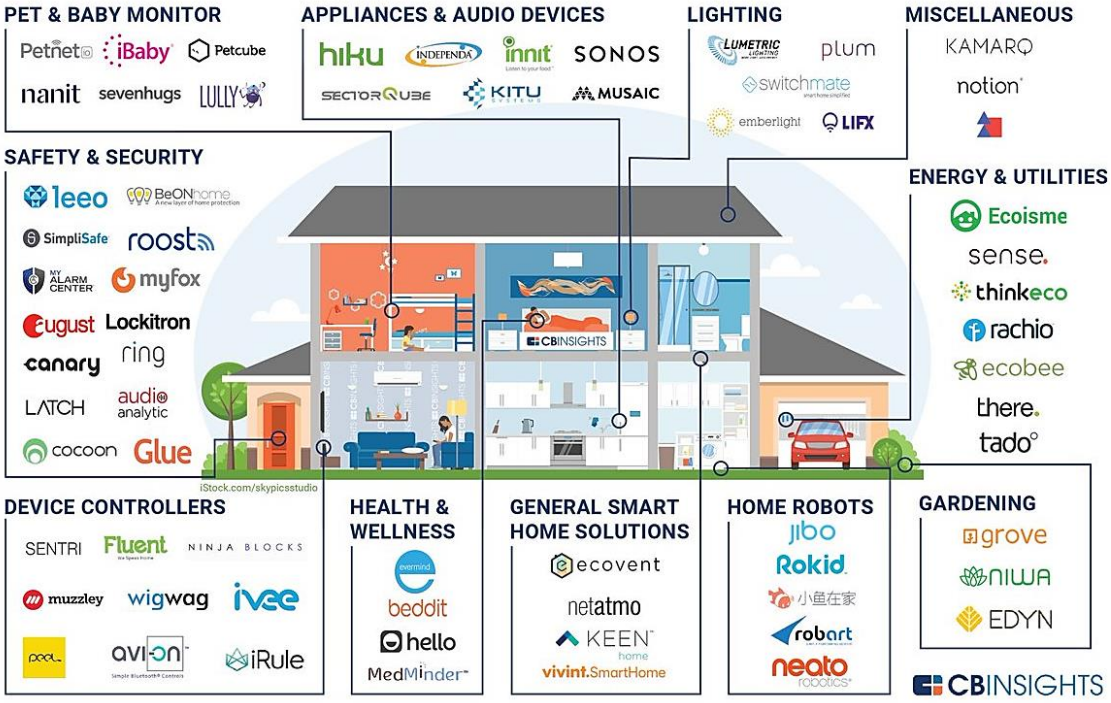

Рисунок 1.4 – Брендовий аналіз сектору ринку «розумних» побутових технологій, що можуть бути використаними в IoT–системі «розумний дім» [18 – 35]

Загальна концепція кіберфізичної системи «розумний дім» передбачає використання засобів збирання та аналізу інформації, що надходить з контрольованого середовища (датчиків), засобів аналізу інформації (контролерів), що надходить з датчиків середовища та безпосередньо виконавчих засобів реагування (регуляторів) на контрольовані параметри середовища, що безпосередньо впливають на параметри контрольованого середовища, в якому задіяні «розумні» технології інженерного супроводу життєзабезпечення – рис. 1.5 [18 – 35].

На підставі аналізу наукових праць та публікацій [18 – 35] виконаємо аналіз складових частин кіберфізичної системи «розумний дім», що функціонує на базі технології IoT.

Датчиками називають пристрої, що реєструють факт виникнення будь-якої події та перетворюють цю подію на електричний сигнал. У розумному будинку найчастіше застосовуються датчики, різновиди і загальні принципи дії яких зафіксовано в табл. 1.2 [18 – 35].

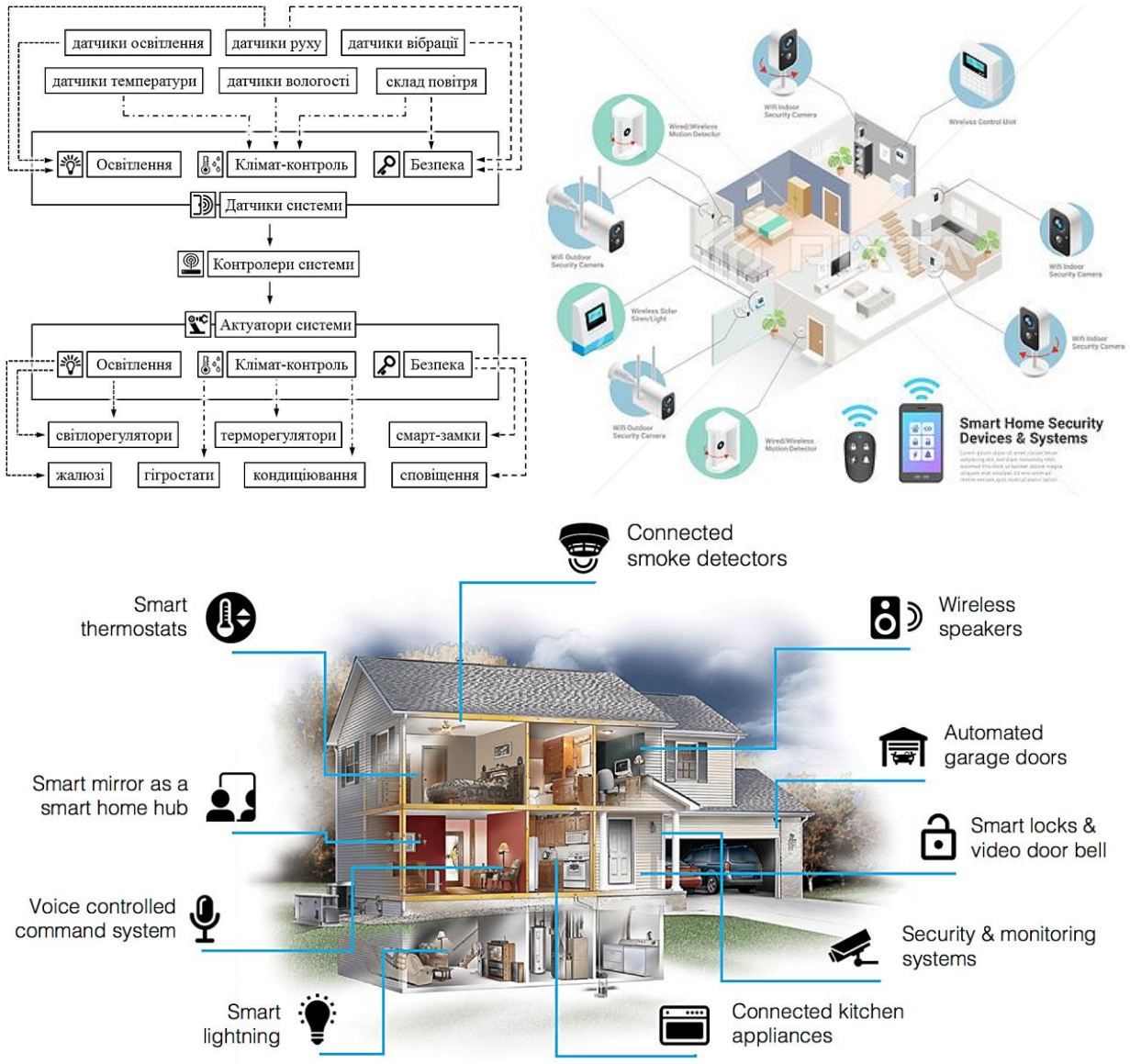

Рисунок 1.5 – Концепт-модель функціонування субструктурних кіберфізичних систем «розумного дому»

Таблиця 1.2

Загальна характеристика найбільш уживаних засобів збирання та аналізу інформації, що надходить з контрольованого середовища

Тип датчику	Загальний опис та принцип дії
Датчик руху	Пристрій, що виявляє рух у певній ділянці простору. Найчастіше застосовують пасивні датчики руху (PIR), принцип дії яких заснований на вимірюванні фонової температури.
Датчик вимірювання температури, тиску та вологості повітря	Це наступний вид датчиків, який часто використовується в системах управління кліматом розумного будинку. Вони використовують різні способи вимірювання та інтерфейси підключення, але досить дешеві і можуть бути встановлені в кожній кімнаті.

Продовження табл. 1.2

Датчик освітленості	Пристрій призначений для вимірювання рівня освітленості. Найчастіше він використовується в системах керування освітлення для автоматичного увімкнення світла в темний час.
Датчики розбиття скла	Пристрій найчастіше використовуються у системах безпеки. Вони реагують на звук скла, що розбився, і короткочасний звук, недоступний юшку людини, який виникає при прогині скла.
Датчики вимірювання якості повітря	Це ціла група датчиків, яка вимірює рівень оксиду вуглецю у повітрі, вміст метану, наявність диму, рівень запиленості. Такі датчики можуть використовуватись для системи безпеки та пожежної сигналізації, а також систем вентиляції.

У системах управління «розумного дому» можуть застосовуватись датчики та інших типів, наприклад, датчики витоку води, відкриття дверей, охорони периметра. Все залежить від ваших вимог та бажання отримати всебічну інформацію про те, що відбувається у конкретному житловому середовищі та його околицях – рис. 1.6 [18 – 35].

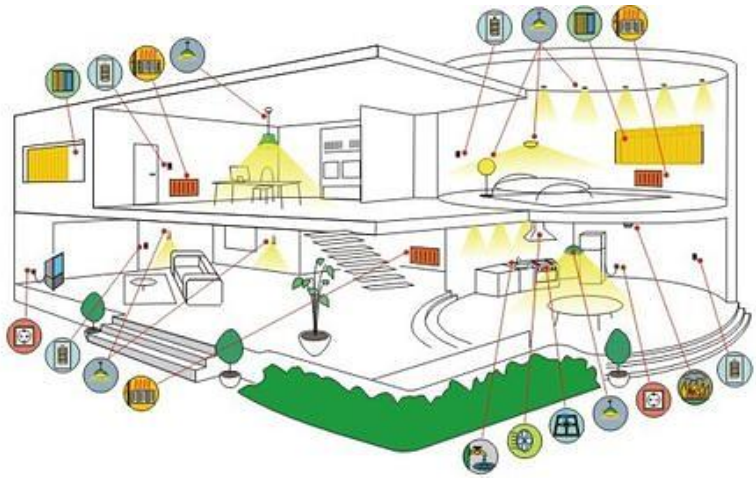

Рисунок 1.6 – Концепт-схема розміщення датчиків у кіберфізичній системі «розумного дому»

Вся оброблена інформація, яку зібрали датчики, повинна бути певним чином оброблена, проаналізована, і на її підставі повинні бути виконані будь-які дії. Всім обробленням інформації в системі «розумного» будинку займаються контролери, панелі керування або персональні комп'ютери. На ринку є величезна кількість контролерів різних виробників, техніко-електронне

виконання яких варіюється в залежності від потреб споживачів та цінового діапазону [18 – 35].

Ключовим параметром контролера є його швидкодія. Саме від цього параметра залежить швидкість реакції на події, а значить і складність алгоритмів, які використовуються для аналізу. Швидкодія контролера надає прямий вплив на його швидкість та споживану потужність. Необхідну продуктивність контролера можна розрахувати, проте в домашній автоматизації це зазвичай не робиться, і вибирається контролер з великим запасом.

Ще однією важливою характеристикою контролера є його надійність. Є досить складні методики аналізу надійності, але з метою домашньої автоматизації її можна пояснити так: надійність – це ймовірність того, що контролер буде несподівано перезавантажений, і ваша програма почне виконуватися спочатку (всі замки стануть відкритими, світло увімкнено і т.д.). На надійність контролера впливає якість виготовлення, температурний режим роботи, відсутність, або навпаки наявність дефектів програмного забезпечення, якість та стабільність джерела живлення, електромагнітні перешкоди. Крім того, сама архітектура системи розумного будинку дуже впливає на надійність роботи. Наприклад, неправильно прокладені кабелі, або неправильні режими роботи можуть призводити до «падіння» навіть найдосконалішого пристрою.

Керуючий вплив від контролера у вигляді електричних сигналів, повинні бути перетворені на зовнішні дії. Тобто, необхідно зробити зворотну операцію по відношенню до тієї, яку виконують датчики: електричний вплив перетворити на механічний, звуковий, світловий вплив. Як виконавчі пристрої використовуються лами, світлодіодні стрічки, електродвигуни, електромагнітні клапани. Сам контролер працює на дуже низькій напрузі і має малу потужність, тому не може безпосередньо керувати подібними пристроями. Для цього потрібно силові елементи, які можуть бути виконані як самостійно, так і у складі виконавчого пристрою [18 – 35].

Найпростішим варіантом силового пристрою є електромагнітне реле. Воно використовується для включення джерел світла, живлення електричним

споживачам. Реле використовується в ролі посередника, що посилює малу дію, що виробляється контролером. Крім реле як подібні пристрої можуть застосовуватися й інші електронні компоненти, наприклад транзистори, тиристори, але основна ідея залишається без зміни.

Силові пристрої використовуються для керування різними моторизованими елементами, наприклад, для автоматичного відкриття штор і захисних жалюзі на вікнах. Електромагнітні клапани використовуються в системах автополиву на садовій ділянці або для автоматичного перекриття трубопроводу.

Ще одним виконавчим пристроєм є димер. Для досягнення необхідного рівня комфорту може знадобитися плавно керувати яскравістю освітлення лампи. Саме для таких цілей використовується димер – пристрій, що дозволяє змінювати яскравість свічення лампи залежно від впливу, що управляє. Така дія в розумному будинку приходить на димер від контролера.

Крім керування лампами димери часто використовуються для керування іншими споживачами, наприклад, нагрівальними елементами для регулювання температури, або для управління швидкістю обертання вентилятора. При таких комбінаціях потрібно обов'язково ретельно перевіряти, оскільки є ризик виходу з ладу обладнання або навіть спалаху в самому несприятливому випадку.

У системах управління часто використовуються сенсорні панелі, що випускаються різними виробниками. Ці пристрої можуть працювати по дротовій та бездротовій мережі, але у будь-якому випадку потребують додаткового кабелю живлення. Панелі можуть виводити HD відео, мати інтегровані динаміки, мікрофон, камеру, біометричний сканер, інтегровані датчики руху, освітленості, температури. Панелі, крім сенсорного екрана, можуть мати звичайні кнопки, які дозволяють отримати тактильні відчуття від натискання. Деякі виробники випускають бездротові переносні панелі з вбудованим акумулятором, що дозволяє вільно пересуватися по дому [18 – 35].

Можливості розумного будинку визначаються не тільки обладнанням, що використовується. Дуже сильно функціональність та інтелект системи залежить

від програмного забезпечення (ПЗ). Програмне забезпечення розробляється для контролерів, панелей керування, мобільних пристроїв, серверної частини розумного будинку. Більшість виробників зробили свої типові рішення, які можуть бути налаштовані для будь-якого будинку або квартири. При налаштуванні системи описується конфігурація, кількість контролерів, датчиків, виконавчих елементів, допрацьовуються типові сценарії, зроблені постачальником системи.

Ще одним елементом розумного будинку є кабельна інфраструктура. Незважаючи на розвиток систем бездротового зв'язку, прокладання кабелів у багатьох випадках є єдиним варіантом. Крім того, цей спосіб є надійнішим. Для передачі різних сигналів потрібне застосування різних типів кабелів. Зараз випускається безліч кабелів, які можна підібрати для вирішення будь-якого завдання. Якщо будинок великий, то оптимальним варіантом є використання оптичних кабелів для з'єднання поверхових шаф будинку. Використання оптичних ліній дозволить створити інфраструктуру, здатну передати величезну кількість інформації із високою швидкістю.

Загальна концепт-схема улаштування кіберфізичної системи «розумний дім» на базі IoT–технології з застосуванням датчиків, контролерів та виконавчих пристроїв вказана на рис. 1.7.

Ринок домашньої автоматизації активно розвивається з початку 80-х років минулого століття. На ринку працює безліч компаній, тому за цей час було створено безліч різних технологій, найчастіше несумісних між собою, реалізованих в обладнанні, доступному на ринку. Розглянемо найбільш уживані [18 – 35].

X10. Це один із перших протоколів домашньої автоматизації, який з'явився ще у 70-х роках минулого століття. Стандарт є відкритим. Це провідний протокол, який використовує як середовище передачі силову електропроводку будинку. Відповідно при використанні пристроїв, що працюють за цим стандартом, немає потреби у прокладанні додаткових дротів.

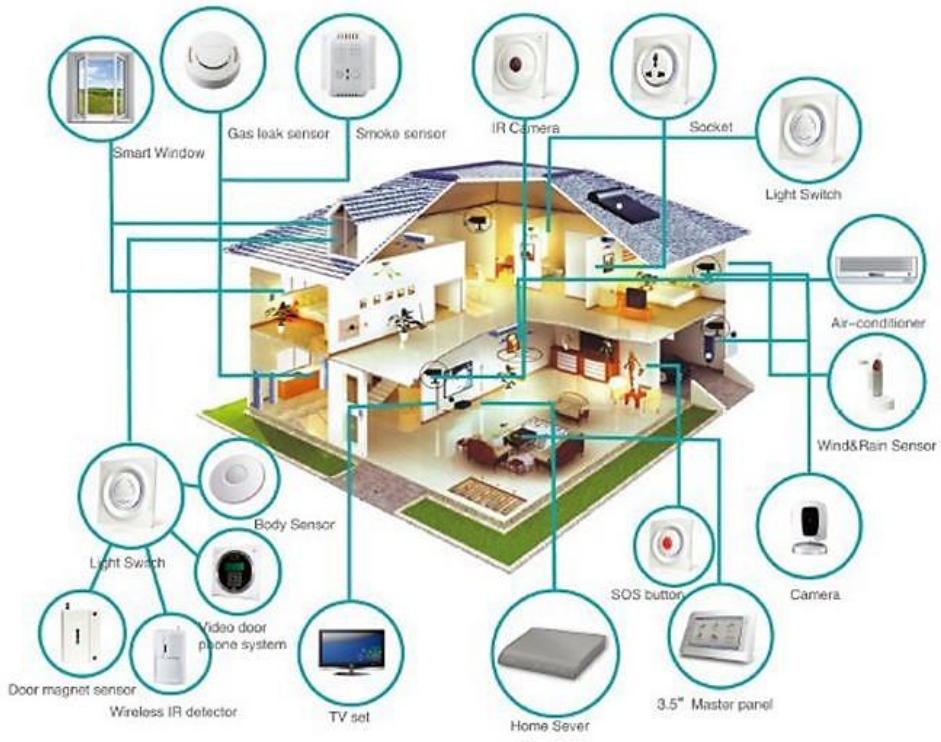

Рисунок 1.7 – Загальна концепт-схема улаштування кіберфізичної системи «розумний дім» на базі IoT–технології з застосуванням датчиків, контролерів та виконавчих пристроїв

Для цього протоколу випускається безліч виконавчих модулів для управління освітленням, електроприладами, опаленням, вентиляцією та охоронними системами. Також випускається велика кількість різних вимикачів, датчиків, які можуть працювати спільно з виконавчими модулями, але додатково може знадобитися встановлення відповідного контролера. Для зв'язку з персональним комп'ютером та роботи з контролерами за стандартними протоколами потрібні комунікаційні модулі [18 – 35].

Серйозним недоліком X10 є низька швидкість передачі, через яку реакція на події відбувається з певною затримкою. Вона не дуже велика, але помітна, наприклад, при побудові системи керування освітленням. Ще одним недоліком протоколу є відсутність шифрування та гарантованої доставки повідомлень. Це може призвести до того, що команда на увімкнення світла просто не буде виконана.

Всі ці недоліки пов'язані з використанням силової лінії живлення передачі даних. Крім того, протокол був розроблений давно, а імпульсні джерела живлення, які активно створюють перешкоди, що заважають роботі пристроїв X10, з'явилися пізніше, тому серйозних претензій до розробників протоколу не можна пред'явити. Незважаючи на всі ці недоліки, у світі працює безліч систем автоматизації, побудованих на основі X10.

KNX. Побудова системи автоматизації на базі стандарту KNX – це найдорожчий варіант, але дуже популярний у Європі, і є європейським стандартом автоматизації будівель. Стандарт відносно рідко використовується при автоматизації будинків, ще рідше він використовується при автоматизації квартир, але часто зустрічається при автоматизації будинків та офісів.

Стандарт з'явився на початку 90-х років минулого століття. В основі стандарту лежить шина EIB (European Installation Bus). Стандарт характеризується великою кількістю закладених у нього функцій, а також складністю проектування та монтажу. Як середовище передачі даних протокол KNX може використовувати шину, електричну мережу чи радіоканал.

Стандарт передбачає різні варіанти топології мережі. Але у більшості професіоналів KNX асоціюється саме з провідним варіантом, оскільки він використовується найчастіше. Система є децентралізованою, у ній може бути відсутнім центральний контролер. Але обов'язково має бути джерело харчування [18 – 35].

Протокол відмінно підходить для автоматизації великих будівель, в одну мережу можна поєднати до 50 тисяч пристроїв. Створено всесвітню асоціацію KNX, до якої входять понад 350 компаній у всьому світі. Найбільш відомими виробниками обладнання сьогодні є Schneider Electric, ABB, Gira. У світі випускається безліч пристроїв з різним функціоналом. Тому при використанні цього стандарту можна вирішити будь-яке завдання – рис. 1.8.

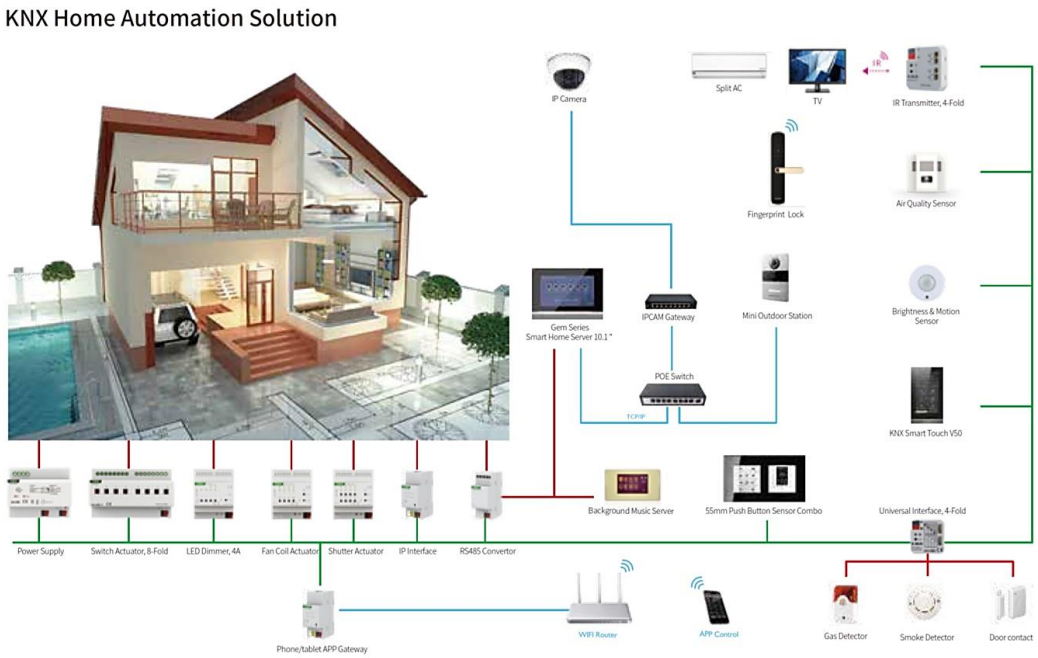

Рисунок 1.8 – Приклад рішень технології KNX–«розумний дім»

Для роботи пристроїв найчастіше прокладається кабель 4×0,8, при цьому для роботи шини KNX використовується одна пара ліній, друга пара використовується для подачі живлення. Обмін даних між пристроями здійснюється безпосередньо, без участі виділеного контролера, тому вихід з ладу окремого пристрою не призведе до вимкнення всієї системи. Такий підхід має як свої плюси, і мінуси. Однак ніхто вам не заважає використовувати окремий контролер для вирішення складних завдань взаємодії, які не можуть бути виконані налаштуванням пристроїв.

Єдиним недоліком KNX є висока вартість обладнання та його орієнтація на професіоналів. Впровадженням проектів займаються великі компанії, оскільки початкові витрати навчання персоналу, придбання необхідного програмного забезпечення та тестового устаткування дуже великі. Стандарт практично не підходить під ідеологію "Зроби сам", хоча теоретично це можливо. Як резюме можна сказати, що стандарт KNX дуже дороге, хороше, престижне і надійне рішення для систем автоматизації будівель [18 – 35].

ZigBee. ZigBee є бездротовим протоколом передачі. Це є відкритий стандарт. Рішення на основі цього протоколу дуже добре підходять для домашньої автоматизації. ZigBee заснований на осередку топології мережі, при якій окремі компоненти можуть виступати в якості посередника, що передає сигнал від одного пристрою до іншого. Подібна структура здатна до самоорганізації та самовідновлення, вихід з ладу одного-двох елементів, як правило, не призводить до серйозних наслідків. Комірчаста топологія також дозволяє суттєво збільшити область покриття бездротової мережі – рис. 1.9.

Рисунок 1.9 – Кіберфізична система «розумний дім» на базі технології ZigBee

Стандарт дозволяє створювати датчики з низьким енергоспоживанням, оскільки багато часу бездротові модулі знаходяться в сплячому режимі. У мережі можуть бути три види пристроїв: координатори, маршрутизатори та

кінцеві пристрої. У системі обов'язково має бути присутнім хоча б один координатор. Кінцеві пристрої – це різні датчики та виконавчі пристрої. Датчики отримують живлення від батарей, виконавчі пристрої найчастіше отримують від джерела живлення [18 – 35].

ZigBee підходить для вирішення всіх типових завдань, пов'язаних із автоматизацією будинку. Вартість пристроїв є відносно низькою, а процес встановлення є досить простим. В цілому, пристрої різних виробників добре працюють разом, проте трапляються випадки, коли пристрої виявляються несумісними. Пристрої ZigBee продаються різними компаніями як закінчених пристроїв, і у вигляді комунікаційних модулів. Дуже широко поширені пристрої XBee, які можна бачити у різних проектах, особливо у пристроях, зібраних на основі контролера Arduino.

Також протокол відомий тим, що відомі RGB лампи Philips HUE, які забезпечують дистанційне керування, використовують цей протокол. В цілому, можна сказати, що пристрої ZigBee відмінно підходять для домашньої автоматизації і можуть бути використані в проектах, зроблених професійним інсталятором або з використанням ідеології «Зроби сам».

Z-Wave – протокол бездротового зв'язку, який багато в чому схожий на ZigBee. Він був спеціально розроблений датською компанією Zen-sys наприкінці 90-х років минулого століття для систем домашньої автоматизації. Для цього протоколу також використовується топологія мережі у вигляді осередків і все зроблено для забезпечення наднизького енергоспоживання. Відмінність полягає в тому, що протокол є закритим, тому розробкою та виробництвом комунікаційних модулів займається єдина компанія Sigma Designs. Усі пристрої, незалежно від фірми-виробника, використовують однотипні комунікаційні модулі – рис. 1.10.

Це гарантує сумісність пристроїв, хоча є певні тонкощі, пов'язані із частотним діапазоном [18 – 35].

Z-wave використовує вільний від інтерференцій діапазон 868MHz. Передача даних здійснюється із шифруванням AES. У мережі має бути

обов'язково центральний контролер, який може обслуговувати до 255 пристроїв. При збільшенні кількості пристроїв можливе поєднання двох контролерів [18 – 35].

Рисунок 1.10 – Кіберфізична система «розумний дім» на базі технології Z-Wave

У зв'язку з тим, що протокол є закритим, для нього є значно менше інформації та розробленого програмного забезпечення. Однак є безкоштовні проекти, які дозволяють використовувати обладнання Z-Wave спільно з іншими системами домашньої автоматизації, наприклад LinuxMCE.

1-Wire – дротовий протокол передачі. Зареєстрована товарна марка корпорації Dallas Semiconductor. Забезпечує низькошвидкісний інтерфейс для даних (від 16,4 Кбіт/с до 125 Кбіт/с), проте цієї швидкості цілком достатньо для вирішення більшості завдань домашньої автоматизації [18 – 35].

Для зв'язку з пристроєм необхідно лише два дроти: на дані та заземлення. Для цього комунікаційний процесор містить конденсатор ємністю 800 пФ для

живлення лінії даних (режим паразитного живлення). Електроживлення здійснюється за рахунок розряду конденсатора, який заряджається під час високого рівня напруги на лінії даних. Тут слід враховувати, що зв'язок із пристроями, що використовують паразитне живлення, можливий лише на коротких лініях. На довгих лініях доводиться застосовувати додаткове проведення живлення.

Створення розподілених систем на базі шини 1-Wire є на сьогодні найоптимальнішим рішенням для більшості практичних завдань автоматизації. В даний час Dallas Semiconductor постачає широку номенклатуру однопровідних компонентів різних функціональних призначень для реалізації різноманітних мережних додатків. Тому є величезна кількість конкретних прикладів використання інтерфейсу 1-Wire для цілей автоматизації в різних областях, і все більше розробників виявляють інтерес до цієї технології. Як середовище передачі даних найчастіше застосовується кабель «вита пара», проте можливе використання звичайного телефонного кабелю.

Використовується топологія загальної шини, коли кожний пристрій підключено до лінії зв'язку. Типовий є структура з одним майстром мережі та безліччю ведених пристроїв. Конфігурація мережі є динамічною, пристрої можуть бути додані без вимкнення живлення. Кожен пристрій має індивідуальну унікальну 64-бітну адресу. Відсутність збігу адрес для компонентів, що випускаються Dallas Semiconductor, гарантується виробником. Тому мережа має практично необмежений адресний простір.

У протоколі присутні команди пошуку керованих пристроїв, які дозволяють швидко визначити нові керовані пристрої. Кожен пристрій просто підключається до мережі без необхідності налаштування. Основними перевагами протоколу 1-Wire є: низька вартість компонентів, відсутність вимог до лінії зв'язку, дуже простий протокол, можливість живлення пристроїв від лінії зв'язку, значна протяжність лінії зв'язку [18 – 35].

Крім того, простота протоколу призводить до того, що він може бути реалізований програмним способом практично для будь-яких мікроконтролерів,

доступних на ринку. Наприклад, поширені контролери Arduino легко забезпечують роботу з пристроями 1-Wire. Найчастіше пристрої використовуються для вимірювання температури, вологості, як енергонезалежні пристрої пам'яті (наприклад, широко відомі «таблетки» iButton, що використовуються в домофонах, охоронних системах). Є навіть система домашньої автоматизації BENUKS, яка повністю побудована на базі пристроїв 1-Wire [18 – 35].

Bluetooth Low Energy (BLE). З пристроями Bluetooth знайомі майже всі юзери сучасних гаджетів. Це бездротовий протокол невеликого радіусу дії та невеликою швидкодією. Основною відмінністю четвертої версії стандарту, випущеного у грудні 2009 року, є дуже низьке енергоспоживання.

Це дуже важливо для бездротових датчиків руху, температури та інших бездротових пристроїв. Чим менший пристрій споживає енергії, тим довше він зможе працювати на одному заряді батареї, що позначається на зручності експлуатації системи. BLE дозволяє пристроям задовольнятися значно меншою кількістю енергії, ніж стандартні з'єднання Bluetooth. При цьому він надає більшу частину звичайної функціональності на відстані, приблизно вдвічі меншій у порівнянні зі звичайним – приблизно 15 метрів проти 50 для Bluetooth (але цей параметр дуже залежить від режиму роботи). Пристрої, що працюють за протоколом Bluetooth LE, здатні роками працювати без необхідності змінювати або заряджати батарею Стандарт є відкритим та підтримує шифрування AES. Відсутність жорсткої стандартизації призводить до того, що пристрої різних виробників можуть бути несумісними між собою.

Пристрої стандарту Bluetooth 4.0 підтримують різні програми, які можуть бути використані для медичних пристроїв, різних спортивних датчиків, розумного годинника.

Практично всі сучасні мобільні пристрої, планшети, персональні комп'ютери оснащені вбудованим комунікаційним процесором, щоправда, не всі підтримують модифікацію 4.0 [18 – 35].

З найвідоміших новинок, пов'язаних з BLE 4.0, є пристрої iBeacon, які розробляє компанія Apple. Починаючи з 2013 року, підтримка iBeacon додана в IOS 7. Технологія iBeacon використовується як система позиціонування всередині приміщень. Фактично iBeacon є маячком, який постійно надсилає повідомлення. Знаючи розташування маячків, можна математичним способом визначити місце розташування пристрою [18 – 35].

Wi-Fi. Технологія Wi-Fi застосовується повсюдно, тому докладно зупинятися на ній немає сенсу. Проте є певні складнощі у розгортанні домашніх мереж. При експлуатації точки доступу в квартирі сучасного багатоквартирного будинку, проблематикою є низькою швидкістю роботи, що пов’язано з завантаженістю окремих каналів та неоптимізованим розташуванням роутерів. Від так, необхідно залучати фахівців для улаштування оптимальної кіберфізичної системи «розумний дім» на базі бездротової технології Wi-Fi [18 – 35].

На підставі проведено аналітичного огляду, встановлена численна варіативність електронно-конструктивного виконання як окремих пристроїв так і комплексних систем, що представлені в профільному сегменті ринку та з урахуванням відповідних особливостей функціонування і проектних рішень можуть бути залучені до побудови кіберфізичної IoT–системи «розумний дім».

Зважаючи на факт використання в досліджуваній кібернетичній системі значної кількості мережних та виконавчих засобів доцільно розглянути типові уразливості та кіберзагрози, що виникали для «розумних» технологій інженерного супроводу житлового середовища.

1.3 Аналіз кібернетичних загроз для IoT–системи «розумний дім»

Понятійні основи цифрової безпеки формують відповідні державні засади, такі як Закон України від 05.10.2017 № 2163-VIII [2], Стратегія кібербезпеки України [5] та галузеві нормативи (сформовані на підставі

впровадження успішного світового досвіду цифрових безпекових принципів) ДСТУ ISO/IEC 27032:2016 [36] та доповнюються результатами відповідних досліджень, зафіксованих в публікаціях державних [37 – 42] та світових [43 – 48] дослідників.

Відповідно до результатів понятійних досліджень, що сформовані на підставі регуляторних державних та галузевих регламентів [2–5, 36], встановимо, що кібернетична загроза – це фактично можливість здійснення кібернетичних атак для здійснення протиправних дій (несанкціонованого доступу, злам та викрадення конфіденційних цифрових баз, несанкціоноване використання інфраструктурних об'єктів та мереж, тощо) шляхом пошуку та протиправного впливу на вразливості цифрових баз даних і мереж.

Розвиток цифрових технологій не лише вдосконалює системи захисту у кібер-цифровому просторі, а й сприяє розвитку шкідливого програмно-технологічного інструментарію, з допомогою якого відбувається безпосередні кібератаки. Так, автором [49] зафіксована еволюція засобів кібер-цифрових атак – рис. 1.11.

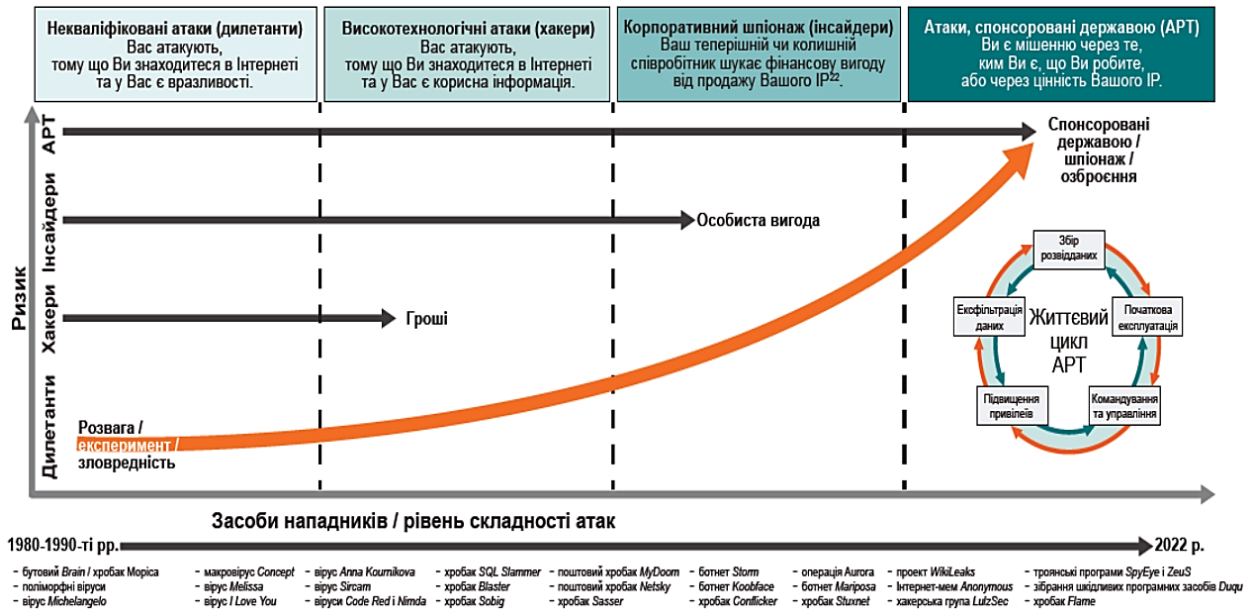

Рисунок 1.11 – Динаміка розвитку засобів для кібернетичних атак

Відповідно до аналізу публікацій [50 – 52] підтверджено також синхронне (до розвитку технічних засобів кібератак) ускладнення кіберзагроз, що зафіксовано на рис. 1.12.

Відповідно до даних, наведених на рис. 1.12, можливо виокремити, що останнім часом кібератаки стали одним з цільових інструментів протиправної дії не тільки стосовного початкових рівнів диференціації за рівнем користувача (приватно-побутовий, комерційно-технологічний), а і в рамках міждержавних актів агресії.

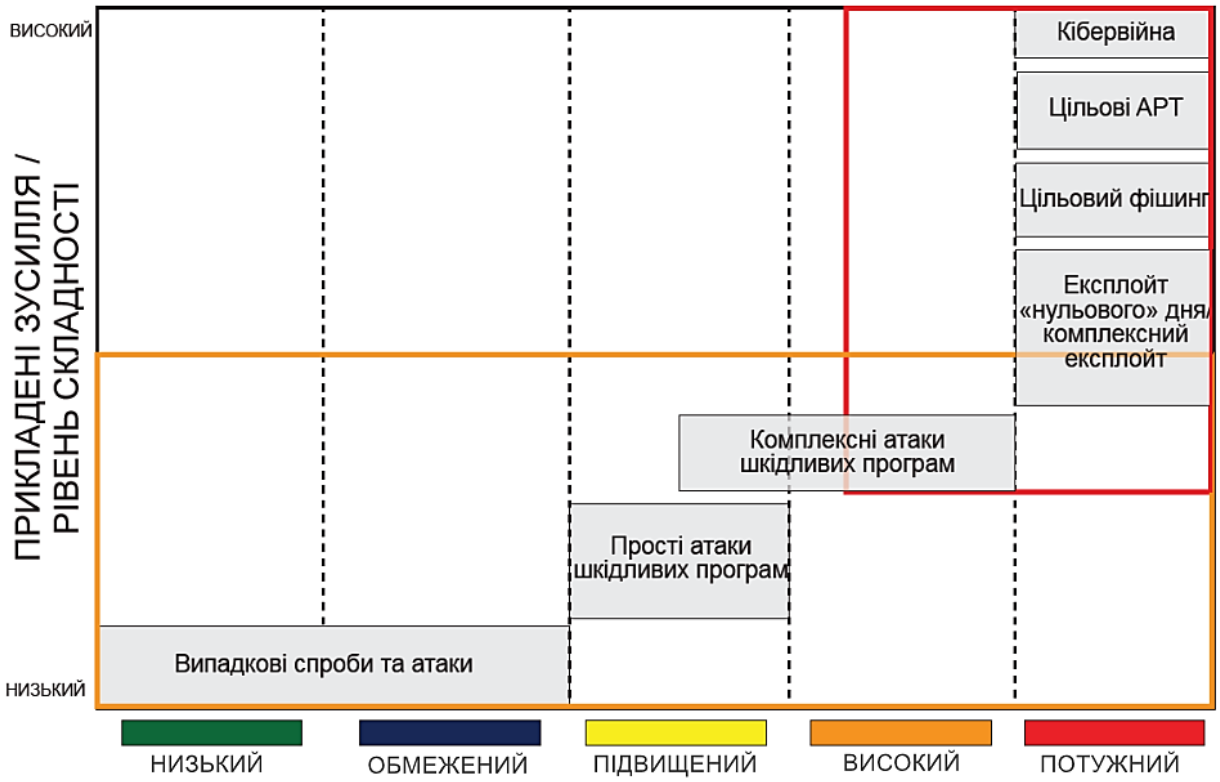

Рисунок 1.12 – Динаміка рівня складності кібератак

Відповідно до результатів аналіз наукових праць та публікацій [53 – 62] існує декілька типів класифікації кібер-цифрових атак, що впроваджені державним регламентом ДСТУ ISO/IEC 27032:2016 [36] (за об’єктами і механізмами дії), Міжнародною кримінальною Поліцією «Інтерполом» (за видами і засобами атак) та П. Нойманом (за типом, механізмом дії та наслідками атак).

З метою виявлення більш доцільної класифікації кібер-цифрових атак на IoT–систему «розумний дім» визначимо відомі факти реалізації кібернетичних загроз безпосередньо на прилади і субсистеми досліджуваної кіберфізичної технології, спираючись на результати аналітичного огляду наукових праць і публікацій [63 – 76] – табл. 1.3.

Таблиця 1.3

Відомі атаки на прилади і субсистеми досліджуваної кіберфізичної технології «розумний дім» [63 – 76]

Хроно-метрична точка / тип атаки	Принцип дії та наслідки
2012 / Злам веб-камери TRENDnet	У 2012 році компанія під назвою Trendnet продала камери SecurView для споживачів для використання в домашніх умовах та спостереження за немовлям. Експерти з питань безпеки виявили, що облікові дані для входу користувачів передаються в простому тексті через Інтернет, що дає хакерам можливість викрасти ці дані. Це дозволило б зловмисникам переглядати камеру та слухати її мікрофон.
2016 / Мірай Ботнет	До 2016 року хакери поступово заражали тисячі домашніх Wi-Fi камер та маршрутизаторів шкідливим програмним забезпеченням, яке залишалося неактивним і чекало сигналу активації. Сигнал розгорнув масштабну атаку, яка перетворила ці розумні домашні пристрої на велику бот-мережу. Ця атака використовувала ці пристрої для знищення великих веб-сайтів, таких як CNN, Guardian і навіть Twitter та Netflix.
2016 / DDoS	У листопаді 2016 року в результаті потужної розподіленої атаки відмови в обслуговуванні (Distributed Denial-of-Service, DDoS) на «розумну» систему контролю температури води та тиску в батареях опалення мешканці багатоквартирних будинків у фінському місті Лаппенранта провели тиждень без опалення та гарячої води.
2016 / Злам «розумного замка»	Замки одних вендорів передавали паролі доступу в незашифрованому вигляді. Так що зловмисники могли легко перехопити їх, використовуючи Bluetooth-сніффер. Декілька замків попалися на методі повторного відтворення: дверима можна було маніпулювати за допомогою заздалегідь записаних сигналів відповідних команд. У світлі поширення різноманітних голосових помічників дедалі актуальнішим стає і злом розумного замку через голосові команди. Декілька років тому з'ясувалося, наприклад, що якщо господарський гаджет лежить досить близько до зачинених дверей, то досить голосно промовивши через двері «Привіт, Сирі, відчини двері», і вас можуть впустити. Поширеним сценарієм злому більшості «розумних» замків є наступний: при отриманні сторонньою особою фізичного доступу до замку натисканням кнопок на ньому можна зробити авторизацію будь-яких гаджетів.

Продовження табл. 1.3

Хроно-метрична точка / тип атаки	Принцип дії та наслідки
2017 / Злам «розумної» камери	Часто камери атакують методом man-in-the-middle, вбудовуючись між клієнтом та сервером. У такий спосіб можна не тільки читати та змінювати повідомлення, а й підміняти відеопотік. Особливо у тих системах, де не підтримується протокол HTTPS. Лінійка камер мала прошивку, яка дозволяє змінювати налаштування камери за допомогою звичайних http-запитів без авторизації. У іншого вендора прошивка IP-камер дозволяла, також без авторизації, підключитися до камери та отримувати зображення в реальному часі. Не варто забувати і про відомі вразливості. Наприклад CNVD-2017-02776, проникнувши через яку до камери, далі за допомогою EternalBlue можна отримати доступ до комп'ютера користувача. Експлоїт EternalBlue, який використовує вразливості в протоколі SMB, знайомий багатьом: саме він використовувався для поширення шифрувальника WannaCry у 2017 році та в ході атак зловреда Petya. А ще EternalBlue був включений до складу Metasploit, його використовували розробники криптовалютного майнера Adylkuzz, черв'яка EternalRocks, шифрувальника Uiwix, трояна Nitol (він же Backdoor.Nitol), зловреда Gh0st RAT і т.п.
2018 / Помилка безпеки монітора дитини	У лютому 2018 року Forbes повідомив, що 50000 моніторів MiCam мали серйозну помилку безпеки, яка дозволяла хакерам перехоплювати трафік між батьковим телефоном і дитячою камерою. Хакер дав можливість хакерам побачити все, що могли бачити монітори.
2018 / Помилки Samsung SmartThings	У липні 2018 року експерти з безпеки Cisco виявили, що виявили понад 20 вразливих місць у центрі Samsung SmartThings Hub. Ці помилки можуть дозволити хакерам розблоковувати розумні замки, переглядати розумні камери, відключати детектори руху та керувати домашніми термостатами.
2018 / Взлом «розумного замка»	Інший цікавий експеримент дослідників із Pen Test Partners був присвячений перевірці захищеності замків марки Tapplock. Як з'ясувалося, їх можна розблокувати без відбитка пальця власника. Справа в тому, що коди розблокування генеруються на підставі MAC-адреси пристрою в мережі BLE. А оскільки адреса перетворюється з використанням застарілого алгоритму MD5, він легко може бути з'ясований. Оскільки Bluetooth-замки мають властивість розголошувати свої MAC-адреси по BLE, то зловмисник здатний дізнатися адресу, «хакнути» її з використанням вразливості MD5 та отримати хеш для розблокування замка. З'ясувалося, що API сервер компанії розголошує конфіденційні дані користувачів. Будь-яка стороння людина може дізнатися не тільки про місцезнаходження замку, а й розблокувати його. Зробити це досить просто: потрібно завести обліковий запис на Tapplock, взяти ID облікового запису жертви, пройти автентифікацію та захопити управління пристроєм. При цьому на рівні back-end виробник не використовує HTTPS. І навіть не потрібно ніякого злому або необхідності брутфорсити, тому що номери ID присвоюються акаунтам за елементарною схемою, що наростає. І ягідка на торті — API не обмежує кількість звернень, тому можна нескінченно завантажувати дані користувача з серверів. І цю проблему все ще не усунуто.

Продовження табл. 1.3

Хроно-метрична точка / тип атаки	Принцип дії та наслідки
2020/ Бекдор SSH→MitM	ESET попереджає про виявлення серйозних уразливостей в безпеці трьох різних домашніх центрів для управління системою розумного дому — Fibaro Home Center Lite, Home Matic Central Control Unit (CCU2) та eLAN-RF-003. Спеціалісти ESET виявили ряд уразливостей, які можуть бути використані зловмисниками для здійснення атак методом Man-in-the-Middle (MitM), підслуховування жертв, створення бекдорів або отримання доступу до деяких пристроїв та їх вмісту. У гіршому випадку, ці проблеми можуть навіть дозволити зловмисникам взяти під контроль центральний блок та всі підключені до нього девайси. Одним з уразливих пристроїв став Fibaro Home Center Lite — контролер домашньої автоматизації, призначений для управління різними пристроями IoT. Спеціалісти ESET знайшли ряд серйозних недоліків, які можуть відкрити доступ для сторонніх користувачів та зловмисників. Зокрема одна з уразливостей розумного дому дозволяє кіберзлочинцям створити бекдор SSH та отримати повний контроль над цільовим пристроєм. Після отримання повідомлення про виявлену уразливість розумного дому виробник швидко виправив недолік. В центральному пристрої системи розумного дому Homematic CCU2 також було виявлено недолік безпеки під час тестування ESET, а саме здатність зловмисника здійснювати несанкціоноване виконання віддаленого коду (RCE) від імені користувача root. Ця уразливість розумного дому могла дозволити зловмисникам отримати повний доступ до системи Homematic CCU2 та до підключених девайсів. Варто зазначити, що уразливість розумного дому була негайно виправлена виробником. Третім прикладом є розумний комунікатор eLAN-RF-003, який дозволяє користувачу керувати різноманітними домашніми системами через додаток на смартфоні, смарт-годиннику, планшеті або смарт-телевізорі. Результати тестування ESET показали, що підключення системи до Інтернету або навіть керування ним у своїй локальній мережі може бути потенційно небезпечним для користувача через низку критичних недоліків. Зокрема до них відноситься некоректна перевірка аутентифікації команд, яка дозволяла виконувати всі дії без входу в систему, або радіозв'язок з девайсами, які уразливі до атак типу повторного відтворення. Виробник виправив деякі уразливості розумного дому та зосередився на розробці нового покоління пристроїв.
2020 / DDoS-атака на світлодіодні лампи Philips Hue	У мосту Hue Bridge, через який лампочки спілкуються один з одним, існував пролом. І траплялися випадки, коли через цю вразливість зловмисники могли дистанційно перехопити контроль над роботою ламп. Хакери це зробили так. Вони змусили лампочку мерехтіти із частотою понад 60 Гц. Людина цього не помічає, а ось прилад зовні будівлі здатний розпізнати послідовності мерехтіння. Звичайно, в такий спосіб багато не «наміркаєш», але для передачі якихось паролів або айдішників цілком достатньо. У результаті секретна інформація була скопійована. Крім цього, Philips не подбали про посилення захисту при спілкуванні лампочок один з одним у локальній мережі, обмеживши тільки застосуванням шифрованого бездротового протоколу. Через це зловмисники могли запустити в локальну мережу підроблене оновлення софту, яке потім «розіллється» по всіх лампах. Таким чином черв'як отримає можливість підключати лампи до DDoS-атак.

Продовження табл. 1.3

Хроно-метрична точка / тип атаки	Принцип дії та наслідки
2021 / DDoS-атака на розетки SP-1101W компанії Edimax	У розетці моделі SP-1101W компанії Edimax для захисту сторінки з налаштуваннями використовувався тільки логін і пароль, причому виробник не пропонував змінити дані за замовчуванням. Це наводить на підозри, що ті самі паролі використовувалися на переважній більшості пристроїв цієї компанії (або використовуються до цього дня). Додайте до цього ще й відсутність шифрування під час обміну даними між сервером виробника та клієнтською програмою. Це може призвести до того, що зловмисник зможе прочитати будь-які повідомлення або навіть перехопити керування пристроєм, наприклад, для підключення до DDoS-атак.

Деякі механізми дії кібератак на розумні системи інженерного супроводу життєдіяльності вказано на рис. 1.13 [63 – 76].

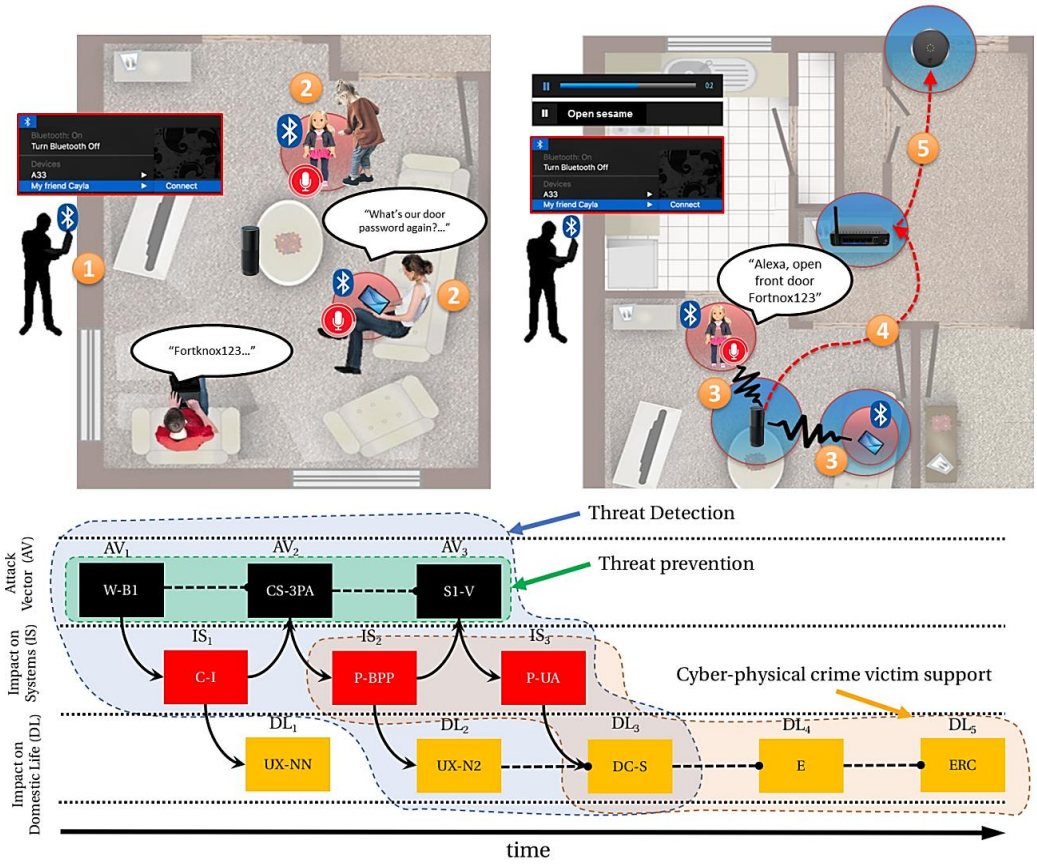

Рисунок 1.13 – Приклад покрокового здійснення атаки на кіберфізичну систему «розумний дім» для отримання коду доступу, шляхом викрадення паролю доступу при приєднанні до внутрішніх протоколів та мережі Bluetooth

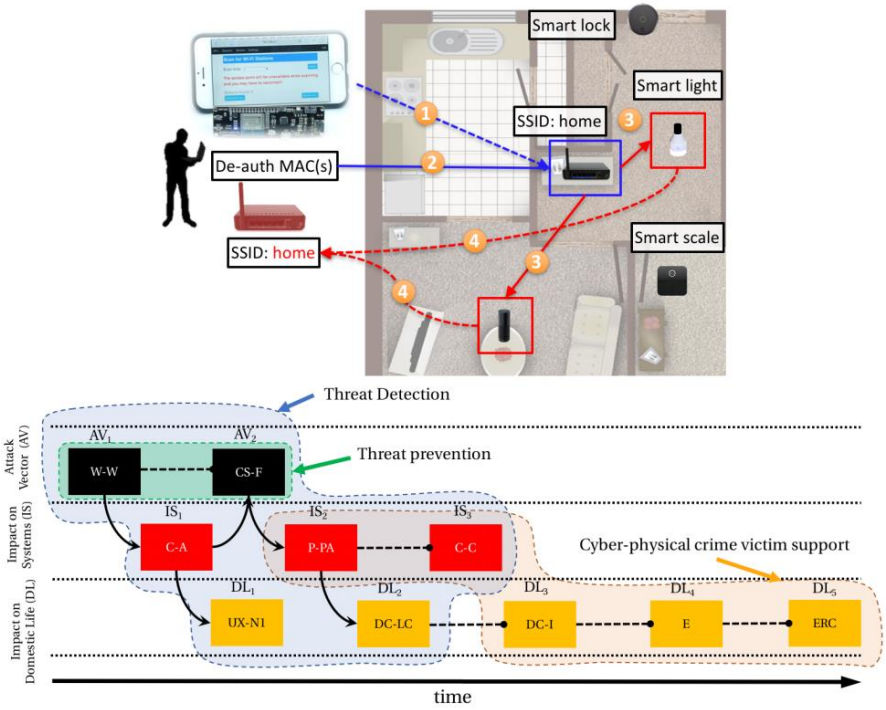

Рисунок 1.14 – Приклад покрокового здійснення атаки на кіберфізичну систему «розумний дім» для отримання доступу над побутовими приладами та системами шляхом де-аутентифікації домашньої мережі WiFi

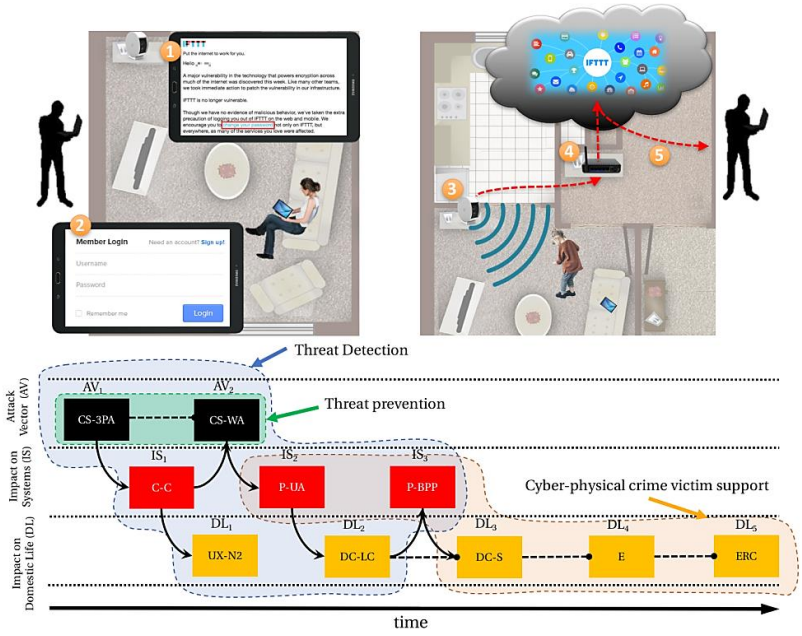

Рисунок 1.15 – Приклад покрокового здійснення атаки на кіберфізичну систему «розумний дім» для отримання контролю над центральним контролером через технологію фішингу та зовнішньомережного (або хмарного) впливу

Всі можливі варіації сучасних кібер-цифрових загроз, що можуть бути застосовані до кіберфізичної системи «розумний дім» систематизовано в таксономічну карту – рис. 1.16 [63 – 76].

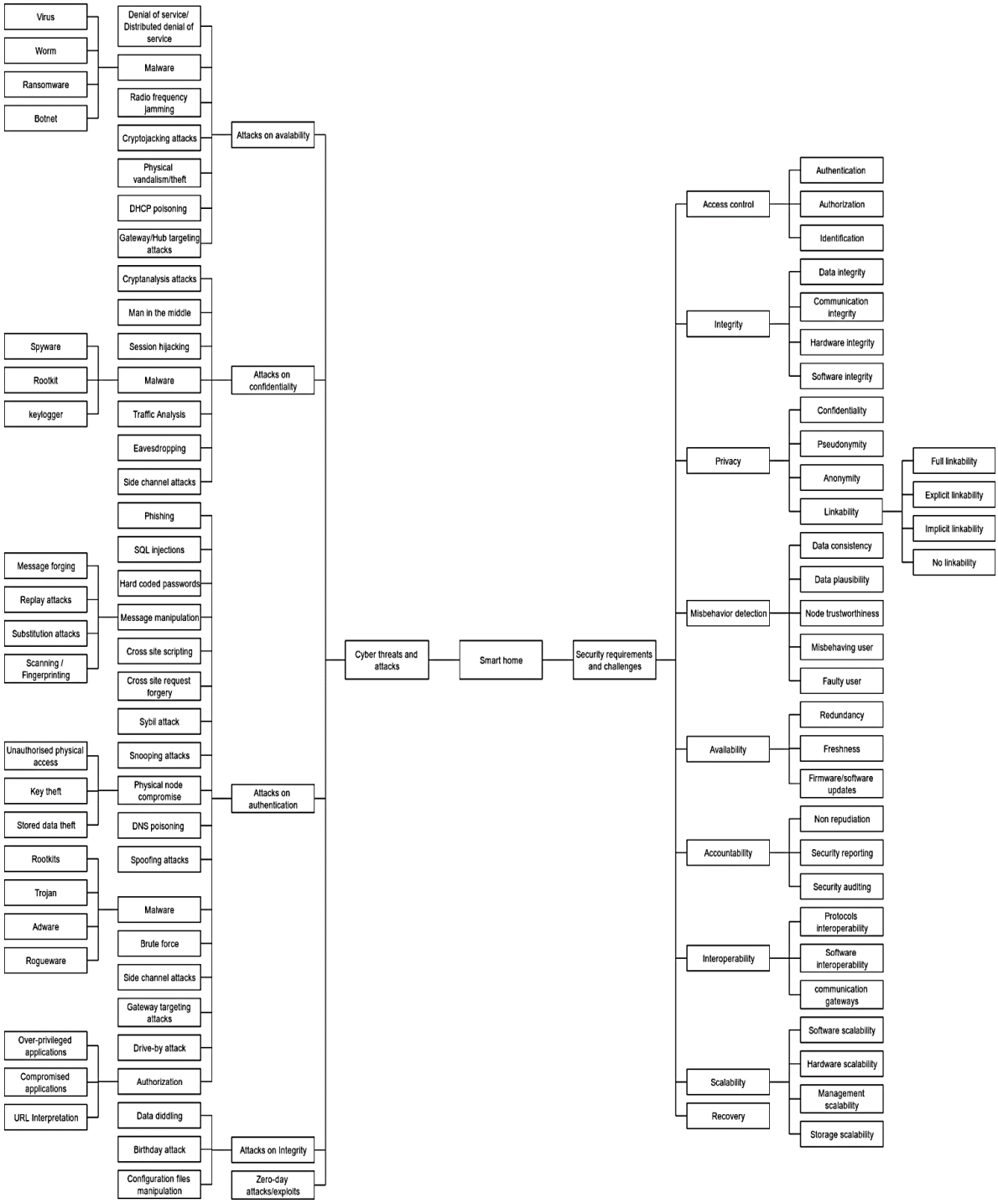

Рисунок 1.16 – Таксономічна карта можливих варіацій сучасних кібер-цифрових загроз, що можуть бути застосовані до кіберфізичної системи «розумний дім»

На підставі проведеного аналіз можливих варіацій сучасних кібер-цифрових загроз, що можуть бути застосовані до кіберфізичної системи «розумний дім» [63 – 76], сформулюємо найбільш вірогідні атаки та загрози, що представлені у вигляді концепт-схеми на рис. 1.17 та розшифровки цих атак в табл. 1.4.

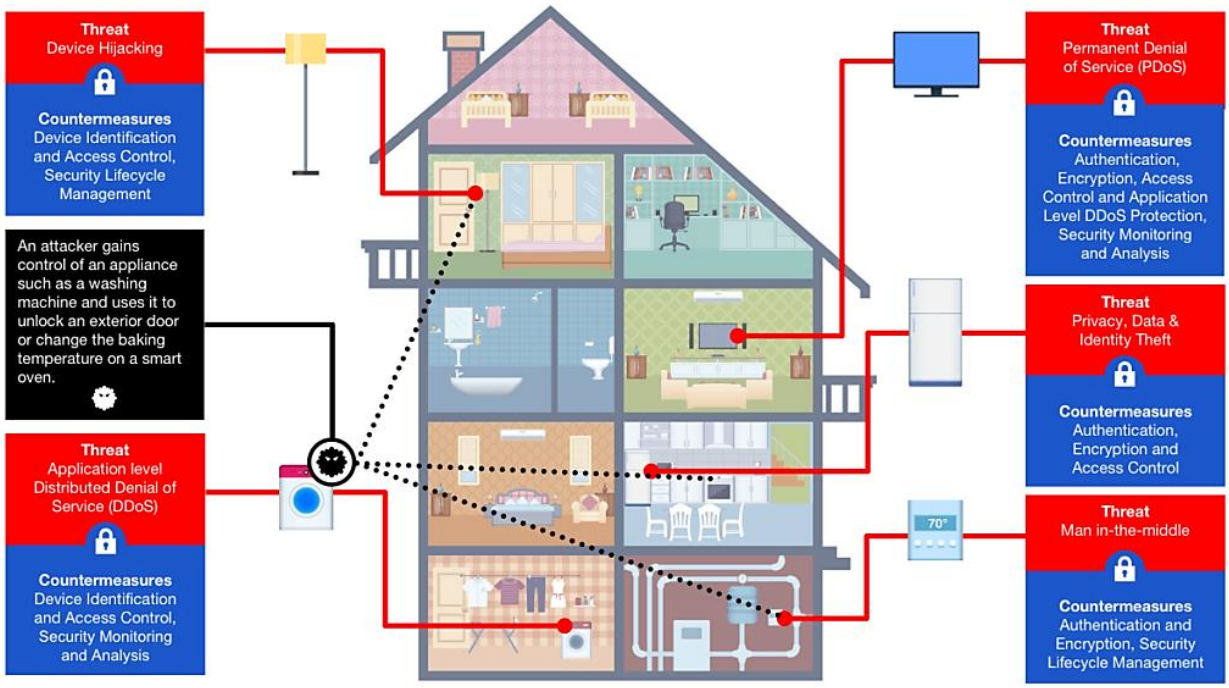

Рисунок 1.17 – Концепт-схема найбільш вірогідних атак та загроз безпеці кіберфізичної IoT–системи «розумний дім» (розшифровка – табл. 1.4)

Таблиця 1.4

Принцип дії найбільш вірогідних атак та загроз безпеці кіберфізичної IoT–системи «розумний дім» (відповідно до схеми – рис. 1.17)

Атака	Принцип дії та наслідки
Man-in-the-middle	Зловмисник порушує, перериває або підробляє зв'язок між двома системами. Наприклад, підроблені дані про температуру, «генеровані» пристроєм моніторингу навколишнього середовища, можна підробити та переслати в хмару. Аналогічно, зловмисник може вимкнути вразливі системи HVAC під час хвилі спеки, створюючи катастрофічний сценарій для постачальників послуг із ураженими моделями.
Крадіжка даних та особистих даних	Дані, створені незахищеними носовими та розумними пристроями, надають кіберзловмисникам велику кількість цільової особистої інформації, яку потенційно можна використати для шахрайських транзакцій та виявлення крадіжки.

Продовження табл. 1.4

Атака	Принцип дії та наслідки
Злам пристрою	Зловмисник захоплює пристрій і фактично бере на себе контроль над ним. Ці атаки досить важко виявити, оскільки зловмисник не змінює базову функціональність пристрою. Більше того, потрібен лише один пристрій, щоб потенційно повторно заразити всі розумні пристрої в домі. Наприклад, зловмисник, який спочатку зламав термостат, може теоретично отримати доступ до всієї мережі та віддалено розблокувати двері або змінити PIN-код клавіатури, щоб обмежити вхід.
Distributed Denial of Service (DDoS)	DoS-атака намагається зробити машину або мережевий ресурс недоступними для передбачуваних користувачів шляхом тимчасового або невизначеного зриву послуг хоста, підключеного до Інтернету. У разі розподіленої атаки відмови в обслуговуванні (DDoS), вхідний трафік, який переповнює ціль, надходить з кількох джерел, що ускладнює зупинку кібернаступу, просто блокуючи одне джерело. Насправді, DDoS-атаки стрімко зростають, насамперед через відсутність безпеки в пристроях IoT.
Permanent Denial of Service (PDoS)	PDoS, також відомі як флешинг, — це атака, яка настільки сильно пошкоджує пристрій, що вимагає заміни або перевстановлення обладнання. BrickerBot, закодований для використання жорстко закодованих паролів в пристроях IoT і спричинення постійної відмови в обслуговуванні, є одним із таких прикладів. Інший приклад може бачити, як підроблені дані надходять до термостатів, щоб завдати непоправної шкоди через екстремальний перегрів.

Висновок до першого розділу

На підставі результатів проведеного аналіз кібернетичних загроз для IoT–системи «розумний дім» доходимо висновку, що поруч з розвитком інженерних мереж та пристроїв супроводу життєзабезпечення, проблемою є саме особливість кіберфізичної системи як такої, оскільки існує загроза шляхом кібер-цифрової атаки безпосередньо впливати на фізичний рівень контрольованих пристроїв та мереж, що створює глобальну цивілізаційну загрозу та актуалізує дослідження та розробку рішень щодо захисту складових технології «інтернету речей». Виявлено, що найпоширенішою загрозою для IoT–системи «розумний дім» є втрата конфіденційної інформації, що призводить до втрати контролю над кіберфізичними керованими елементами і мережами інженерного супроводу життєдіяльності в локальному житловому середовищі.

РОЗДІЛ 2

РОЗРОБКА РІШЕНЬ З УДОСКОНАЛЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В IoT–СИСТЕМІ (КІБЕРФІЗІЧНІЙ СИСТЕМІ) «РОЗУМНИЙ ДІМ»

2.1 Моделювання кібернетичних загроз

Аналіз наукових праць, досліджень і публікацій [77 – 84] дозволяє виокремити найбільш вживані методи моделювання кіберзагроз, що в тому числі використовуються для тестування безпеки IoT–систем – табл. 2.1.

Таблиця 2.1

Найбільш вживані методи моделювання кіберзагроз, в тому числі для тестування безпеки кіберфізичних IoT–систем [77 – 84]

Метод моделювання	Загальна характеристика і принципи моделювання
STRIDE	STRIDE (Spoofing, Tampering, Disclosure, Information Disclosure, Denial of Service і Elevation of Privilege). Винайдений у 1999 році і прийнятий Microsoft у 2002 році, STRIDE на даний момент є найзрілішим методом моделювання загроз. STRIDE розвивався з часом, щоб включати нові таблиці для конкретних загроз і варіанти STRIDE-per-Element і STRIDE-per-Interaction. STRIDE оцінює детальний дизайн системи. Він моделює систему на місці. Створюючи діаграми потоків даних (DFD), STRIDE використовується для ідентифікації системних сутностей, подій і меж системи. STRIDE застосовує загальний набір відомих загроз на основі своєї назви, яка є мнемонікою. Категорії загроз STRIDE: Spoofing identify (ідентифікувати підробку); Tampering with data (підробка даних); Repudiation (відмова); Information disclosure (розкриття інформації); Denial of service (відмова в обслуговуванні); Elevation of privilege (підвищення привілею). STRIDE успішно застосовується в кібер-фізичних систем. Хоча Microsoft більше не підтримує STRIDE, він реалізується як частина життєвого циклу Microsoft SDL за допомогою засобу моделювання загроз, який все ще доступний.

Продовження табл. 2.1

Метод моделювання	Загальна характеристика і принципи моделювання
PASTA	PASTA (Process of Attack Simulation and Threat Analysis) – це методологія моделювання загроз, орієнтована на ризики, спільно заснована у 2015 році генеральним директором VerSprite Тоні УседаВелесом та лідером із безпеки Марко М. Морана. Організації в усьому світі, як-от GitLab, використовують PASTA як стандарт моделювання внутрішньої загрози через свій підхід, орієнтований на ризики, тенденції до співпраці, дані про загрози, засновані на доказах, і зосередженість на ймовірності кожної атаки. PASTA дозволяє співпрацювати між розробником і зацікавленими сторонами бізнесу, щоб по-справжньому зрозуміти ризики, властиві вашому додатку, його ймовірність атаки та вплив на бізнес у разі компромісу. Інші традиційні рамки моделювання загроз можуть бути гіперфокусовані на одному компоненті, наприклад, кодуванні або фактичній атаці. Цей метод піднімає процес моделювання загроз на стратегічний рівень, залучаючи ключових осіб, які приймають рішення, і вимагаючи внеску безпеки від операцій, управління, архітектури та розробки. Широко розцінений як структура, орієнтована на ризик, PASTA використовує перспективу, орієнтовану на зловмисників, щоб отримати результати, орієнтовані на активи, у формі перерахування загроз та оцінки.
LINDDUN	LINDDUN (можливість зв’язування, ідентифікація, невідповідність, виявлення, розкриття інформації, не інформованість, невідповідність) зосереджується на проблемах конфіденційності та може використовуватися для безпеки даних. LINDDUN, що складається з шести кроків, забезпечує систематичний підхід до оцінки конфіденційності. LINDDUN починається з DFD системи, яка визначає системні потоки даних, сховища даних, процеси та зовнішні об’єкти. Систематично перебираючи всі елементи моделі та аналізуючи їх з точки зору категорій загроз, користувачі LINDDUN визначають застосовність загроз до системи та будують дерева загроз.
CVSS	Загальна система оцінки вразливостей (CVSS) фіксує основні характеристики вразливості та створює числову оцінку серйозності. CVSS був розроблений NIST і підтримується Форумом груп реагування на інциденти та безпеки (FIRST) за підтримки та внеску CVSS Special Interest Group. Ця система призначена для того, щоб допомогти групам безпеки отримати доступ до загроз, виявити вплив та визначити існуючі контрзаходи. Це також допомагає фахівцям з безпеки оцінювати та застосовувати розвідку загроз, розроблену іншими, надійним способом. CVSS надає користувачам загальну стандартизовану систему оцінки на різних кібер-фізичних платформах. Оцінку CVSS можна обчислити за допомогою калькулятора, доступного в Інтернеті. Оцінка CVSS визначається на основі значень, призначених аналітиком для кожного показника. Показники докладно описані в документації. Метод CVSS часто використовується в поєднанні з іншими методами моделювання загроз. CVSS враховує притаманні властивості загрози та вплив фактора ризику через час з моменту першого виявлення вразливості. Він також включає заходи, які дозволяють командам безпеки спеціально змінювати оцінки ризику на основі окремих конфігурацій системи.

Продовження табл. 2.1

Метод моделювання	Загальна характеристика і принципи моделювання
Attack Trees	Використання дерев атак для моделювання загроз є одним із найстаріших і найбільш широко застосовуваних методів у кібер-системах, кіберфізичних системах і суто фізичних системах. Дерева атак спочатку застосовувалися як окремий метод і з тих пір поєднувалися з іншими методами та структурами. Дерева атак – це діаграми, які зображують атаки на систему у вигляді дерева. Корінь дерева — це мета атаки, а листя — шляхи досягнення цієї мети. Кожна ціль представлена у вигляді окремого дерева. Таким чином, аналіз системних загроз створює набір дерев атак. У разі складної системи дерева атак можна побудувати для кожного компонента, а не для всієї системи. Адміністратори можуть будувати дерева атак і використовувати їх для прийняття рішень щодо безпеки, для визначення, чи є системи вразливими до атаки, і для оцінки конкретного типу атаки.
Persona non Grata	Підхід Persona non Grata, розроблений в Університеті ДеПола, робить моделювання загроз більш зручним, просить користувачів зосередитися на зловмисниках, їх мотивації та здібностях. Після завершення цього кроку користувачам пропонується обдумати цілі та ймовірні механізми атаки, які зловмисники розгорнуть. Persona non Grata зосереджується на мотивації та навичках людейнападників. Він характеризує користувачів як архетипи, які можуть неправильно використовувати систему, і змушує аналітиків розглядати систему з точки зору ненавмисного використання. Теорія цього підходу полягає в тому, що якщо інженери зможуть зрозуміти, якими можливостями може володіти зловмисник і які типи механізмів вони можуть використовувати для скомпрометації системи, інженери отримають краще розуміння цілей або слабких місць у своїх власних системах і ступінь які вони можуть бути скомпрометовані.
Security Cards	Картки безпеки – це методологія, заснована на мозковому штурмі та креативному мисленні, а не на підходах до структурованого моделювання загроз. Він розроблений, щоб допомогти командам безпеки враховувати менш поширені або нові атаки. Цей метод використовує колоду з 42 карт для полегшення діяльності з виявлення загроз: Вплив людини (9 карт), Мотивація супротивника (13 карт), Ресурси противника (11 карт) і Методи противника (9 карт). Картки безпеки визначають незвичайні та складні атаки. Це не формальний метод, а, скоріше, свого роду техніка мозкового штурму.
hTMM	Метод гібридного моделювання загроз (hTMM) був розроблений SEI у 2018 році. Він складається з комбінації SQUARE (метод інженерних вимог до якості безпеки), карток безпеки та дій PnG. Цільові характеристики методу включають відсутність помилкових спрацьовувань, відсутність упущених загроз, постійний результат незалежно від того, хто моделює загрозу, а також економічну ефективність.

Продовження табл. 2.1

Метод моделювання	Загальна характеристика і принципи моделювання
Quantitative Threat Modeling Method	Цей гібридний метод складається з дерев атаки, методів STRIDE та CVSS, які використовуються в синергії. Він спрямований на вирішення кількох нагальних проблем із моделюванням загроз для кіберфізичних систем, які мають складну взаємозалежність між своїми компонентами. Першим кроком методу кількісного моделювання загроз (Quantitative TMM) є створення дерев компонентних атак для п'яти категорій загроз STRIDE. Ця активність показує залежності між категоріями атак і атрибутами низькорівневих компонентів. Після цього застосовується метод CVSS і обчислюються бали для компонентів дерева.
Trike	Trike був створений як система аудиту безпеки, яка використовує моделювання загроз як техніку. Він розглядає моделювання загроз з точки зору управління ризиками та захисту. Щоб оцінити ризик атак, які можуть вплинути на активи через CRUD, Trike використовує п'ятибальну шкалу для кожної дії на основі її ймовірності. Актори оцінюються за п'ятибальною шкалою ризиків, які вони, як передбачається, представляти (менше число = вищий ризик) для активу. Крім того, актори оцінюються за тривимірною шкалою (завжди, іноді, ніколи) для кожної дії, яку вони можуть виконати з кожним активом.
VAST Modeling	Методологія візуального, швидкого та простого моделювання загроз (VAST) була розроблена після огляду недоліків та проблем із впровадженням, притаманних іншим методологіям моделювання загроз. Основний принцип полягає в тому, що для ефективного моделювання загроз має масштабуватися в інфраструктурі та всьому портфоліо DevOps, безперешкодно інтегруватися в середовище Agile і забезпечувати ефективні, точні та послідовні результати для розробників, команд безпеки та керівників вищого рівня.
OCTAVE	OCTAVE — це гнучка методологія, яка дозволяє невеликій команді, що складається з операційного персоналу та IT, працювати разом для задоволення потреб організації в безпеці. Метод оцінки оперативно-критичних загроз, активів та вразливості (OCTAVE) — це метод стратегічної оцінки та планування кібербезпеки на основі оцінки ризиків. Він був створений відділом CERT SEI у 2003 році та доопрацьований у 2005 році. OCTAVE зосереджується на оцінці організаційних ризиків і не розглядає технологічні ризики. Його основними аспектами є операційний ризик, методи безпеки та технології. Існує кілька варіацій OCTAVE, які корисно знати, якщо стандартний OCTAVE не відповідає вашій ситуації.

Приклад реалізації data-моделі атаки і захисту на кіберфізичну IoT–систему, що передбачає застосування методу і принципів STRIDE вказано на рис. 2.1 [77 – 84].

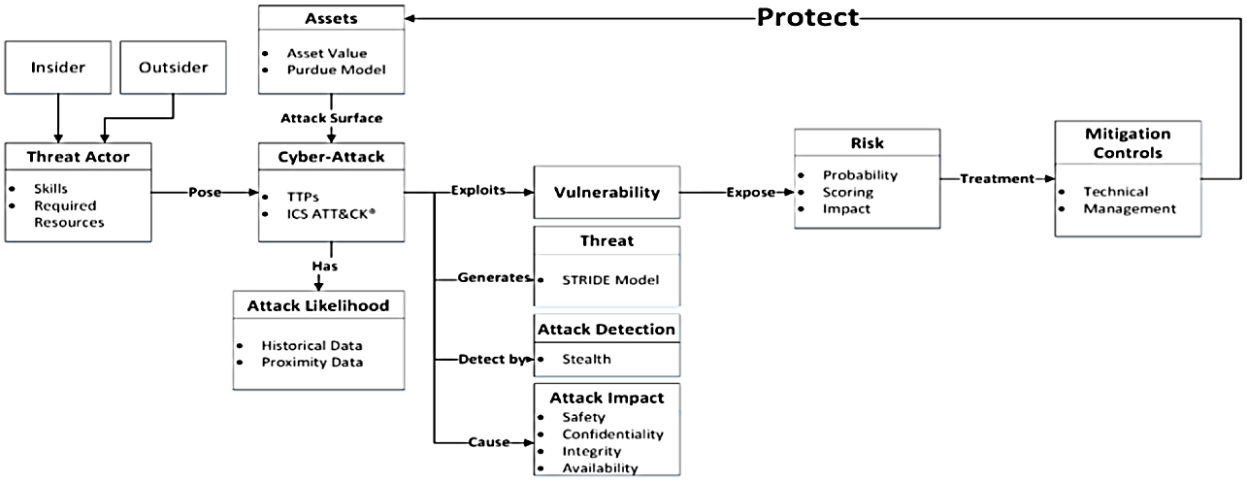

Рисунок 2.1 – Приклад реалізації data-моделі атаки і захисту на кіберфізичну IoT–систему, що передбачає застосування методу і принципів STRIDE

Відповідно до зазначеної моделі (рис. 2.1) формується диференціально-критеріальна система оцінка рівня загрози кіберфізичній IoT–системі – табл. 2.2. Зазначена система формує критеріальну матрицю – рис. 2.2.

Таким, чином продукується відповідна послідовність у виконанні операцій з моделювання кібернападу на IoT–систему – рис. 2.3 [77 – 84].

Таблиця 2.2

Диференціально-критеріальна система оцінка рівня загрози кіберфізичній IoT–системі [63 – 76]

Data Model parameter	Criteria Description for each level				
	Very High – 5	High – 4	Moderate – 3	Low – 2	Very Low – 1
Threat Actor					
Skills: what level of skill or knowledge is required by the adversary to conduct the cyber-attack	High skills with knowledge about target ICPS	High skills without knowledge about target ICPS	Some knowledge about target ICPS	Generic technical skills	No skills and no knowledge about target ICPS
Required Resources: tools and software resources required to conduct the cyber-attack	Significant resources about target ICPS are available	Significant resources available but not related to target ICPS	Some resources available related to target ICPS	Minimal resources available, not related to target ICPS	No resources available and required to be developed
Assets					
Asset Value: reflects ICPS asset criticality based on Purdue Model levels	Level-1 assets	Level-2 assets	Level-3 assets	Level-3.5 assets	Level-4&5 assets
Vulnerability					
Vulnerability: How vulnerable is the target asset to be exploited	Published vulnerabilities and known vulnerabilities on ICPS with significant impact	Known vulnerabilities with high impact on ICPS	Customised tools required to identify ICPS vulnerabilities with high impact on ICPS	Customised tools required to identify ICPS vulnerabilities with low impact on ICPS	Customised tools required for vulnerability discovery on patched ICPS
Attack Impact					
Confidentiality: impact measure on loss of ICPS confidentiality from a successful cyber-attack	Severe impact	High impact	Limited impact	Minor impact	No impact
Integrity: impact measure on loss of ICPS integrity from a successful attack	Severe impact	High impact	Limited impact	Minor impact	No impact
Availability: impact measure on loss of ICPS availability from a successful cyber-attack	Severe impact	High impact	Limited impact	Minor impact	No impact
Safety: impact measure on loss of ICPS safety from a successful attack	Severe impact	High impact	Limited impact	Minor impact	No impact
Attack Likelihood					
Likelihood: How frequent a cyber-attack could happen for ICPS based on historical data and future expectations	Happened in past 3 years for target ICPS industry sector or expected to occur in the next 6 month	Happened in past 6 years for target ICPS industry sector or very likely to occur in next 1 year	Happened in the past 10 years for target ICPS sector or likely to occur in next 3 years	Happened in the past 10 years for target ICPS sector or likely to occur in next 6 years	Not happened in the past or likely to occur in next 10 years
Attack Detection					
Stealth: How detectable is the conducted cyber-attack	Not detectable	Detection possible with customised monitoring tools and high forensic skills	Detection possible with customised monitoring	Detection possible with some forensic skills	Detection without any monitoring tools

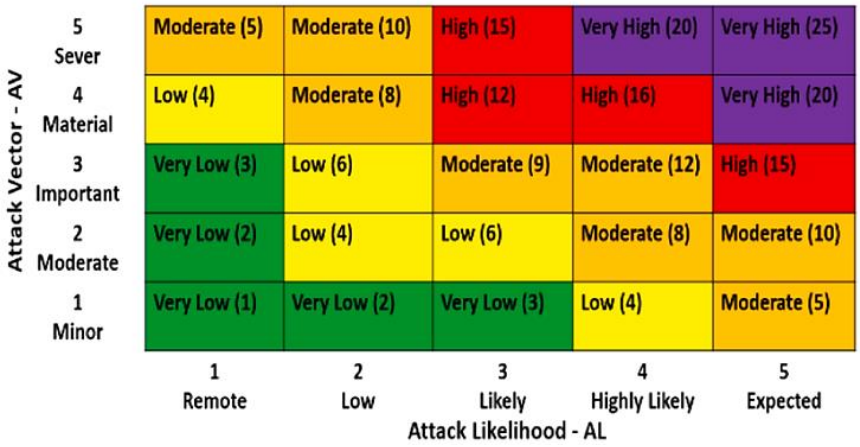

Рисунок 2.2 – Критеріальна матриця оцінки рівня кіберзагрози IoT–системі

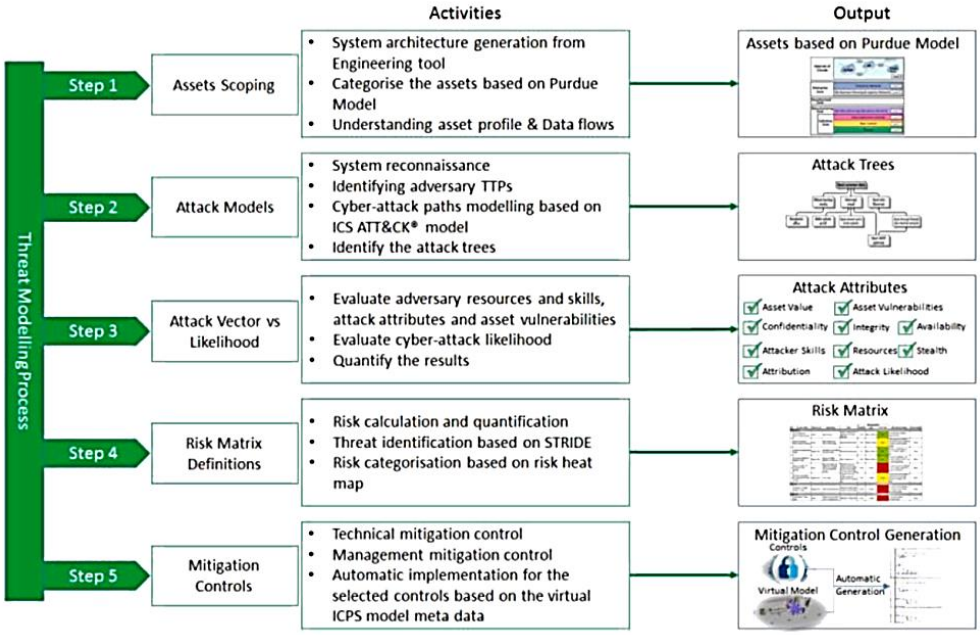

Рисунок 2.3 – Покроковий алгоритм функціонування data-моделі атаки і захисту на кіберфізичну IoT–систему, що передбачає застосування методу і принципів STRIDE

Для моделювання кібернетичних загроз на досліджувану кіберфізичну систему «розумний дім» використовують метод і принципи OCTAVE. Приклад data-моделі атаки і захисту на кіберфізичну IoT–систему розумний дім зазначено на рис. 2.4 [77 – 84].

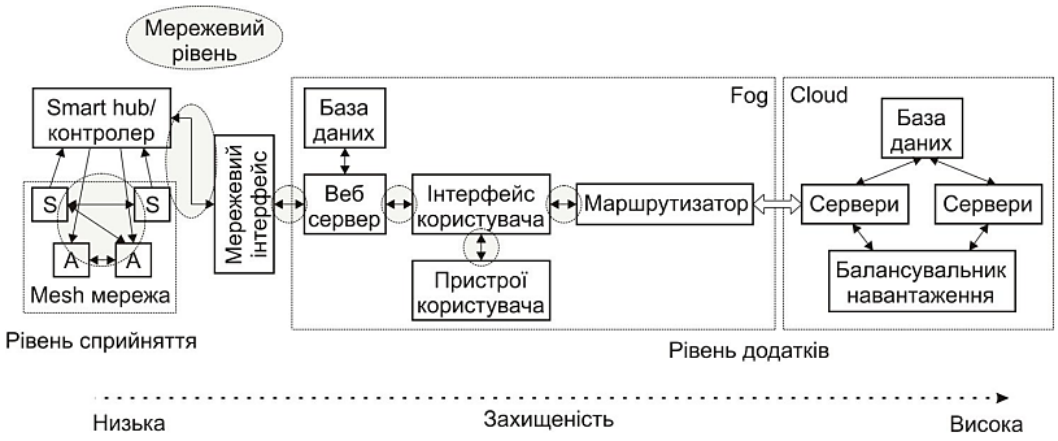

Рисунок 2.4 – Приклад реалізації data-моделі атаки і захисту на кіберфізичну IoT–систему «розумний дім», що передбачає застосування методу і принципів OCTAVE

Відповідно зміниться і послідовність моделювання кібернападу, згідно з принципами моделювання OCTAVE в рамках можливих кіберзагроз для IoT–системи «розумний дім» – рис. 2.5 [77 – 84].

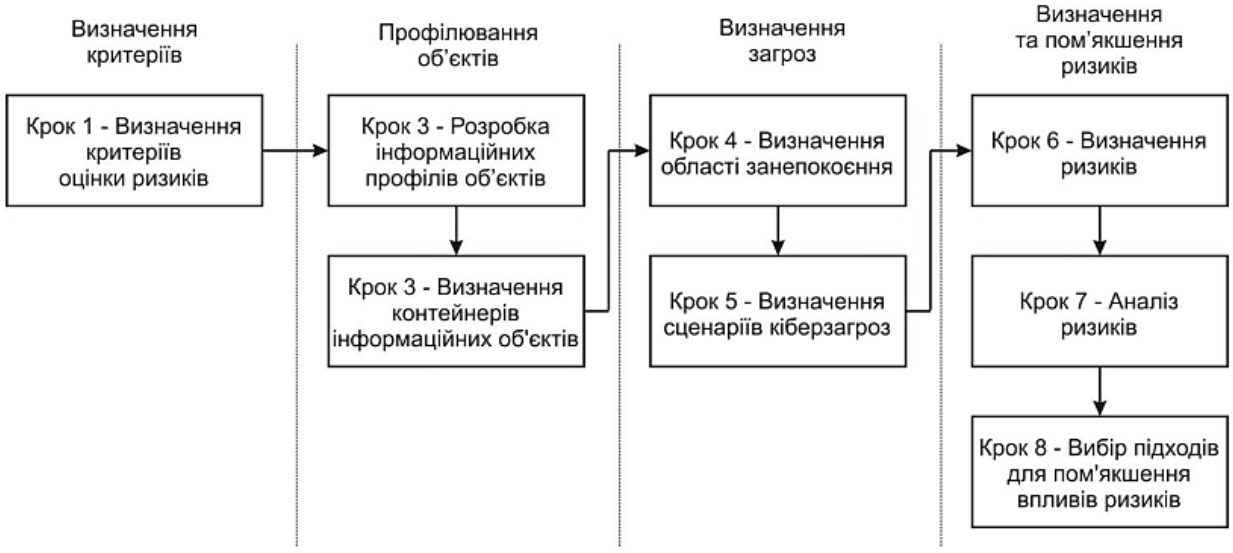

Рисунок 2.5 – Покроковий алгоритм функціонування data-моделі атаки і захисту на кіберфізичну IoT–систему «розумний дім», що передбачає застосування методу і принципів OCTAVE

Відповідно встановлено, що наразі існує достатня кількість методів та інструментаріїв моделювання кіберзагроз і кібернападу, що успішно

використовуються для тестування і пошуку загроз безпеки кіберфізичних систем на базі технології IoT та можуть бути застосовані безпосередньо для моделювання кібер-цифрових атак на комплекс пристроїв та мереж інженерного супроводу життєдіяльності «розумний дім».

2.2 Розробка математичного апарату для моделювання кібернетичних загроз

Відповідно до результатів аналізу наукових праць та публікацій [85 – 89], встановлені типи розроблених та впроваджених математичних апаратів, що використовуються для моделювання кібер-цифрових атак у т. ч. на кіберфізичні IoT–системи – табл. 2.3.

Таблиця 2.3

Дослідження вживаності існуючих математичних апаратів для моделювання кібер-цифрових атак на кіберфізичних IoT–систем [85 – 89]

Математичний апарат	Загальний опис
Традиційний підхід до моделювання поведінки агентів у системах безпеки	Метою тесту на вторгнення в мережу є виявлення потенційних вразливостей у мережі, доступної потенційному зловмиснику. Знаючи про вразливості мережі, тестувальник/зловмисник може використовувати їх для подальшого проникнення в мережу для отримання додаткової інформації. Цей тестувальник вторгнень використовуватиме цю інформацію, щоб виявити більше вразливостей, доки зловмисники не вичерпають усі свої можливості. Для цього розробляється так званий граф атаки, який являє собою набір усіх можливих шляхів, якими може пройти зловмисник у мережі. Цей процес традиційно виконується вручну зловмисником або групою аналітиків і може бути виснажливим процесом. Процес формалізовано для автоматичного створення повного набору можливих графіків атак для даної мережі. Графіки атак генеруються на основі опису мережі та знань зловмисника про цю мережу. з наступним описом набору станів, які описують фактичні атаки, які можуть статися. Змодельовано мережу з двох хостів з IDS (IDS – Intrusion Detection System) та брандмауером. Результатом був графік атаки з 5948 вузлів з 68 364 ребрами, що є надзвичайно великим для дуже невеликої кількості типів атак і нереально маленької мережі. Цей метод аналізу не є гнучким, масштабованим або простим у використанні, що необхідно для успішної оцінки недоліків мережі. Описано використання графіків атак для створення шаблонів сповіщень IDS для спрогнозування майбутніх і поточних атак. Використовуючи ці графіки атак і знання області кібератак, можна оцінити ймовірність досягнення цілей атаки для прогнозування майбутніх атак. Цей метод вимагає, щоб кожен графік атак був перетворений в мережу, а експерт з кібербезпеки аналізував його, щоб визначити ймовірність успішної кібератаки. Цей підхід має дві проблеми: перші атаки, які не суворо дотримуються плану атаки, неможливо змоделювати, а ймовірність базується виключно на досвіді експерта. Визначте лише різні шляхи, якими може йти зловмисник, а не те, чи здійснить зловмисник насправді цю атаку чи ні.
Агентно-орієнтовані моделі сторін кібер-конфлікту	При розробці програм для моделювання поведінки агентів необхідно відповісти на питання, як моделювати процеси прийняття рішень агентами в системі безпеки. У обчислювальній соціальній науці загалом і в області агентного соціального моделювання (ABSM), зокрема, ведеться постійна дискусія про найкращий спосіб моделювання прийняття рішень людиною. Причина цього в тому, що більшість обчислювальних моделей процесу прийняття рішень досить прості. Як і будь-яка хороша наукова модель, при моделюванні поведінки людини об’єкти, що моделюються, слід аналізувати з точки зору лише тих властивостей, які мають відношення до даного сценарію поведінки. Для ABSM було розроблено велику кількість архітектур і моделей, які намагаються представити процес прийняття рішень людиною. Незважаючи на спільну мету, кожна архітектура має дещо різні цілі і, як наслідок, включає різні припущення та спрощення. Тому знання цих відмінностей є важливим при виборі моделі рішення агента в ABSM.

Продовження табл. 2.3

Математичний апарат	Загальний опис
Теоретико-ігрові моделі конфліктних ситуацій	Підходи, засновані на теорії ігор, у багатьох відношеннях перевершують традиційні рішення щодо кібербезпеки та конфіденційності мережі, включаючи наступне: математична обґрунтованість та доказовість. Більшість традиційних рішень безпеки, які реалізуються або в пристроях запобігання (наприклад, брандмауери), або в засобах швидкого реагування на загрози (наприклад, антивірусні програми), спираються лише на евристики. Тим не менш, теорія ігор може досліджувати рішення безпеки за допомогою математично обґрунтованих методів, правильність і ефективність яких можна математично обґрунтувати; надійний захист. На основі аналітичних результатів застосування методів теорії ігор можна розробити надійні механізми захисту кіберсистем від егоїстичної поведінки (внутрішніх або зовнішніх атак) зловмисних користувачів/вузлів; своєчасне реагування. Хоча прийняття традиційного рішення щодо безпеки відбувається досить повільно через відсутність стимулів для учасників, теоретико-ігрові підходи відстоюють інтереси захисників, використовуючи основні механізми стимулювання в контексті виділення обмежених ресурсів для збалансування передбачуваних ризиків; розподілені рішення. Більшість традиційних механізмів захисту приймають рішення централізовано, а не індивідуально (або розподілено). В іграх із мережевою безпекою централізований підхід майже неможливий через відсутність координатора в автономній системі. Використовуючи відповідні моделі теорії ігор, рішення безпеки будуть реалізовані розподіленим чином. Теоретико-ігровий аналіз зосереджується на визначенні ймовірної поведінки гравців щодо вибору стратегії, таким чином визначаючи передбачуваний результат гри. Що моделі, засновані на теорії ігор, демонструють переваги в продуктивності та вартості порівняно з іншими моделями управління ризиками, пов’язаними з кіберзлочинністю.
Системно-динамічні моделі конфліктно-кооперативної взаємодії агентів	При розробці моделі поведінки в першу чергу необхідно визначити межу застосовності моделі та основні припущення, що входять до неї. Запропонована модель орієнтована на динаміку взаємодії зловмисника і захисника у сфері інформаційної безпеки для визначення інвестиційних стратегій, які використовують опоненти. Модель представляє компанію як захисника, який захищає актив від групи зловмисників, які намагаються порушити безпеку активу компанії за допомогою зловмисних кібератак. Актив може мати багато форм, наприклад, список клієнтів, веб-сайт, реєстр кредиторської заборгованості або стратегічний план. Підвищений рівень безпеки може бути пов’язаний із захистом конфіденційності, цілісності, автентичності або доступності активу для авторизованих користувачів. Моделювання обмежується трьома можливими векторами загрози. Захист від кожного з векторів загроз реалізується в результаті інвестування у відповідний захист. Захист вважається ефективним, якщо він може компенсувати вхідні атаки.

На підставі визначених методів математичного моделювання кібер-цифрових загроз для IoT–систем (табл. 2.3), заважаючи на особливості для

кожного з досліджуваних методів, доходимо висновку, що для розробки математичного апарату моделювання кібернападу безпосередньо на кіберфізчину систему «розумний дім» доцільно застосувати теорію ігор, що адаптується під диференціально-ігрову модель, оскільки за результатами аналізу кіберзагроз (п. 1.3 цієї праці) встановлено, що для досліджуваної IoT–системи найбільш вірогідною загрозою є втрата конфіденційної інформації, внаслідок чого зловмисники можуть отримати контроль над виконавчими елементами інженерного супроводу життєдіяльності [85 – 89].

Розробка зазначеної математичної моделі провадиться покроково:

1 Визначення множини станів кіберфізичної системи інформаційної безпеки (СІБ). За результатами дослідження кіберзагроз та фактично здійснених кібератак (табл. 1.3 цієї праці) встановлено, що для кіберфізичної системи «розумний дім» найбільш вірогідними загрозами є (за частотою виявлення):

– втрата конфіденційної інформації – «конфіденційність»;

– атаки на елементи та мережі IoT–системи інженерного супроводу життєдіяльності – «цілісність»;

– блокування доступу до елементів та мережі кіберфізичної системи «розумний дім» – «доступність».

Зазначені характеристики є складовими безпеки інформаційного ресурсу (ІР) розумного дому та складає множину параметрів, що визначається за показником інтенсивності реалізації кібератак (КБа) $\mu_i(t)\left(i=\overline{1,n}\right)$ (n – кількість КБа), відмов СІБ $\beta_i(t)$, знаходження вразливостей $\gamma_i(t)$, тощо. В кіберфізичній системі «розумний дім» центральним контролером має визначатись множина можливих станів $\{P_z(t)\}$ (де $P_z(t)$ – ймовірність перебування СІБ у яких може бути досліджувана IoT–система; $z=\overline{0,c}$, c – кількість можливих станів СІБ.

2 Вибір стратегії кіберзахисту (КБз). Відповідно до отриманої множини станів СІБ $\{P_z(t)\}$, типізації кібіратак (КБа), а також параметрів останніх, центральним контролером IoT–системи «розумний дім» має обиратись

стратегія кіберзахист (КБз), що відповідно до результатів дослідження наукових праць та публікацій [85 – 89] може бути наступною:

– стратегія побудови СІБ реального часу (РЧ);

– стратегія ешелонованого захисту (СЕЗ);

– стратегія відведення гравця КБн на псевдосервіс (ПсС);

– стратегія відведення гравця КБн на псевдосервіс з подальшим втягуванням його в кібератаці (інформаційному конфлікті – ІК) (ПсС та ІК);

– стратегія КБз, що характеризується змінними потоками захисних дій (ЗП); стратегія розподіленого (Р) захисту.

За результатами визначеною стратегії формується граф станів кіберфізичної системи, що зазнала впливу кібератаки, відповідно до чого формується модель кібератаки (КБа для ІК), що є основою для загального моделювання кібернападу (КБн).

3 Застосування методу диференціально-ігрового моделювання для оптимізації стратегії кіберзахисту (КБз) та оцінювання рівня захищеності кіберфізичної системи «розумний дім» (РЗ) [85 – 89] (оптимізація стратегій КБз та оцінювання РЗ). Оптимізація здійснюється на основі визначеної стратегії кіберзахисту (КБз) $\lambda_{zmin}^{opt(t)}$ та оцінки прогнозованого рівня захищеності (РЗ) – $I^*\left(\lambda_{zmin}^{opt_{zmin}^{opt}}\right)$. Процедура оцінювання здійснюється за параметром поточного значення I та прогнозованого I^*, значення яких варіюються в інтервалі $I, I^* \in [0,1]$. Тобто, ближче значення I до нульового, тим вищий рівень захисту досліджуваної IoT–системи (вищий показник РЗ).

4 Прогнозування динаміки розвитку кібернападу (КБн). Використовуючи однокритерійні диференціально-ігрові моделі (ОДІМ) $P_0^{NT}(t)$, $P_{0_P}^{G^{Lopt}}(t)$ та $P_0^{opt}{}_i(t)$ здійснюється прогнозування динаміки розвитку кібернападу $P_0^{opt}(t)$. Для системи ОДІМ, крім оцінювання за вищевказаними параметрами $\lambda_{zmin}^{opt(t)}$ та I^*, додатково вводяться вимоги до похибки моделі 2^q (де q – кількість дискрет, які враховуються для диференціальних спектрів (ДС) $P_0(k)$ при побудові

відповідної моделі (k – цілочисловий аргумент, $k =: 0,1,2,\ldots$), її точності y^*, а також діапазону прогнозування $t \in [t_0, T]$, на якому вона працює із заданими характеристиками.

Виходячи з висунутих вимог обирається один з трьох диференціально-ігрових методів моделювання [85 – 89]:

– метод моделювання на основі нетейлорівських перетворень (НТ) – «метод НТ»;

– метод гібридного (ГБ) моделювання – «метод ГБ»;

– метод числово-аналітичного моделювання (ЧАМ) – «метод ЧАМ».

Відповідно до визначеного методу моделювання створюється диференціально-ігрова модель (ДІМ) прогнозування динаміки розвитку кібернападу (КБн), що визначається з наступних можливих варіацій (згідно з переліком вищезазначених) [85 – 89]:

– $P_0^{NT}(t)$ – НТ–ДІМ;

– $P_{0_P}^{G^{Lopt}}(t)$ – ГБ (P–L)–ДІМ;

– $P_0^{NT}(t)$ – НД(неперервна-дискретна)–ДІМ.

Варто зауважити, що за результатами огляду публікацій [85 – 89] встановлено, що найточнішим методом прогнозування динаміки розвитку кібернападу є ГБ (P–L)–ДІМ.

5 Оптимізація ресурсів, залучених до кіберзахисту (КБз) та оцінка рівня захищеності (РЗ) IoT–системи «розумний дім». Мета цього етапу моделювання полягає в оптимізації обмеженого ресурсу системи кіберзахисту «розумного дому» $\lambda_{zmin}^{opt(t)}$, звісно, з урахуванням суворого дотримання умови $I^* \to I_0^{VR}$ (де I_0^{VR} – вартість гри). Супутня мета – підвищення достовірності значення I^* та рівня адекватності визначених ДІМ

$P_0^{opt^{VR}}(t)$. Механізм реалізації процесів оптимізації ресурсів та оцінки РЗ виконується центральним контролером IoT–системи «розумний дім» шляхом впровадження додаткових критеріїв $\mathrm{I}_j = \hat{\mathrm{O}}_j[\lambda_i(t), \mu_i(t), T, P_0(t)]$ (де $\hat{\mathrm{O}}_j$ – функції, що мають неперервні частинні похідні за $\lambda_i(t)$ та $\mu_i(t)$), що є

характеристиками функціонування кіберфізичної системи, що зазнала впливу кібератаки. Частинні критерії I_j є компонентами r –мірного векторного критерію $I_0 = \overline{I_1, I_r}$, який обмежений допустимою областю $I_0 \in M$.

6 Оцінювання ефективності застосовуваної системи інформаційної безпеки (СІБ) кіберфізичної системи «розумний дім». Центральний контролер досліджуваної IoT–системи визначає найефективнішу альтернативу $I_{0\theta}^{(j)^*}$ з можливих, тобто $I_{0\theta}^{(j)^*} \in \left\{I_{0\theta}^{(j)}\right\}$ (де j – показник ієрархічності частинних критеріїв, θ – оцінювані властивості). Надалі, для оцінюваної множини властивостей визначається коефіцієнт пріоритету – ф. (2.1) [85 – 89]:

$$\alpha_{S\theta}^{(j-1)} = f_{S\theta}\left[\sum_{S=1}^{L_\theta^{(j-1)}} f_{S\theta}\right]^{-1}, \theta \in \left[1, L^{(j)}\right], j \in [2, m], \qquad (2.1)$$

де $\alpha_{S\theta}^{(j-1)}$ – S –а компонента вектору пріоритету критерію на $(j-1)$–у рівні ієрархії при розрахунках ефективності θ –ї властивості j –го рівня$S \in \left[1, L^{(j-1)}\right]$;

$L^{(j-1)}$– кількість частинних критеріїв, за якими оцінюється ефективність функціонування системи кіберзахисту «розумного дому» на $(j-1)$–у рівні ієрархії;

$f_{S\theta}$ – оцінка важливості S –ї властивості $(j-1)$–го рівня ієрархії для θ –ї властивості j –го рівня, що визначена центральним контролером IoT–системи «розумний дім» за бальною шкалою.

Таким чином, знаходяться кількісні та якісні оцінки ефективності системи $\left\{I_{0\theta}^{(j)^*}, I_{\text{Å}\hat{O}}\right\}$, де $I_{\text{Å}\hat{O}}$ – базова терм-множина лінгвістичної змінної, яка визначається п’ятьма термами – ф. (2.2):

$$I_{\text{Å}\hat{O}} = \bigcup_{i=1}^{5} I_{\text{Å}\hat{O}} \Rightarrow \begin{Bmatrix} "абсолютнонеефективна"(АН), \\ "недостатньоефективна(НЕ), \\ "ефективна"(Е), \\ "достатньоефективна"(ДЕ), \\ "абсолютноефективна"(АЕ) \end{Bmatrix} \qquad (2.2)$$

2.3 Формування рішення з удосконалення захисту інформації в IoT–системі «розумний дім» на базі новітніх методів шифрування службового спілкування елементів досліджуваної кіберфізчиної системи

Аналіз публікацій та наукових праць [90 – 101], з урахуванням виявлених найбільш актуальних та найбільш застосовуваних кібер-цифрових загроз для досліджуваної кіберфізичної системи «розумний дім», дозволяє виокремити найперспективніші вектори розвитку систем інформаційної безпеки цієї IoT–системи – табл. 2.4.

Таблиця 2.4

Дослідження сучасних концепцій підвищення рівня захищеності кіберфізичних IoT–систем «розумний дім» [90 – 100]

Перспективна технологія кіберзахисту	Загальний опис
Архітектурний метод з трьома модулями для збереження конфіденційності аналізу даних для розумних будинків	Запропоновано архітектурний метод з трьома модулями для захисту конфіденційності аналізу даних для розумних будинків. Модуль збору даних регулярно збирає дані своїх датчиків та надсилає їх модулю приймача даних. Той перетворює та зберігає їх у двох різних наборах даних. Модуль результатів контролює доступ до результатів обробки даних для захисту конфіденційності. Діяльність цього модуля можна класифікувати на чотири групи. Перший – модуль контролю доступу, який автентифікує, авторизує та визначає рівень конфіденційності для будь-якої спільної інформації. Другий — модуль ретривера ідентифікаторів. Він запитує сховище словника ідентифікаторів для створення списку персональних (як фактичних, так і хешованих значень) даних, до яких кінцевий користувач має право доступу. Модуль трансформатора за допомогою цього списку узагальнює фактичні особисті значення та створює набір даних із хешованими, фактичними та узагальненими значеннями. Модуль процесора результатів запускає завдання на ідентифікованому сховищі та замінює хешовані особисті значення в наборі результатів відповідними узагальненими значеннями на основі виходу модуля трансформатора. Цей метод забезпечує доступ до даних лише справжньому користувачеві.

Продовження табл. 2.4

Метод обмеження на рівні мережі	Продемонстровано, що на позаштатних пристроях IoT відсутні базові гарантії безпеки, зламавши різноманітні пристрої розумного дому, включаючи лампочку, вимикач та димовий сигнал. Вони запропонували рішення щодо захисту таких пристроїв шляхом обмеження доступу на рівні мережі. Щоразу, коли до мережі підключений новий пристрій IoT, користувач мережі, адміністратор або навіть Інтернет-провайдер може запитувати метод захисту від постачальника SaaS. Це рішення не вимагає змін від виробників пристроїв, воно зменшує навантаження на кінцевих користувачів і дозволяє забезпечити безпеку як послугу накладення Інтернетпровайдером або спеціалізованим постачальником в хмарі. Метод не узагальнений на інші пристрої розумного дому. Як недолік, вразливість від атак, здійснених смартфонами користувачів.
Технологія Blockchain	Блокчейн – це структурована база даних, «ланцюжок блоків», де кожен блок пов'язаний з попереднім (рис. 2.6). Блок містить в собі набір записів (інформацію). Кожен новий блок з інформацією додається в кінець ланцюжка. Кожному блоку присвоюється цифровий підпис – хеш–сума, що є унікальним ідентифікатором. Хеш (hash) – це унікальний код, який змінюється при зміні навіть одного символу в тексті, розраховується за складною математичною формулою і завжди буде однаковим для однієї і тієї ж інформації. Отже, не може бути два різних хеша для абсолютно однакової інформації, тому «розірвати ланцюг», тобто внести правки у блок або додати блок між іншими неможливо. Пропонується розподілене та надійне зберігання інформації IoT на основі комбінації IPFS та алгоритму шифрування. Інформація IoT зберігається в системі IPFS, а повернене хеш-значення шифрується для зберігання шифротексту в Blockchain. Авторизовані користувачі можуть отримати хеш-значення унікального індексу, що зберігається у системі IPFS, через смарт-контракт для підтвердження дозволу. Правило відповіді заздалегідь встановлено у смарт-контракті. Коли користувачеві потрібно отримати доступ до інформації про дані, потрібно ініціювати транзакцію, а інші вузли в Blockchain перевіряють транзакцію, і коли верифікація проходить і встановлене правило доступу дотримується, авторизацію можна отримати.

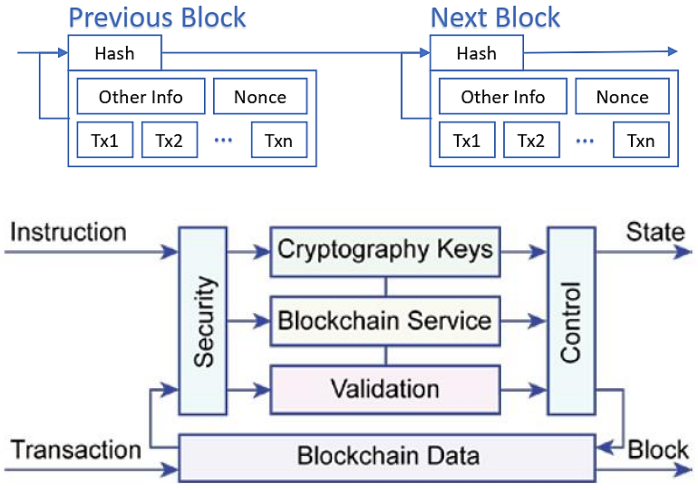

Рисунок 2.6 – Концепт-схема Blockchain–технології

Останнім часом на Blockchain–технологію (BC) все частіше звертають увагу розробники кіберфізичних систем «розумний дім», що засвідчується дотичними показниками – частотою пошуку за синергетичним запитом через глобальний пошуковий сервіс Google (субсервіс Google Trends) – рис. 2.7 [90 – 100].

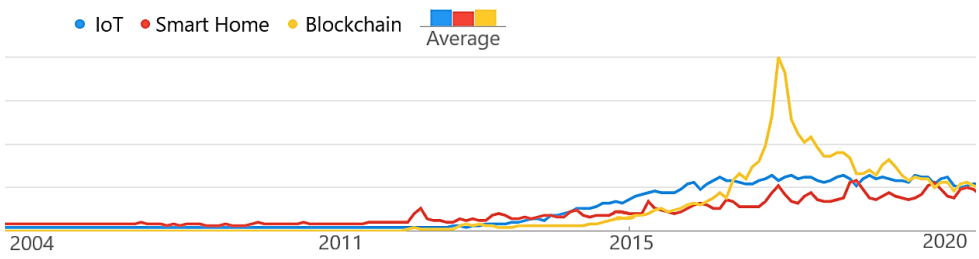

Рисунок 2.7 – Динаміка синергетичного пошуку для захисту кіберфізичних IoT–систем «розумний дім» Blockchain–технологію (за даними глобального пошукового сервісу Google (субсервіс Google Trends))

Також виявлений зв'язок BC–технології з іншими сучасними цифровими доробками для базової технології IoT для різних кіберфізичних систем, що в подальшому формують майбутнє цифрових технологій та визначають цивілізаційний вектор розвитку людства – рис. 2.8 [90 – 100].

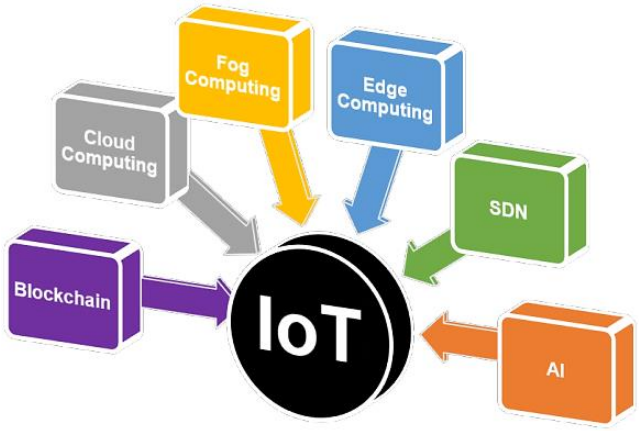

Рисунок 2.8 – Синергетична схема зв’язку сучасних цифрових технологій з кіберфізичними системами IoT

В публікаціях [90 – 100] сформовано декілька концепцій улаштування ВС–технології для захисту інформаційної безпеки кіберфізичної IoT–системи «розумний дім», що представлені на рис. 2.9 – 2.11 [90 – 100].

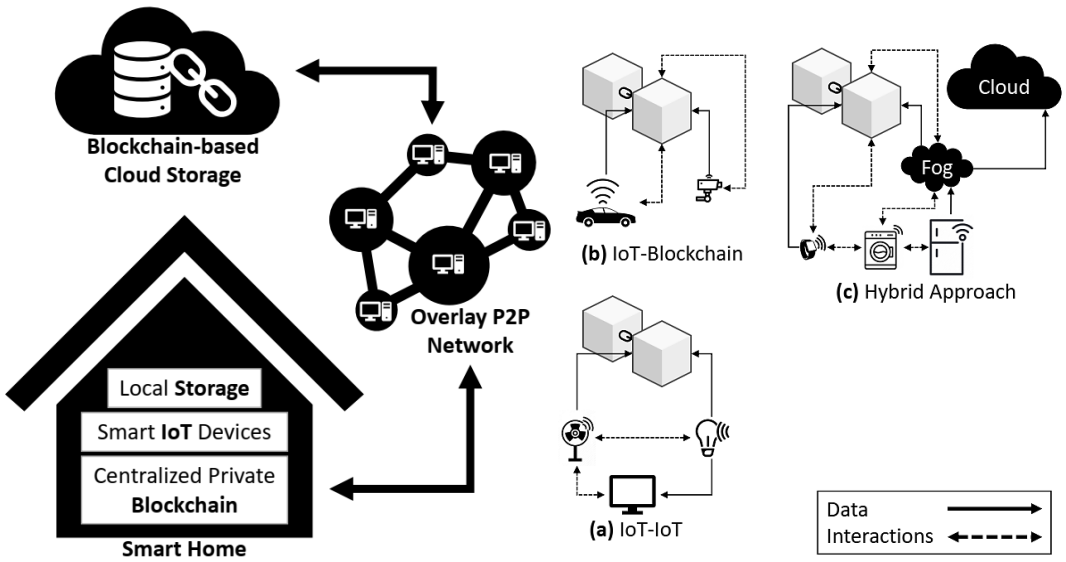

Рисунок 2.9 – Концепт-схема застосування ВС–технології для інформаційного захисту кіберфізичної IoT–системи «розумний дім»

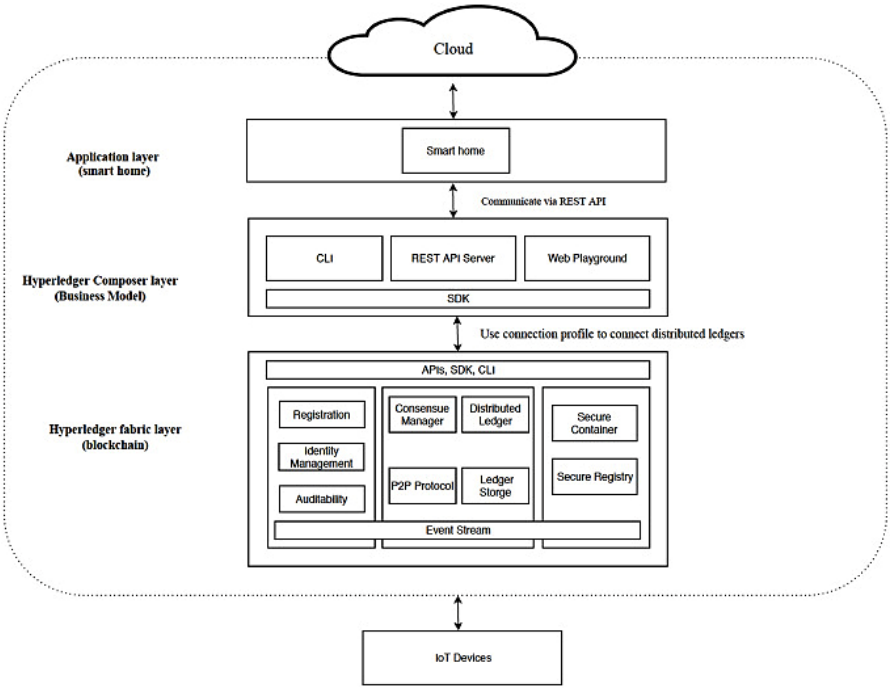

Рисунок 2.10 – Блок-апаратна схема застосування ВС–технології для інформаційного захисту кіберфізичної IoT–системи «розумний дім»

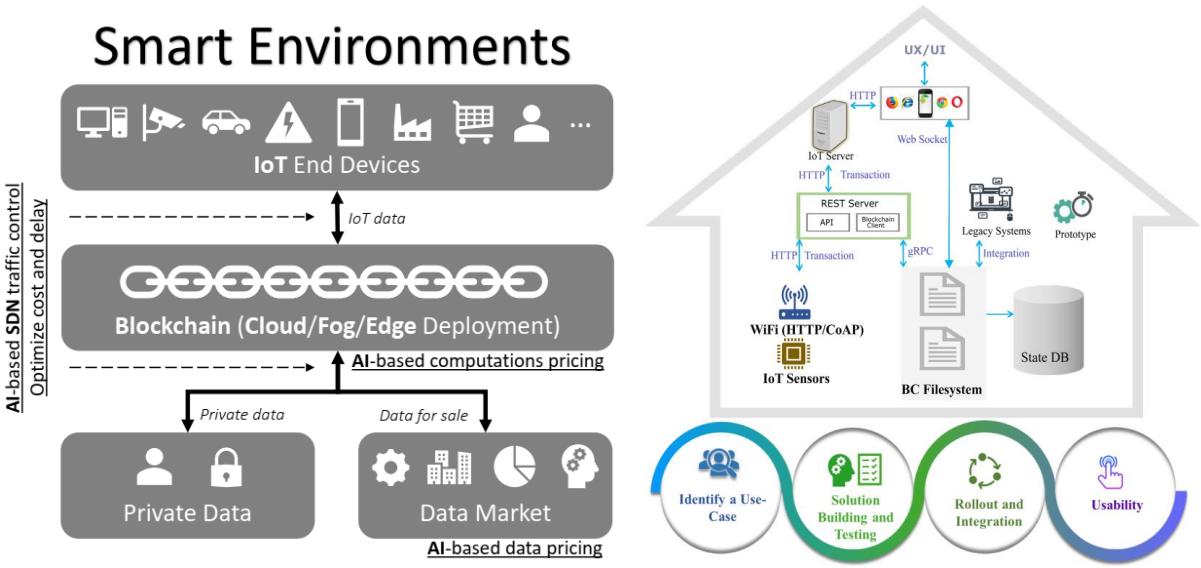

Рисунок 2.11 – Синергетична схема застосування ВС–технології для інформаційного захисту кіберфізичної IoT–системи «розумний дім»

Таким чином, встановлено, що існує достатня кількість доробків щодо застосування ВС–технології для інформаційного захисту кіберфізичної IoT–системи «розумний дім». Відповідно до зазначеного вище аналітичного матеріалу, в рамках цієї праці пропонується застосувати технологію Blockchain у якості сучасного методу захисту інформації для досліджуваної кіберфізичної системи інженерного супроводу життєдіяльності у кіберфізичному просторі приватного житла – технологію Blockchain, що буде використовуватись як засіб надійної аутентифікації та захисту конфіденційної інформації від сторонніх користувачів (зловмисників).

Однак, використання ВС–технології пов’язане зі значною ресурсо- та енергоємністю цього цифрового доробку на сучасному етапі розвитку та потребує відповідних оптимізаційно-адаптивних рішень.

Базуючись на наукових дослідженнях, що представлені в публікаціях [90 – 100], використаємо математичний аналіз для пошуку можливості удосконалення запропонованого методу захисту досліджуваної кіберфізичної системи.

При побудові математичних моделей блокчейн–середовища теоретико–автоматна модель виникає природним чином, оскільки функціонування блокчейн–середовища – це детермінований процес, в ході якого рішення про включення або невключення блоку до Реєстру залежить як від попередніх блоків (бульовий тип даних), так і від часу (тип даних – дійсні числа). Таким чином, якщо розглядати поточний стан реєстру як попередній стан, а стан реєстру відразу після включення до нього чергового блоку як наступний стан, то процес зміни вмісту реєстру можна описати за допомогою поняття «автомат із мітками часу» (timed automaton), для якого далі використовується термін Т–автомат або коротко – ТА [90 – 100]

У плані математичних моделей блокчейн–середовища на основі ТА представляє інтерес концепція, в якій моделюється функціонування смарт-контрактів у біткойн–середовищі (остання є окремим випадком блокчейн–середовища), що є одним з найбільш важливих моментів для повноцінного функціонування цифрової економіки на основі блокчейн–середовища (а не тільки для реалізації криптовалют). Більш того, відомі методи отримання опису смарт-контрактів як кінцевих автоматів з функціонуючого в часі блокчейн-середовища [90 – 100] – рис. 2.12.

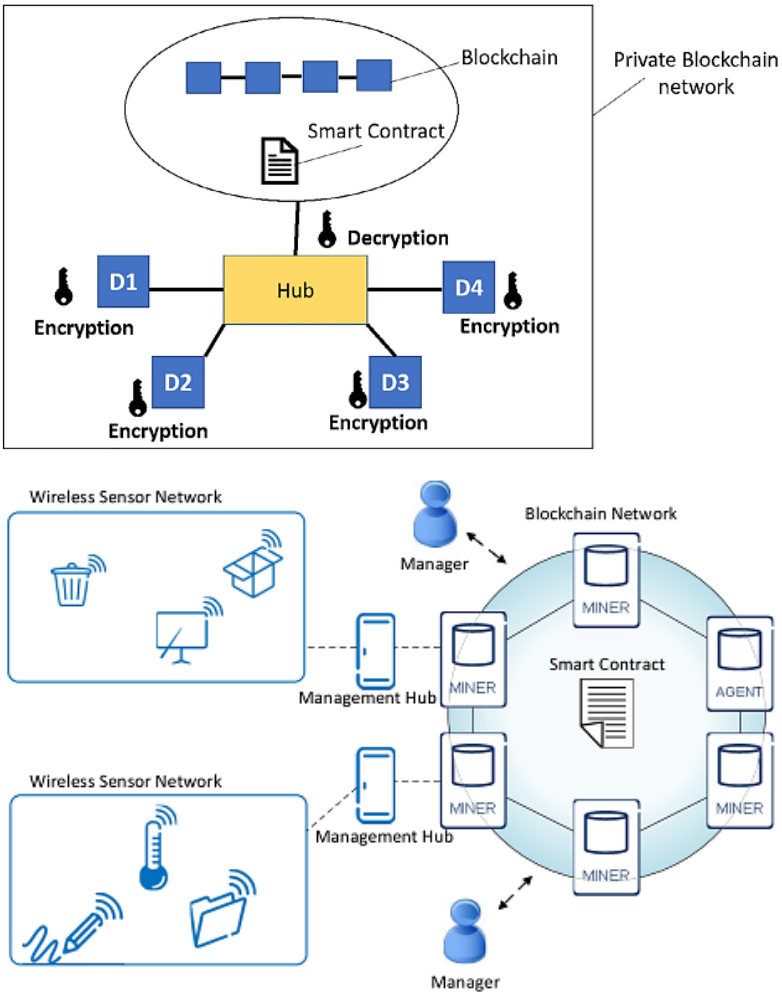

Рисунок 2.12 – Дослідження реалізації «смарт–контакту» в ВС–технології як найбільш ресурсоємнісною субситемою

Доводиться, що функціонування смарт-контрактів у блокчейн–середовищі можна розглядати як взаємодію автоматів у часі, тобто ТА можна розглядати як релевантну модель опису такої взаємодії [90 – 100].

Зазначимо, що моделювання функціонування смарт-контрактів у блокчейн–середовищі є одним із важливих методів перевірки стійкості проти компрометації. Смарт–контракт використовує вхідні дані від інших смарт-контрактів, користувачів, а також про поточний час і видає вихідні дані, що використовуються іншими користувачами та/або іншими смарт–контрактами, тому помилкове функціонування одного смарт-контракту може призвести до збою в роботі всіх пов'язаних з ним смарт–контрактів та вузлів мережі. Проте смарт–контракт може бути дуже складно влаштований навіть уже на рівні

юридичного документа, не кажучи вже про його програмну реалізацію, тому потрібна ретельна перевірка правильного функціонування смарт–контракту і в юридичному плані, і як комп'ютерна програма. Таку перевірку досить складно виконати вручну, проте моделювання смарт–контракту дозволяє поставити ряд машинних експериментів для вивчення поведінки смарт-контракту як автомата при подачі на нього тих чи інших вхідних даних, тобто змоделювати його поведінку в різних умовах.

Пропонується принципово інший підхід до побудови теоретико–автоматних моделей функціонування блокчейн–середовища (зокрема, функціонування смарт-контрактів у цьому середовищі) як автомата з тимчасовими мітками, в якому фізичний час є не дійсними, а 2–адичними числами. Такий підхід видається автору виправданим та плідним з кількох причин [90 – 100]:

– підсумкова модель є автоматом у стандартному розумінні цього визначення; при цьому задається автоматично перетворення слів реалізується не у вигляді таблиці переходів станів, а у вигляді програми без розгалуження, що є послідовністю стандартних команд процесора, а саме: арифметичних та порозрядних логічних операцій;

– оскільки отриманий автомат є «звичайним» автоматом, опис його функціонування може бути зведений до вивчення функції, заданої та приймаючої значення у просторі цілих 2–адичних чисел з огляду на те, що кожна детермінована функція (тобто функція, що задається автоматом) є p –адична функція, що задовольняє умові Ліпшица з константою 1 щодо відповідної p –адичної метрики, і назад: всі такі функції є детермінованими;

– сказане дає можливість застосовувати до вивчення таких автоматів (а значить, і до вивчення функціонування смарт–контрактів у блокчейн–середовищі) розвинений апарат p -адичного аналізу та, ширше, алгебраїчної динаміки;

– нарешті, 2–адичний (і, ширший, p –адичний) час є хоч і не загальноприйнятою, проте досить широко використовуваною і в багатьох

випадках релевантною математичною моделлю фізичного часу, що активно вивчається вже майже три десятиліття в рамках p –адичної математичної фізики.

Поняття «автомат» використовується в різних сенсах, яким відповідають англійські терміни state machine, sequential machine, transducer і т.д., тому щоб уникнути непорозумінь введемо визначення, що використовуються в даній роботі. Скрізь далі під «алфавітом» розуміється кінцева непорожня множина, що містить хоча б два елементи [90 – 100].

Визначення 1. Автомат–визначник (надалі – d –автомат) – це кортеж – ф. (2.3) [90 – 100]:

$$\langle I', S', F', S, s_0 \rangle, \tag{2.3}$$

де I' – вхідний алфавіт;

S' – непуста (необов'язково кінцева) множина, що носить назву «множина станів»;

F' – кінцева непуста підмножина множини S', що носить назву «множина приймаючих станів»;

$s_0 \in S'$ – «початковий стан»;

Функція переходу – ф. (2.4):

$$S: I' \times S' \to S. \tag{2.4}$$

Автомат-визначник є «кінцевим», у випадку, якщо кінцева множина S його станів.

Множина всіх кінцевих послідовностей $W(I')$ на множиною I′ приймає назву «множина слів». Зазначимо, що $W(I')$ не містить пустого слова («слова нульової довжини») $\emptyset$, відповідно до чого вводимо припущення – ф. (2.5) [90 – 100]:

$$W_0(I') = W(I') \cup \{\emptyset\}. \tag{2.5}$$

Використовуємо стандартне визначення мови, що розпізнається d –автоматом, та регулярної мови (мови, що розпізнається кінцевим

d –автоматом). Зазначимо, що даному поняттю кінцевого d –автомата відповідає поняття DFA – deterministic finite automaton [90 – 100].

Визначення 2. Автомат–перетворювач (надалі – f –автомат) – це кортеж – ф. (2.6) [90 – 100]:

$$\langle I', S', O', S, O, s_0 \rangle, \tag{2.6}$$

де I', S', S, s_0 – параметри, що визначені в ф. (2.3);

O' – вхідний алфавіт;

Функція виходу – ф. (2.7):

$$O: I' \times S' \to O'. \tag{2.7}$$

Наведене вище визначення відповідає поняттю автомата Мілі, або, що те ж саме, поняттю 1–рівномірного перетворювача (1–uniform transducer), з тією різницею, що безліч станів автомата в сенсі визначення 2 може бути і нескінченним; якщо безліч станів звичайно, то визначення 2 перетворюється на стандартне визначення автомата Мілі (Mealy sequential machine).

Кожний перетворювач природним шляхом задає відображення множини $W(I')$ у множину $W(O')$, а кожний d –автомат задає відображення множини $W(I')$ в множину – ф. (2.8) [90 – 100]:

$$F' \cup R, \tag{2.8}$$

де $R \notin S'$.

Також в R відображаються ті, та саме ті слова, що не приймаються d –автоматом.

T –автомати, вони ж автомати з мітками часу, або timed automata, використовувалися для моделювання функціонування блокчейн–середовища, оскільки різні вузли, що функціонують в блокчейн–середовищі, отримують черговий блок, взагалі кажучи, в різні моменти часу. Цілий ряд атак на блокчейн заснований саме на факті «різночасності» отримання чергових блоків користувачами.

Щоб ввести поняття T –автомата, спочатку знадобиться визначення (нескінченного) слова з мітками часу (timed word), або, для стислості, t –слова.

Визначення 3. («Нескінченне») «слово з мітками часу» (t –слово) над алфавітом A' («нескінченна») «послідовність пар» – ф. (2.9) [90 – 100]:

$$\left((a_i, \tau_i)\right)_{i=0}^{\infty}, \tag{2.9}$$

де $a_i \in A'$;

$\tau_i \in \mathbb{R}_{\geq 0}$.

При чому послідовність $(\tau_i)_{i=0}^{\infty}$ дійсних послідовних невід'ємних чисел τ_i суворо та необмежено зростає – ф. (2.10) [90 – 100]:

$$\tau_0 < \tau_1 < \tau_2 \ldots \Leftrightarrow \lim_{i \to \infty} \tau_i = \infty. \tag{2.10}$$

На змістовному рівні слово з мітками часу $\left((a_i, \tau_i)\right)_{i=0}^{\infty}$ (ф. (2.9) інтерпретується як послідовність символів $(a_i)_{i=0}^{\infty}$ алфавіту A′, що подається в автомат в моменти часу $\tau_0, \tau_1, \ldots$ відповідно.

Визначення 4. Нехай T – це (розрахункова) множина змінних, що має назву «тимчасові змінні», тоді $t_j \in T$. «Тимчасовим обмежувачем» називається будь-яка булева комбинація предикатів виду – ф. (2.11) [90 – 100]:

$$t_j \leq qmaq \leq t_j, \tag{2.11}$$

де $q \in \mathbb{Q}_{\geq 0}$ – невід'ємні раціональні константи;

$\leq$ – інтерпретація бінарного відношення «менше чи рівно».

Наведемо приклад. Нехай дано: (вхідний) алфавіт I′, кінцева множина S' станів, кінцева множина C, що маж назву «множини таймерів», та множина $\Phi(C)$ тимчасових обмежень від тимчасових змінних $t_1, \ldots, t_{|C|}$. Тоді «таблиця переходів станів з мітками часу» (надалі – ТТТ) – це деяка множина кортежів виду – ф. (2.12) [90 – 100]:

$$\langle s, a, s', G, \varphi \rangle, \tag{2.12}$$

де $s, s' \in S'$;

$\varphi \in \Phi(C)$;

$G \in 2^C$ – підмножина множини таймерів (можливо і пуста).

Визначення 5. «Детермінований автомат з мітками часу (надалі – T –автомат) – це кортеж – ф. (2.13) [90 – 100]:

$$\langle I', S', E', C, \Phi(C), s_0 \rangle, \tag{2.13}$$

де I', S', s_0 – параметри, що визначені в ф. (2.3);

$C, \Phi(C)$ – параметри, що визначені в ф. (2.12);

E' – ТТТ, відповідно до визначення 4, при чому мають виконуватись наступні зауваження:

– у початковому стані s_0 поточне значення всіх тимчасових змінних дорівнюють 0;

– для будь-яких $a \in I'$, $s' \in S'$та будь-якої пари елементів ТТТ E′ виду $(s, a, *, *, \varphi_1)$, $(s, a, *, *, \varphi_2)$тимчасових обмежень φ_1 та φ_2 є взаємовиключними, тобто $\varphi_1 \wedge \varphi_2$ рівність хибна [90 – 100].

«Фізичною основою» для такої «апроксимації» функціонування блокчейн-середовища за допомогою більш простої f –автоматної моделі, ніж за допомогою більш складної Т –автоматної, що використовується в літературі, служить таке обмеження: у реальному житті час, що розділяє дві наступні один за одним події , Не може бути довільно малим, воно завжди обмежене знизу деякою величиною. Наприклад, у квантовій фізиці передбачається, що події, розділені планківським часом, тобто проміжком приблизно в 5×10^{-44} с, відбуваються одночасно, і, більше того, нині мінімальний інтервал часу, доступний фізичному виміру, становить приблизно 10^{-20} с. Звідси випливає, що будь-який часовий інтервал кратний деякому мінімальному часовому інтервалу (у граничному випадку – планківському часу) і, таким чином, з точністю до множника, що дорівнює довжині цього мінімального інтервалу, є натуральним числом.

З іншого боку, T –автоматні моделі дозволяють розглядати поведінку моделюється в «граничних» ситуаціях; наприклад, коли тимчасовий проміжок

між сусідніми «подіями» прагне досягнути нульового значення. Розгляд «граничної» поведінки часто виявляється дуже корисним для опису не тільки якісних, але нерідко і кількісних характеристик системи, що моделюється. Можливість «переходу до межі» у T –автоматних моделях заснована на тому, що множина $\mathbb{Q}_{\geq 0}$ всюди щільна у множині $\mathbb{R}_{\geq 0}$ відносно звичайної дійсної метрики.

Таким чином, для моделювання блокчейн–середовища хотілося б побудувати аналог ТА, в яких час, з одного боку, був би «дискретним», тобто як «вихідні» позначки часу виступали б натуральні, а не раціональні (як у визначенні ТА) числа, проте, щоб зберігалася і можливість «граничного переходу» як з метою отримання опису поведінки всієї системи у часі на (хоч би) якісному рівні, так і отримання оцінок «точності» моделі. Оскільки йдеться про граничний перехід, то необхідно задати деяку метрику на безлічі всіх натуральних чисел, щодо якої такий граничний перехід був можливий щодо якої натуральні числа утворювали б всюди щільне підмножина подібно до того, як множина $\mathbb{Q}_{\geq 0}$ є скрізь щільною підмножиною в $\mathbb{R}_{\geq 0}$ відносно дійсної метрики. Такі метрики існують – це p –адичні метрики [90 – 100].

Будемо досліджувати t –слова з мітками часу з $\mathbb{N}_0 = \{0,1,2,3,\dots\}$ (а не з $\mathbb{R}_{\geq 0}$) над кінцевим алфавітом A', що містить хоча б два символи. Без обмеження загальності можливо вважати, що якщо $\mathrm{p} \geq 2$ – це потужність алфавіту $A^{'}$, а символами алфавіту $A^{'}$ є числа $0,1,\dots,p-1$. Зазначимо, що такі t –слова є окремим випадком так званих «слів з даними» (data word), а саме: коли множина даних $D^{'}$ співпадає з $\mathbb{N}_0$. Введені у визначення 3 слова з мітками часу також являють собою «слова з даними» для випадка, коли дані лежать в $\mathbb{R}_{\geq 0}$. На підставі поняття «слів з даними» природним шляхом вводиться поняття «мови з даними» (data language), а також «автомата з даними» (data automaton), далі – D –автомат [90 – 100].

Визначення 6. «Автомат $\mathfrak{A}$ з даними D – це кортеж – ф. (2.14) [90 – 100]:

$$\mathfrak{A} = \langle I^{'}, S^{'}, F^{'}, T^{'}, k, \sim, s_0 \rangle, \qquad (2.14)$$

де I', S', F', s_0 – параметри, що визначені в ф. (2.3);

k – натуральне число, що має назву «число регістрів даних»;

$\sim$ – відношення еквівалентності кінцевого індексу, що визначено на D'^k.

Кінцева множина переходів – ф. (2.15) [90 – 100]:

$$T' \subseteq S' \times \frac{D'^k}{\sim} \times I' \times \frac{D'^k}{\sim} \times S'. \quad (2.15)$$

U' – множина модифікацій стану регістрів $upd: D'^k \to D'^k$, що задовольняє наступним обмеженням – ф. (2.16) [90 – 100]:

– для будь-якого кортежа

$$(s, g, a) \in S' \times \frac{D'^k}{\sim} \times I'. \quad (2.16)$$

Існує (едина) модифікація регістрів $upd \in U'$ так, що у випадку $(s, g, a, upd', g', s') \in T'$ для деякого $upd' \in U'$, то $upd' = upd$.

Якщо $(s, g, a, upd, g', s), (s, g, a, upd, g', s') \in T'$, то $s' = s$.

Для будь-якого детермінованого T –автомата з визначення 5, що має n таймерів (відповідно до визначення в), існує D –автомат з $2n + 2$ регістрів, що розпізнає в точності ту саму мову. Далі побудуємо f –автомати (відповідно до визначення 2), що апроксимують з будь-якою наперед заданою точністю (у деякому точно визначеному нижче сенсі) даний детермінований T –автомат і тим самим зведемо завдання моделювання функціонування блокчейн–середовища (насамперед, моделювання смарт–контрактів) T –автоматами до моделювання «звичайними» автоматами з двійковими входами та двійковими виходами. Для цього спочатку потрібно ввести новий приватний тип D –автоматів, а саме: «автомати з p –адичним часом» [90 – 100].

Зафіксуємо деяке просте число p (в межах даного дослідження найважливішим випадком є $\mathrm{p} = 2$) та дослідимо у якості міток даних (у «словах з даними») «цілі p –адичні числа», тобто елементи простору $\mathbb{Z}_p$ «цілих p –адичних чисел».

Множина $\mathbb{Z}_p$ може досліджуватись як множина $W^{\infty}(A')$ всіх «нескінченних» слів над алфавітом $\mathrm{A}' = \{0,1,\ldots,\mathrm{p}-1\}$, символи якого можна

вважати елементами кільця $\frac{\mathbb{Z}}{p\mathbb{Z}}$ вирахувань за модулем p, тобто елементи поля з p –елементів. Якщо $p = 2$, то «нескінченні» бінарні рядки можна вважати як представлення чисел в узагальненому «зворотному двійковому коді». Використання узагальненого зворотного двійкового коду дає можливість записувати в регістр нескінченної довжини як всі цілі негативні числа (їм відповідають рядки з кінцевим числом одиниць), так і всі цілі негативні числа (їм відповідають рядки з кінцевим числом нулів), а також всі раціональні числа у вигляді простих нескоротних дробів з непарними знаменниками (їм відповідають періодичні з якогось моменту рядки).

Множина $\mathbb{Z}_p$ є повним компактним метричним простором відносно «p –адичної метрики» d_p, що задається наступним чином – ф. (2.17) [90 – 100]:

$$d_p(a,b) = \frac{1}{p^j}. \tag{2.17}$$

Відтак, коли – ф. (2.18):

$$\begin{gathered} a = \ldots a_{i+1} a_i c_{i-1} \ldots c_0; \\ b = \ldots b_{i+1} b_i c_{i-1} \ldots c_0 \ ; \\ a_i \neq b_i \ . \end{gathered} \tag{2.18}$$

При чому за визначенням $d_p(a,b) = 0$, якщо такого i не існує, тобто якщо «нескінченні» слова a і b співпадають. Абсолютна велична $\left|\left|a\right|\right|_p$ водиться стандартним чином як відстань до нульового числа. Цьому числу відповідає «нескінченному» рядку тільки з нульових значень – ф. (2.19) [90 – 100]:

$$\|a\|_p = d_p(a,0). \tag{2.19}$$

Можливо ввести поняття «приведення по модулю p^n» та «порівняння по модулю p^n» для цілих p –адичнних чисел, а саме: приведення по модулю p^n «нескінченного слова» в алфавіті $\mathrm{A}' = \{0,1,\ldots,\mathrm{p}-1\}$ позначає всього лиш перехід до кінцевого начального відрізку довжини n цього «нескінченного» слова, тобто – ф. 2.20 [90 – 100]:

$$mod\, p^n : W^{\infty}(A') \to W^n(A'). \tag{2.20}$$

де $W^n(A')$ – це множина всіх слів довжини n над алфавітом A'.

Відзначимо, що елементи множини $W^n(A')$ природним шляхом ототожнюється з числами $0,1,\ldots,\mathrm{p}^n-1$, що представлені в системі відліку з основою p , а ці числа, в свою чергу ототожнюються з елементами кільця $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ відрахувань по модулю p^n. Більш того, виявляється, що будь-яке відображення, що задається автоматом–перетворювачем $\mathfrak{A}$, вхідний та вихідні алфавіти – ф. (2.21), ф. (2.22) [90 – 100]:

$$f_{\mathfrak{A}}: W^{\infty}(A') \to W^{\infty}(A'); \tag{2.21}$$

$$I' = O' = A' = \{0,1,\ldots,p-1\}. \tag{2.22}$$

Функція ф. (2.22) визначається на $\mathbb{Z}_p$ і приймаюче значення $\mathbb{Z}_p$, яка задовольняє p –адичній умові Ліпшица з константою 1, а, відповідно, є неперервною відносно метрики d_p функцією – ф. (2.23) [90 – 100]:

$$\|f_{\mathfrak{A}}(a) - f_{\mathfrak{A}}(b)\|_p \le \|a-b\|_p \Leftrightarrow a,b \in \mathbb{Z}_p. \tag{2.23}$$

Вірне і зворотне твердження: будь-яке відображення $\mathbb{Z}_p$ в $\mathbb{Z}_p$, що задовольняє p –адіатичній умові Ліпшица з константою 1, задається деякими автоматом–перетворювачем (не обов'язково кінцевим), вхідний та вихідний алфавіти, зміст якого $\{0,1,\ldots,p-1\}$.

Варто зауважити, що кожний з двох типів автоматів: автомати–визначники, тобто d –автомати з визначення 1, та автомати–перетворювачі, тобто f –автомати з визначення 2 – можуть бути зведені до іншого. Таким чином, у випадку $p=2$ задачі про d –автомати з розпізнаваними ними мовами можуть бути зведені до задач про функції, що задовольняють 2–адичній умові Ліпшиця з константою 1. Такі функції називаються «функціями трикутного виду, двійковими, сумісними, T –функціями».

Комп'ютерна реалізація детермінованої функції автомата, вхідний та вихідний алфавіти якого складаються з двох символів, не вимагає реалізації його таблиці переходів станів, а може бути записана (у тому числі і для автоматів з нескінченним числом станів) у вигляді T –функції, яка, у свою черга, являє собою програму без розгалужень, що складається з послідовності

стандартних комп'ютерних команд, таких як арифметичні команди (складання та множення натуральних чисел) та порозрядні логічні команди OR, AND, XOR, NOT, а також похідних від них команд, таких як зсув убік старших розрядів, маскування та інших, таких як розподіл на непарні числа, зведення непарних чисел у ступінь та інших [90 – 100].

Зазначене залишається в силі і для автоматів, вхідний та вихідний алфавіти яких складаються відповідно з 2^n та 2^m символів, оскільки такі автомати можливо вважати автоматами, що мають n двійкових входів та m двійкових виходів, а значить, як багатовимірні T –функцій, тобто як безперервні відносно 2–адичної метрики відображення $\mathbb{Z}_2^n$ в $\mathbb{Z}_2^{\mathrm{T}}$, що задовольняють багатовимірному 2–адичній умові Ліпшица з константою 1. Для T –функцій розроблений достатній математичний апарат, що заснований на 2–адичному аналізі та існують численні (в першу чергу – криптографічні) додатки [90 – 100].

Сформулюємо визначення автомату з 2–адичним часом.

Визначення 7. D –автомат з визначення 6 отримує назву «автомату з 2–адичним часом» ($\mathbb{Z}_2$–автомат), якщо виконується умова – ф. (2.24):

$$I' = \{0,1\} \text{ та } D' = \mathbb{Z}_2. \qquad (2.24)$$

Зрозуміло, що схожим чином можливо сформулювати і поняття $\mathbb{Z}_2$–автомата з вхідним алфавітом з 2^r символом, тобто $\mathbb{Z}_2$–автомата з r –двійковими входами. Мова, що розпізнається $\mathbb{Z}_2$–автоматом, визначається звичайним чином на підставі визначення 7.

Будь-який T –автомат може вважатися «автоматом з двома входами»: часовим та алфавітним, де на кожному такті роботи подається на алфавітний вхід черговий символ вхідного слова, а на часовий вхід – дійсне число, що слугує міткою часу цього вхідного символу. З цією точки зору $\mathbb{Z}_2$–автомат також має два входи; при цьому на алфавітний вхід подається символ вхідного алфавіту, тобто 0 та 1, а на часовий вхід – мітка часу, тобто ціле 2–адичне число [90 – 100].

Всі t –слова можуть бути рівномірно наближені словами з 2–адичними мітками часу (надалі – $\mathbb{Z}_2$–словами) в наступному значенні. Спочатку усі символи вхідного алфавіту T –автомату нумеруємо та запишнимо у вигляді двійкових представлень відповідних чисел. Таким чином, можливо вважати, що алфавітний вхід автомата завжди подається r –бінарних послідовностей, де r – число двійкових розрядів, необхідних для запису всіх символів вхідного алфавіту.

Надалі зафіксуємо будь-яке дійсне число $\varepsilon > 0$ і виберемо раціональні числа $z_i(w)$, що формуються у вигляді простих нескоротних дробів з непарними знаменниками (всі ці раціональні числа лежать в множині $\mathbb{Z}_2$), так, щоб виконалось умова – ф. (2.25) [90 – 100]:

$$|\tau_i(w) - z_i(w)| < \varepsilon, \tag{2.25}$$

де $\tau_i(w)$ – i –мітка часу в t –слові w.

Такий вибір завжди можна зробити, наприклад, наступним чином.

Формулюємо – ф. (2.26):

$$\tau_i(w) = [\tau_i(w)] + (\tau_i(w) - [\tau_i(w)]), \tag{2.26}$$

де $[\tau_i(w)]$ – ціла (з недоліками) частина числа $\tau_i(w)$.

Виберемо $h \in \mathbb{N}$ таким, щоб виконувалась умова – ф. (2.27):

$$\frac{1}{3^h} < \varepsilon. \tag{2.27}$$

Дрібна частина формулюється у вигляді $(\tau_i(w) - [\tau_i(w)])$ числа $\tau_i(w)$ в трійковій системі розрахунків з точністю до h трійкових розрядів після коми. Тоді ця дрібна частина являє собою число виду $\frac{c}{3^h}$, де $c \in \{0,1,\dots,3^h - 1\}$ та, відповідно, є цілим 2–адичним числом. Добавляючи до отриманого в такий спосіб числа цілі (з недоліком) частину $[\tau_i(w)]$ числа $\tau_i(w)$, отримуючи ціле 2–адичне число $z_i(w)$. В такому значенні кожне t –слово $w = \big((a_i, \tau_i)\big)_{i=0}^{\infty}$ наближається з точністю не гірше, ніж ε –словом $\Big(\big((a_i), z_i(w)\big)\Big)_{i=0}^{\infty}$, що є вхідним $\mathbb{Z}_2$–словом для $\mathbb{Z}_2$–автомата з r –алфавітними входами, при чому алфавіт кожного алфавітного входу бінарний [90 – 100].

Надалі всі $\mathbb{Z}_2$–слова можуть бути рівномірно наближені $\mathbb{Z}_2$–словами з мітками часу з $\mathbb{N}_0$ (та навіть з $\frac{\mathbb{Z}}{2^h\mathbb{Z}}$) з любою завчасно заданої 2–адичною точністю $\frac{1}{2^h}$. Дійсно, для цього достатньо кожну з 2–адичних міток часу у кожному $\mathbb{Z}_2$–слові привести по модулю 2^h. Таким чином, на підставі вищевказаної процедурі «апроксимації» t –автомата $\mathbb{Z}_2$–автоматом можливо побудувати послідовність $\mathbb{Z}_2$–автоматів $\mathfrak{M}_h$ з мітками часу з $\frac{\mathbb{Z}}{2^h\mathbb{Z}}$, $h = 1,2,3\ldots$, апроксимуючих у вищевказаному значенні вихідний t –автомат.

Застосовуючи вищеописану процедуру побудови f –автомата на підставі даного d –автомата, можна будь-якому D –автомату скласти детерміновану функцію з мітками часу, вважаючи, наприклад, що й i –символ відповідного вхідного слова. Таким чином, на підставі цього $\mathbb{Z}_2$–автомата з визначення 7 можливо побудувати детерміновану функцію з мітками часу з $\mathbb{Z}_2$, приймаючи i –й вихідний символ рівним 1, якщо автомат знаходиться в приймаючому стані (тобто в стані з множини F'), та 0 в протилежному.

Нарешті, цим способом кожному з побудованих вище апроксимуючих автоматів $\mathfrak{M}_h$ можливо порівняти детерміновану функцію з мітками часу з $\frac{\mathbb{Z}}{2^h\mathbb{Z}}$. Отже, для цього T –автомату побудована послідовність апроксимуючих його (у зазначеному значенні) T –функцій, тобто «звичайних» f –автоматів в значенні визначення 2, що мають $r + h$ двійкових входів та $h + 1$ двійкових виходів. Таким чином, доведено наступне: кожний T –автомат апроксимується з будь-якою завчасно заданою точністю (у визначеному значенні) деяким f –автоматом над двосимвольним алфавітом.

Висновок до другого розділу

Доведено, що для моделювання функціонування блокчейн–середовища (зокрема, моделювання роботи смарт–контрактів в кіберфізичній системі «розумного дому»), навіть незважаючи на те, що це середовище функціонує в реальному фізичному часі, немає необхідності вдаватися до складних (і досить ресурсоємних) моделей, заснованих на концепції автоматів з мітками часу, що є дійсними числами, а досить обмежитися (без втрати точності) моделюванням цього середовища за допомогою детермінованих функцій над 2–символьним алфавітом (відомих також під назвою T –функцій), тобто за допомогою «звичайних» автоматів із бінарним вхідним/вихідним алфавітом. Ці функції можуть бути реалізовані у вигляді програм без розгалуження, виконаних як послідовності стандартних команд будь-якого процесора, що дозволяє сподіватися на відносну простоту їхньої програмної реалізації та високу швидкодію відповідних програм.

Таким чином, досягнуте наукове завдання щодо удосконалення інформаційного захисту кіберфізичної IoT–системи «розумний дім» шляхом впровадження оптимізованої (за ресурсоємністю механізму дії, як доведено вище) Blockchain–технології для надійної автентифікації, що є актуальним та сучасним рішенням з застосуванням провідних цифрових технологій.

РОЗДІЛ 3

ОЦІНКА ЕФЕКТИВНОСТІ УДОСКОНАЛЕНОГО МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ В IoT–СИСТЕМІ (КІБЕРФІЗІЧНІЙ СИСТЕМІ) «РОЗУМНИЙ ДІМ»

3.1 Визначення показників оцінювання

За результатам аналізу наукових праць та публікацій [85 – 89], відповідно до розробленого математичного апарату (п. 2.2 цієї праці) сформулюємо критерії оцінювання ефективності застосовуваних стратегій та засобів захисту кіберфізичної IoT–системи «розумний дім» від кібер-цифрових загроз (найбільш вірогідна з яких визначені в п. 1.3 цієї праці – загроза втрати конфіденційної інформації).

Один з визначних критеріїв є рівень захищенності (РЗ) модельованої кіберфізичної системи, що визначається при порівнюванні поточного та прогнозованого значення – ф. (3.1) [85 – 89]:

$$I^*\left(\lambda_{zmin}^{opt_{zmin}^{opt}} \Rightarrow I, I^* \in [0,1] \Rightarrow I \to 0 \Rightarrow max\, P3\right). \qquad (3.1)$$

Відповідно до ф. (3.1) встановлюємо, що, чим ближче значення I до нульового, тим вищий рівень захисту досліджуваної IoT–системи (вищий показник РЗ).

Ще один показник якості моделювання похибка моделі 2^q – ф. (3.2) [85 – 89]:

$$2^q \to min, \qquad (3.2)$$

де q – кількість дискрет, які враховуються для диференціальних спектрів (ДС) $P_0(k)$ при побудові відповідної моделі;

k – цілочисловий аргумент, $k =: 0,1,2,\ldots$, її точності y^*, а також діапазону прогнозування $t \in [t_0, T]$, на якому вона працює із заданими характеристиками.

Визначальний параметр оцінювання якості моделювання загроз інформаційній безпеці кіберфізичної IoT–системи «розумний дім» – оптимальні множини – ф. (3.3) [85 – 89]:

$$\left\{I_{0\theta}^{(j)^*}, I_{\text{Å}\hat{\text{O}}}\right\} \tag{3.3}$$

де $I_{0\theta}^{(j)^*} \in \left\{I_{0\theta}^{(j)}\right\}$ – показник найефективнішої множини;

j – показник ієрархічності частинних критеріїв;

θ – оцінювані властивості;

$I_{\text{Å}\hat{\text{O}}}$ – базова терм-множина лінгвістичної змінної, яка визначається п’ятьма термами ф. (3.4):

$$I_{\text{Å}\hat{\text{O}}} = \bigcup_{i=1}^{5} I_{\text{Å}\hat{\text{O}}} \Rightarrow \begin{Bmatrix} "абсолютнонеефективна"(АН), \\ "недостатньоефективна(НЕ), \\ "ефективна"(Е), \\ "достатньоефективна"(ДЕ), \\ "абсолютноефективна"(АЕ) \end{Bmatrix} \tag{3.4}$$

Застосування вказаного методу моделювання забезпечує оцінювання ефективності інформаційного захисту кіберфізичної IoT–системи «розумний дім» на різних рівнях ієрархії, що сприяє розширенню діапазону його практичного застосування на процедури оцінювання ефективності комплексних засобів та систем кіберзахисту, як діючих, так і перспективних.

Також важливими показниками ефективності кіберзахисту є швидкодія і оптимальна витрата ресурсів та енергоносіїв, що варто враховувати при виборі засобів та систем інформаційної безпеки.

3.2 Алгоритмування методів визначення ефективних засобів захисту

На підставі запропонованого математичного апарату моделювання кібер-цифрових загроз для IoT–системи «розумний дім» (п. 2.2 цієї праці) виконаємо його практичну алгоритмізацією для визначення дієвої послідовності визначення кіберзагрози та формування адекватного захисту [85 – 89]:

– параметризація поточного технічного стану системи безпеки інтелектуальних інженерних мереж і пристроїв супроводу життєзабезпечення, що піддалася впливу кібератаки: визначення множини станів СІБ;

– визначення методу захисту від кібер-цифрової атаки у першій ітерації: вибір стратегії КБз;

– оцінка рівня захищеності кіберфізичної системи з виконанням оптимізації ресурсоспоживання: оптимізація стратегії КБз та оцінювання РЗ;

– моделювання (прогноз) динаміки розвитку кібернападу: прогнозування розвитку динаміки процесу КБа;

– оптимізація ресурсоспоживання та оцінювання захищеності кіберфізичної системи у другій ітерації: оптимізація ресурсів КБз та оцінювання РЗ;

– оцінка якості моделювання та захисту: оцінка ефективності СІБ.

Сформований алгоритм представлений на рис. 3.1.

На рис. 3.1 штриховою лінією виділено порядок розв’язання оберненої задачі – задачі синтезу, яка полягає у знаходженні прогнозованого РЗ – I^* та оптимальних стратегій захисту $\lambda_{imin}^{opt(t)}$ при найгірших, з точки зору захищеності ІР проявах кібератак гравцем кібернападу $\mu_{imax}^{opt(t)}$. Лінією в крапку виділено порядок розв’язання прямої задачі – задачі аналізу, яка полягає у знаходженні в аналітичному вигляді диференціально-ігрових моделей процесів КБн $P_0^{opt}(t)$. На основі запропонованої методології синтезу та аналізу диференціальноігрових моделей та методів моделювання процесів КБн можливо будувати як програмні, так і програмно-апаратні СІБ, інтегровані до новостворюваних ІТ–технологій, що призначені для забезпечення в реальному масштабі часу прогнозованого РЗ ІР від кібератак прогнозованого класу.

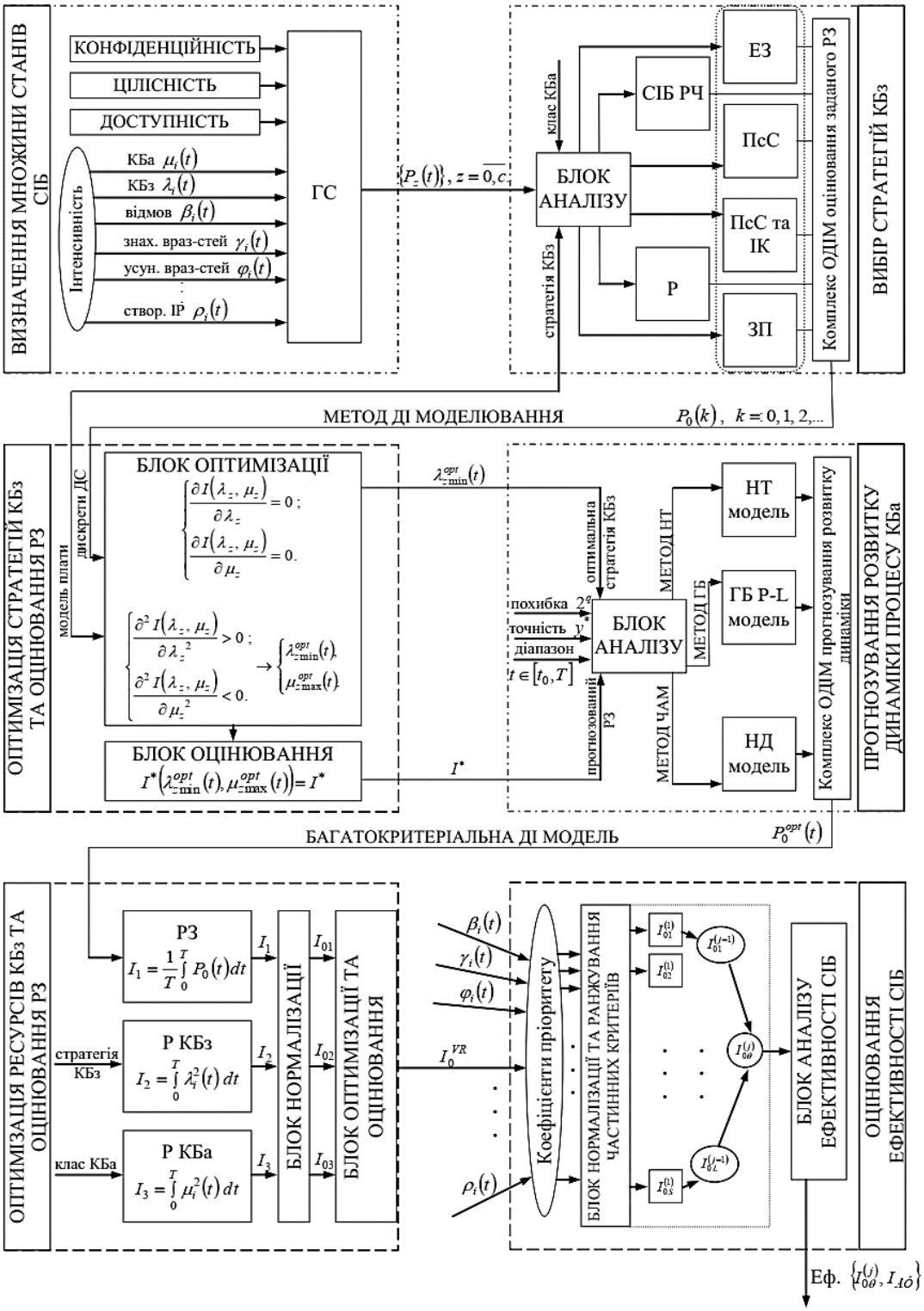

Рисунок 3.1 – Алгоритмування математичного апарату визначення оптимального метода захисту кіберфізичної IoT–системи «розумний дім»

Застосування методології також забезпечує вибір найкращого варіанту побудови прогресивної СІБ, що ґрунтується на інтегральному показнику ефективності системи на базі розроблених моделей та методів моделювання. Створена на основі диференціально-ігрових моделей та методів методологія дозволяє оцінювати поточний та прогнозований РЗ, а також забезпечує прогнозування розвитку динаміки процесу КБн, протягом якого поточний рівень відповідатиме заданому, що сприятиме вибору превентивних стратегій КБз, адекватних умовам протікання ІК в СІБ.

3.3 Визначення показників ефективності та розробка пропозицій до впровадження

Відповідно до результатів огляду наукових праць і публікацій [90 – 100] встановлений ряд перспективних технологій, що можуть бути інтегровані в системи кіберзахисту «розумного дому» – табл. 2.4:

– архітектурний метод з трьома модулями для збереження конфіденційності аналізу даних для розумних будинків;

– метод обмеження на рівні мережі;

– технологія Blockchain для надійної аутентифікації.

Враховуючи динамічний розвиток ВС–технології останнім часом, даний метод захисної автентифікації був визначений як перспективний та адекватний до інтеграції в системи кіберзахисту «розумного дому». Відповідно до наукового завдання для обраної захисної системи виконана оптимізація (п. 2.3 цієї праці), що з допомогою відповідного математичного апарату передбачає заміну складних обчислюваних процесів більш простими, що дозволяє значно знизити витрати ресурсів та енергоносіїв на функціонування СІБ IoT–системи «розумний дім»: для моделювання функціонування блокчейн–середовища (зокрема, моделювання роботи смарт–контрактів в кіберфізичній системі «розумного дому»), навіть незважаючи на те, що це середовище функціонує в

реальному фізичному часі, немає необхідності вдаватися до складних (і досить ресурсоємних) моделей, заснованих на концепції автоматів з мітками часу, що є дійсними числами, а досить обмежитися (без втрати точності) моделюванням цього середовища за допомогою детермінованих функцій над 2–символьним алфавітом (відомих також під назвою T –функцій), тобто за допомогою «звичайних» автоматів із бінарним вхідним/вихідним алфавітом. Ці функції можуть бути реалізовані у вигляді програм без розгалуження, виконаних як послідовності стандартних команд будь-якого процесора, що дозволяє сподіватися на відносну простоту їхньої програмної реалізації та високу швидкодію відповідних програм.

Алгоритмом (3.2 цієї праці) доведена ефективність оптимізованої (за ресурсоємністю) та адаптованої (для потреб IoT–системи «розумний дім») ВС–технології – табл. 3.1.

Таблиця 3.1

Визначення ефективної системи кіберзахисту для інтелектуальних засобів «розумного дому»

Метод	Метод кіберзахисту		
	Архітектурний метод з трьома модулями для збереження конфіденційності і аналізу даних для розумних будинків	Метод обмеження на рівні мережі	Технологія Blockchain (оптимізована (удосконалена) за ресурсоємністю)
$I^*\left(\lambda_{zmin}^{opt_{zmin}^{opt}} \Rightarrow \left\lvert I, I^* \in [0,1] \Rightarrow \left\lvert I \to 0 \Rightarrow max\, P\, 3\right.\right.\right)$	0,1	0,11	0,01
$I_{\text{ÅÔ}} = \bigcup_{i=1}^{5} I_{\text{ÅÔ}} \Rightarrow \Rightarrow \left\{ \begin{matrix} "абсолютнонеефективна"(АН), \\ "недостатньоефективна(НЕ), \\ "ефективна"(Е), \\ "достатньоефективна"(ДЕ), \\ "абсолютноефективна"(АЕ) \end{matrix} \right\}$	ДЕ	Е	АЕ

За результатами оцінювання ефективності виокремлених перспективних методів кіберзахисту (табл. 3.1) встановлено, що найбільш доцільним до впровадження в кіберфізичну IoT–систему «розумний дім» є введення надійної аутентифікації з допомогою BC–технології, оптимізованої в процесі виконання цього дослідження.

Спираючись на розробки блокчейн–середовища для IoT–системи «розумний дім» [90 – 100], визначимо практичні рекомендації для впровадження BC–аутентифікації.

Багаторівнева IoT–система «розумного дому», що базується на BC–аутентифікації представлена на рис. 3.2 [90 – 100].

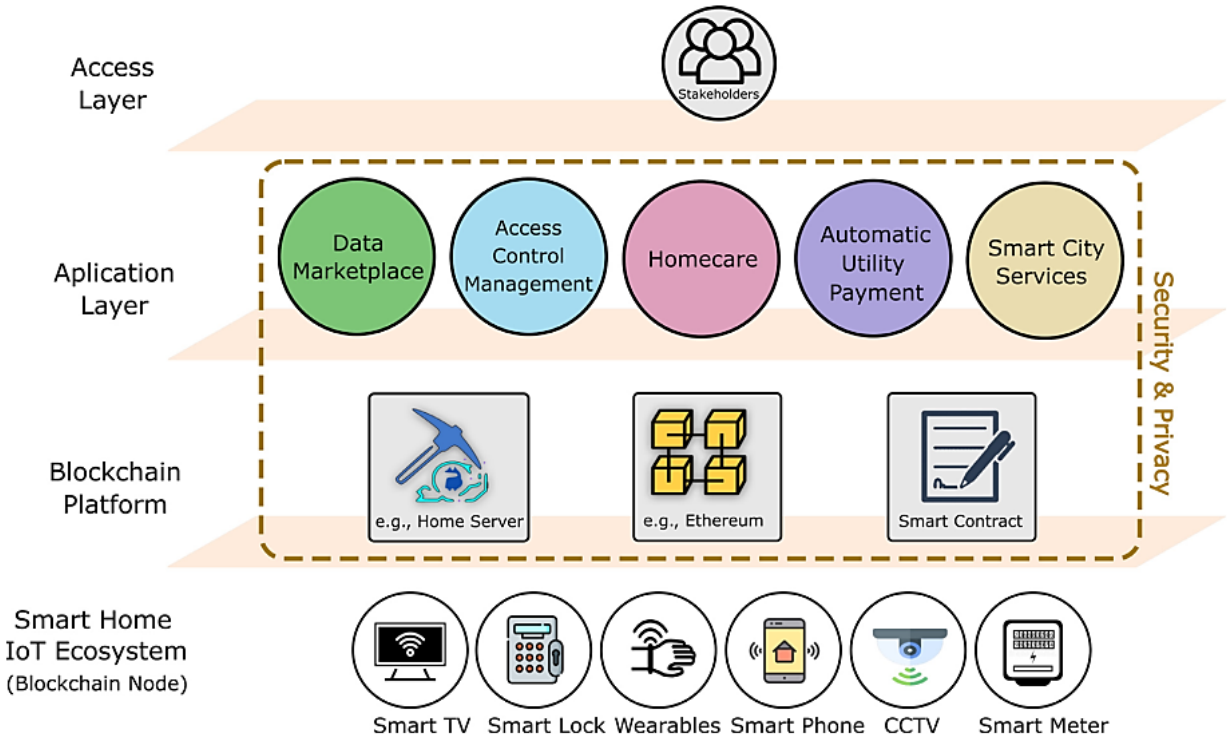

Рисунок 3.2 – Концепт-схема багаторівневої IoT–системи «розумного дому», що базується на BC–аутентифікації

BC–технологія швидко формує інформаційну екосистему «розумного дому», оскільки вона має гнучкість та адаптивність для легкої інтеграції з різнорідними IoT–пристроями розумного дому. Рис. 3.2 ілюструє екосистему «розумного дому» на основі блокчейну. Це чотирирівнева концептуальна

структура, що складається з рівня джерел даних IoT, рівня мережі блокчейну, рівня програм розумного дому та рівня клієнтів:

– рівень джерела даних IoT генерує дані з пристроїв, які відіграють важливу роль в оцінці стану, навколишнього середовища та мешканців розумного будинку. Ці пристрої приблизно поділяються на три основні категорії: сенсорні, мультимедійні та медичні. Датчики вимірюють фактори навколишнього середовища. Дані з цих вузлів консолідуються та зберігаються на централізованому сервері або децентралізованій платформі, наприклад, блокчейні, який створює перший рівень стеку;

– технологія блокчейн знаходиться на вершині екосистеми IoT і складається з двох основних компонентів: структури даних блокчейн і смарт-контракту. Хеш-значення криптографічно з'єднують блоки. Комп’ютер домашнього сервера може розглядатися як майнер, який відповідає за перевірку та додавання нових транзакцій до нових блоків, в той час як смарт-контракти слідують заздалегідь визначеним правилам і полегшують децентралізовані транзакції. Існують різні способи впровадження блокчейну, включаючи публічний, приватний і федеративний, але, як правило, приватний блокчейн використовується в розумній домашній мережі для зниження накладних витрат;

– рівень додатків створений для полегшення різних додатків для розумного дому та їх інтеграції з існуючими платформами блокчейн. Цей рівень включає в себе програми для «розумного дому», такі як «ринок даних», «керування доступом», «взаємодію домашнього догляду» та «охорони здоров’я», а також «автоматизовані комунальні послуги» та «послуги розумного міста». Багато з цих нових програм використовують платформу блокчейн, а деякі все ще досліджуються;

– нарешті, на вершині ієрархії знаходиться рівень клієнта, який дозволяє стороннім зацікавленим сторонам отримувати вигоду від додатків для розумного дому на основі блокчейну, таких як мікромережі, роздрібні магазини, постачальники послуг, доглядачі тощо [90 – 100].

Блокчейн був винайдений Сатоші Накамото в 2008 році. Це базова платформа криптовалют (наприклад, біткойн), яка полегшує систему транзакцій P2P, щоб усунути проблему сторонніх і подвійних витрат. Це децентралізована структура даних, де кожен блок даних криптографічно пов'язаний з хешем попереднього блоку за допомогою SHA-256 (Алгоритм безпечного хешування). Фундаментальна структура блоку включає номер блоку, хеш попереднього блоку, дані транзакції, одноразовий номер і мітку часу. Мітка часу є безперервною змінною, а nonce – випадковою. Статичні (блок) і динамічні (мітка часу та одноразові) дані безперервно хешуються валідаторами або майнерами (обчислювальними вузлами), щоб знайти значення, яке починається з кількох послідовних провідних нулів. Цей процес широко відомий як криптографічна головоломка. Майнер, який знайшов дійсне хеш-значення, першим розглядає переможця, якому надано дозвіл додати блок у блокчейн. Методологія сертифікації блоку, чи є він дійсним чи ні, називається консенсусним алгоритмом Proof-of-Work (PoW). Рис. 3.3 ілюструє архітектуру блокчейну, внутрішній механізм і робочий процес. Наступні кроки описують основні функції [90 – 100]:

(1) Кожен вузол (підключені пристрої IoT у випадку «розумного дому»), включаючи майнерів у мережі блокчейн, складається з пулу пам'яті (Mempool), який включає всі поточні транзакції, які очікують на додавання в блокчейн для створення нового блоку.

(2) Дерево Меркла перевіряє та підсумовує всі транзакції.

(3) Якщо він дійсний, тоді вибрані транзакції включаються в блок, який стає готовим для майнінгу майнерами в мережі «розумного дому».

(4) Майнери генерують хеш блоку, змінюючи одноразовий і часовий штамп.

(5) Потім система порівнює згенерований хеш з цільовим. Як тільки майнер закінчить видобуток блоку, він успішно додається до ланцюжка.

(6) Якщо хеш вище цільового значення, він починається знову з кроку 4.

(7) Якщо хеш нижче цільового значення, тоді PoW перевіряється як успішний і додається в блок до блокчейну. Отже, це повідомлення транслюється на всю мережу, щоб сповістити кожен підключений вузол про видалення оброблених транзакцій з Mempool [90 – 100].

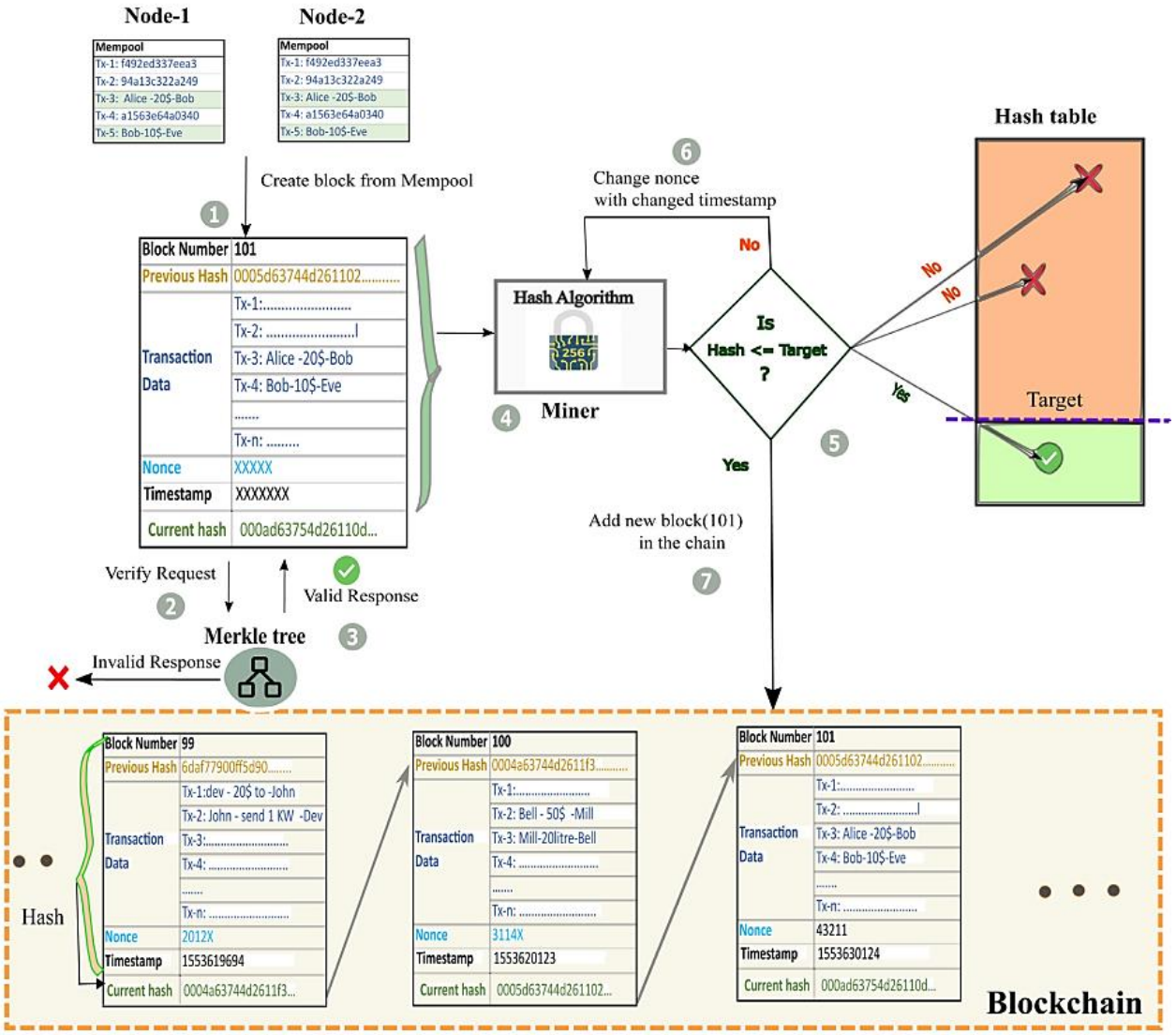

Рисунок 3.3 – Адаптація BC–технології для кіберфізичної IoT–системи «розумний дім»

Смарт-контракт – це комп’ютерна програма, яка вбудована в блокчейн для сприяння, перевірки або забезпечення виконання переговорів щодо контракту в цифровому вигляді. Це набір правил, яким дотримуються різні сторони для регулювання відносин щодо обмінних цінностей. Деталі та дозволи, записані в коді смарт-контракту, вимагають точної послідовності

подій, щоб досягти успіху та ініціювати узгодження правил, написаних у контракті. Більше того, розумний контракт може мати термін, подібний до традиційних контрактів у реальному житті. Традиційні контракти регулюються законом, тоді як розумні контракти керуються програмним кодом, і вони мають юридичну силу. Основна ідея ринкового контракту заснована на простій логіці «ЯКЩО-ТО». Технічно немає обмежень на використання IF-THEN у коді смарт-контракту.

Оскільки кожен вузол майнінгу реплікує повну блокчейн-систему, ми розглянемо передумови з точки зору окремого вузла майнінгу. Системні архітектори можуть розрахувати потенційні характеристики ресурсів, що стосуються кількості вузлів, розміру мережі блокчейну, частоти транзакцій та затримки. «Розумного дому» може бути достатньо, щоб захистити власні мережі IoT від незаконної «мутації», однак, щоб отримати повний комплекс, індивідуальний «розумний дім» повинен брати участь у невеликій спільноті або великому приватному блокчейні – рис. 3.4 [90 – 100].

Рисунок 3.4 – Архітектура забезпечення функціонування ВС–технології для мережі «розумних будинків»

Рис. 3.5 ілюструє схему вимог з точки зору розумного будинку для адаптації блокчейна [90 – 100].

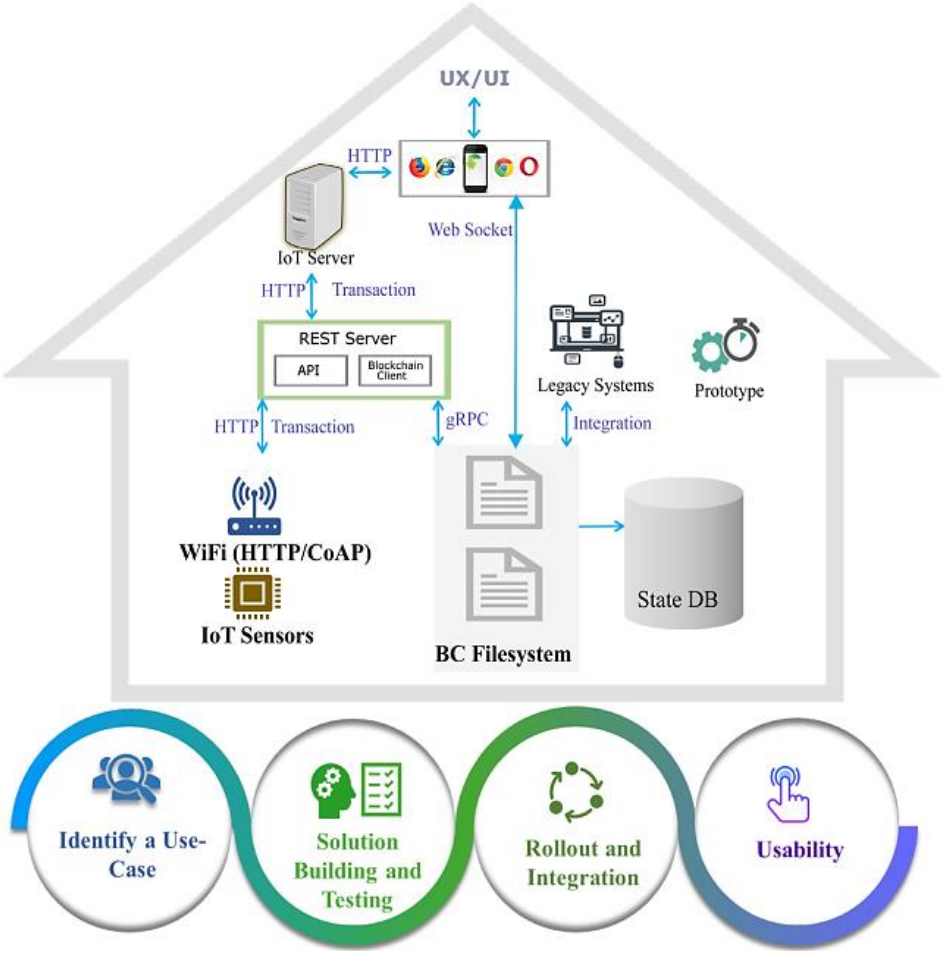

Рисунок 3.5 – Програмно-апаратна схема функціонування кіберфізичної IoT–системи «розумний дім» заснованої на BC–технології

Важливою частиною будь-якої реалізації блокчейну «розумного будинку» є вибір правильної платформи блокчейну (наприклад, з дозволом) та її алгоритм консенсусу. Критерії вибору залежать від кількох факторів, таких як кількість майнерів у мережі, частота транзакцій та частота вставки блоку. Наприклад, якщо частота вставки блоків у запропонованих блокчейн-системах висока, архітектор системи повинен вибрати легку платформу блокчейну та механізм консенсусу. У цьому сценарії можлива приватна блокчейн-платформа з менш дорогим консенсусним протоколом. Однак середовище розробки смарт-

контрактів відрізняється для різних платформ. Реалізація Hyperledger або будь-якого налаштованого протоколу вимагає глибокого знання мови ланцюгового коду [90 – 100].

Вимоги до обладнання залежать від необхідної пропускної здатності системи та архітектури програмного забезпечення. Після того, як вимоги до програмного та апаратного забезпечення будуть визначені належним чином, наступним етапом є впровадження прототипу в реальному розумному домі. Матриця продуктивності та процедура приймального випробування Acceptance Test Procedure (ATP) можуть допомогти досягти бажаної платформи блокчейн.

Після завершення створення та тестування блокчейн–рішення для розумного дому користувач може захопитися і повністю перейти від застарілих систем ІКТ для розумного дому на нову технологію. Однак така спроба може викликати потенційні складності для традиційних систем, оскільки кожна програма має свої сили та обмеження для адаптації до нової платформи. Тому перемикання однієї програми за раз із застарілих систем на нещодавно впроваджені блокчейн–системи було б хорошою практикою. Таким чином, буде легко повернутися назад, якщо інтеграція не вдається через непередбачувані причини. Ця практика поступово об’єднає всі застарілі системи в нову систему блокчейну. Крім того, через обмеження інтеграції користувачеві може знадобитися зберігати як застарілі, так і нові системи блокчейну разом.

Метод матеріалізації переваг блокчейн–систем розумного дому та його послуг із доданою вартістю полягає у створенні простого та легкого UX/UI (досвід користувача/інтерфейс користувача / User experience/User Interface). Цей інтерфейс відіграє важливу роль, оскільки без відповідного UX буде важко отримати задовільний відгук користувачів. Такий зворотній зв’язок має вирішальне значення для широкомасштабного прийняття цієї системи, яка може визначити майбутнє блокчейн-систем «розумного будинку». Таким чином, вимога реального інтерфейсу користувача є надзвичайно важливою. Таким чином, розробка веб-інформаційної панелі може допомогти

адміністратору та користувачеві лише для читання отримати доступ до розумного дому [90 – 100].

Пропонована структура кіберфізичної IoT–системи «розумний дім» на базі BC–технології, що заснована на BC–технології проілюстрована на рис. 3.6.

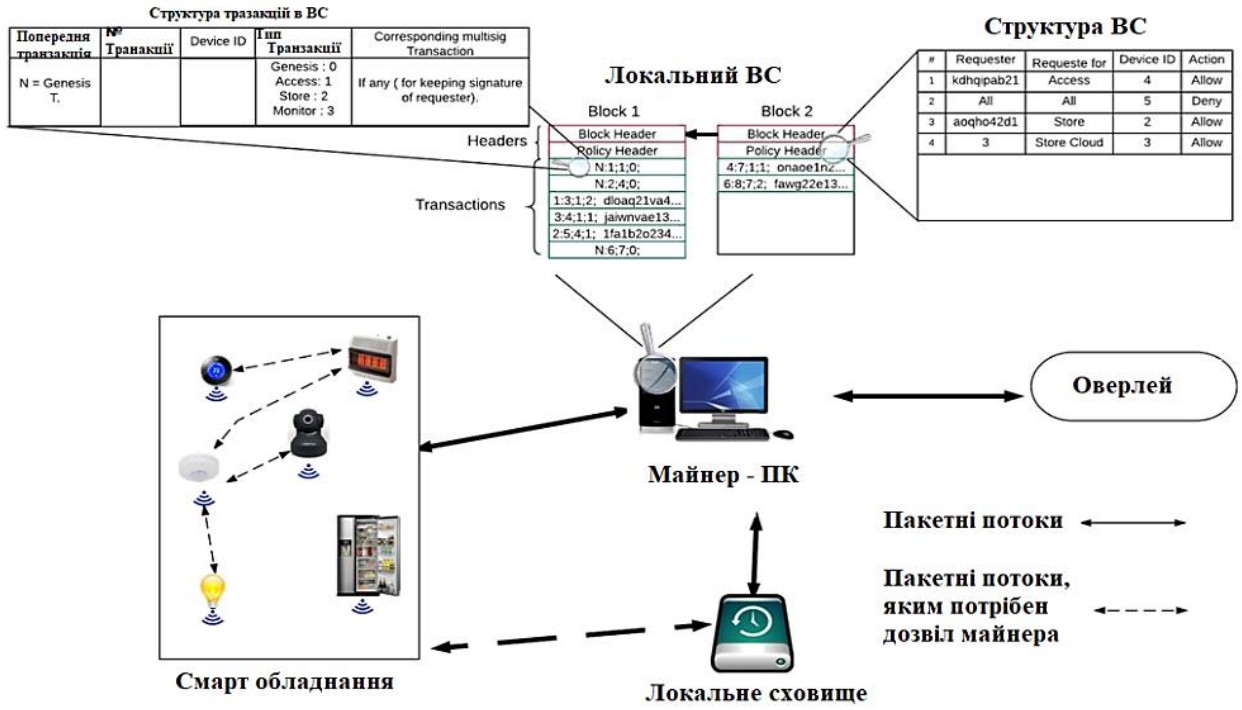

Рисунок 3.6 – Пропонована структура кіберфізичної IoT–системи «розумний дім» на базі BC–технології

Зв'язок між локальними пристроями або оверлейними вузлами називається транзакціями. Є різні транзакції в «розумному будинку» на базі BC, кожен з яких призначений для певної функції. Зберігання транзакції генерується пристроями для зберігання даних. Транзакція доступу генерується Постачальником послуг або власником будинку для доступу до хмарного сховища. Монітор транзакції генерується власником будинку або постачальником послуг для періодичного моніторингу інформації про пристрій.

Додавання нового пристрою в «розумний дім» виконується за допомогою транзакції Genesis, а пристрій видаляється за допомогою транзакції видалення. Всі вищезгадані транзакції використовують загальний ключ для захисту зв'язку. Полегшене хешування використовується для виявлення будь-яких змін у вмісті

транзакцій під час передачі. Всі транзакції в або з «розумного будинку» зберігаються в локальному приватному ланцюжку блоків (BC).

Безпосередній процес BC–аутентифікації користувача інженерними пристроями та мережами супроводу життєвого середовища на базі технології кіберфізичної IoT–системи «розумний дім» вказаний на рис. 3.7, при цьому розглянутий можливий сценарій верифікації нового користувача, що не є власником системи [90 – 100].

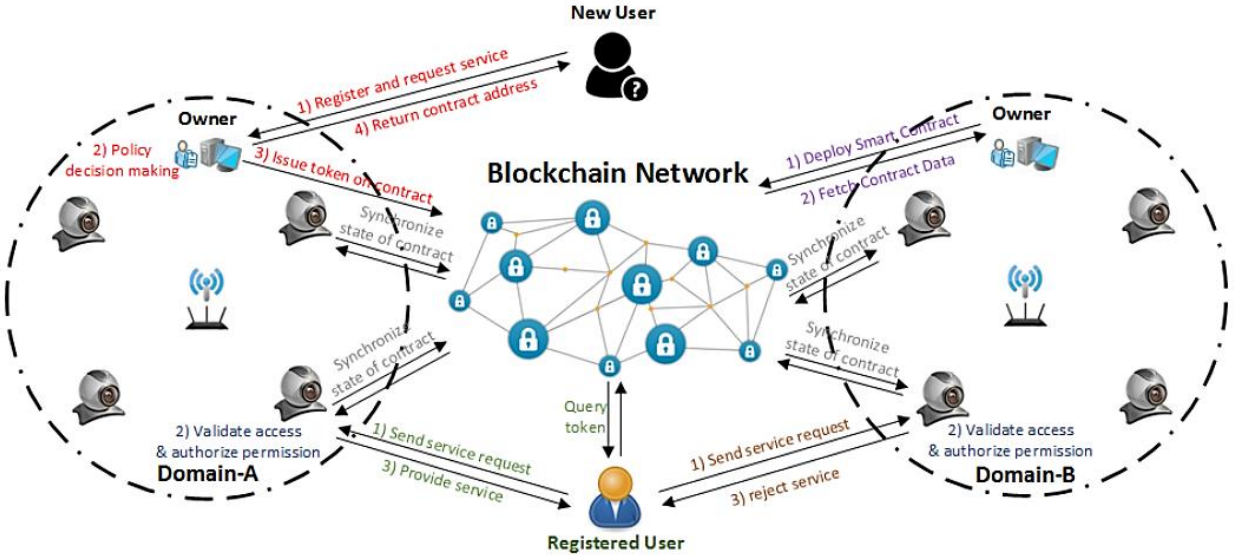

Рисунок 3.7 – Візуалізація процесів BC–аутентифікації в IoT–системі «розумний дім»

Щоб проілюструвати, як працює система, ми розглянемо приклад відвідувача, якому можна надати індивідуальний доступ до розумного дому, щоб годувати домашню тварину, замкнену всередині. На рис. 3.7 показано, як блокчейн допомагає отримати безпечний доступ:

(1) Відвідувач повинен вказати свій рівень доступу та ініціювати запит до комп’ютера, що обслуговує вдома. Наприклад, чоловік/дружина отримує дозвіл найвищого рівня (адміністратора), тоді як підлітки, діти, відвідування родини та няня отримують дозвіл середнього рівня. Сусіди або незнайомці отримують низькорівневий (нульовий) дозвіл доступу.

(2) Отримавши запит відвідувача, домашній сервер перевіряє список контролю доступу (ACL). Потім домашній сервер пересилає цей запит до блокчейну для перевірки політики цього конкретного користувача.

(3) Заголовок політики блокчейну зберігає ACL для різних користувачів і пристроїв. Заголовок політики – це частина даних блоку, яка використовується для реалізації політики керування та пристроїв авторизації.

(4) Запит, отриманий від нового користувача, пересилається до адміністратора, який може авторизувати або відхилити будь-який запит на доступ.

(5) Після того, як адміністратор надає доступ, майнер блокчейн вставляє інформацію в політику заголовка та виконує дії.

(6) Відвідувачам дозволяється отримувати доступ і виконувати дії згідно з правилами, запровадженими в ACL.

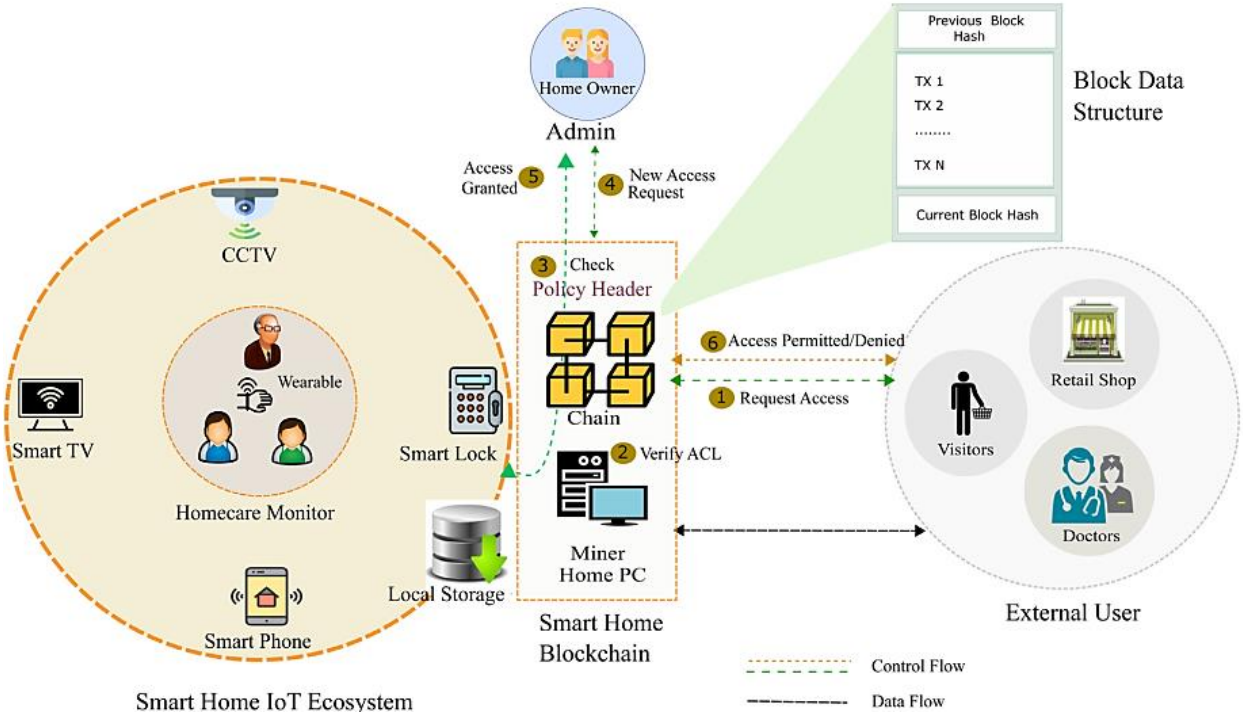

Рисунок 3.8 – Ілюстрація функціонування ВС–аутентифікації в засобах захисту кіберфізичної системи «розумний дім»

Блокчейн забезпечує два рівні захисту вхідного та вихідного трафіку, щоб протистояти атаці розподіленої відмови в обслуговуванні (DDOS).

Висновок до третього розділу

Таким чином, встановлено перспективність застосування ВС–технології для удосконалення кіберфізичної IoT–системи «розумний дім», що може бути оптимізована (за ресусоспоживанням, відповідно до рішень у п. 2.3 цієї праці) та адаптована (відповідно до пропозицій в п. 3.3 цієї праці) для інтелектуальних пристроїв та мереж інженерного супроводу життєдіяльності. Зокрема найвищий потенціал запропонованої до впровадження технологія є ВС–аутентифікація, що дозволить убезпечити екосистему «розумний дім» від найчастіше застосовуваних кібернападів – викрадення конфіденційної інформації з метою отримання контролю над елементами досліджуваної IoT–системи.

ВИСНОВКИ

Удосконалено метод захисту інформації у кіберфізичних системах, на прикладі IoT–системи «розумний дім».

У відповідності до поставних мети та задач дослідження встановлено наступне:

– досліджувана кіберфізична система є не лише засобом задоволення потреб локальних мешканців «розумного» житлового середовища, а є інструментом раціоналізації і оптимізації ощадного використання енергії та ресурсів та інтегрується в комплексну систему «розумного» міста;

– встановлена численна варіативність електронно-конструктивного виконання як окремих пристроїв так і комплексних систем, що представлені в профільному сегменті ринку та з урахуванням відповідних особливостей функціонування і проектних рішень можуть бути залучені до побудови кіберфізичної IoT–системи «розумний дім»;

– поруч з розвитком інженерних мереж та пристроїв супроводу життєзабезпечення, проблемою є саме особливість кіберфізичної системи як такої, оскільки існує загроза шляхом кібер-цифрової атаки безпосередньо впливати на фізичний рівень контрольованих пристроїв та мереж, що створює глобальну цивілізаційну загрозу та актуалізує дослідження та розробку рішень щодо захисту складових технології «інтернету речей». Виявлено, що найпоширенішою загрозою для IoT–системи «розумний дім» є втрата конфіденційної інформації, що призводить до втрати контролю над кіберфізичними керованими елементами і мережами інженерного супроводу життєдіяльності в локальному житловому середовищі;

– наразі існує достатня кількість методів та інструментаріїв моделювання кіберзагроз і кібернападу, що успішно використовуються для тестування і пошуку загроз безпеки кіберфізичних систем на базі технології IoT та можуть бути застосовані безпосередньо для моделювання кібер-цифрових атак на

комплекс пристроїв та мереж інженерного супроводу життєдіяльності «розумний дім»;

– використання адаптованого математичного апарату дозволяє не лише залучити до кіберзахисту IoT–системи «розумного дому» найефективнішої та оптимізованої (в т.ч. за витратою ресурсів), а й дозволяє застосувати ітераційний метод оцінювання ефективності застосовуваних СІБ з метою їх подальшого удосконалення та розвитку (з формуванням відповідної бази даних, що буде використовувана виробниками досліджуваних кіберфізичних систем);

– досягнуте наукове завдання щодо удосконалення інформаційного захисту кіберфізичної IoT–системи «розумний дім» шляхом впровадження оптимізованої (за ресурсоємністю механізму дії, як доведено вище) Blockchain–технології для надійної автентифікації, що є актуальним та сучасним рішенням з застосуванням провідних цифрових технологій;

– встановлено перспективність застосування BC–технології для удосконалення кіберфізичної IoT–системи «розумний дім», що може бути оптимізована (за ресусоспоживанням, відповідно до рішень у п. 2.3 цієї праці) та адаптована (відповідно до пропозицій в п. 3.3 цієї праці) для інтелектуальних пристроїв та мереж інженерного супроводу життєдіяльності. Зокрема найвищий потенціал запропонованої до впровадження технологія є BC–аутентифікація, що дозволить убезпечити екосистему «розумний дім» від найчастіше застосовуваних кібернападів – викрадення конфіденційної інформації з метою отримання контролю над елементами досліджуваної IoT–системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про національну безпеку України [Електронний ресурс] : Закон України від 21.06.2018 № 2469-VIII Про національну безпеку України (З останніми змінами, внесеними Законом України від 16.07.2021 № 1702-IX) / Верховна Рада України. – Офіційний сайт Верховної Ради України : Режим доступу [сайт] : zakon.rada.gov.ua, 2022.

2. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України від 05.10.2017 № 2163-VIII Про основні засади забезпечення кібербезпеки України (З останніми змінами, внесеними Законом від 18.11.2021 № 1907-IX) / Верховна Рада України. – Офіційний сайт Верховної Ради України : Режим доступу [сайт] : zakon.rada.gov.ua, 2022.

3. Про критичну інфраструктуру [Електронний ресурс] : Закон України від 16.11.2021 № 1882-IX Про критичну інфраструктуру / Верховна Рада України. – Офіційний сайт Верховної Ради України : Режим доступу [сайт] : zakon.rada.gov.ua, 2022.

4. Про електронні комунікації [Електронний ресурс] : Закон України від 16.12.2020 № 1089-IX Про електронні комунікації / Верховна Рада України. – Офіційний сайт Верховної Ради України : Режим доступу [сайт] : zakon.rada.gov.ua, 2022.

5. Стратегія кібербезпеки України [Електронний ресурс] : Указ від 01.02.2022 № 37/2022 Про рішення Ради національної безпеки і оборони України від 30.12.2021 року Про План реалізації Стратегії кібербезпеки України / Президент України. – Офіційний сайт Президента України : Режим доступу [сайт] : president.gov.ua, 2022.

6. Li, W. Mapping Two Decades of Smart Home Research: A Systematic Scientometric Analysis [Web resource] / W. Li [et al.]. // Technological Forecasting and Social Change. – 2022. – Vol. 179. – pp. 1-25. // Access mode [site] : sciencedirect.com, 2022.

7. Wilson, C. Benefits and risks of smart home technologies [Web resource] / C. Wilson, T. Hargreaves, R. Hauxwell-Baldwin // Energy Policy. – 2017. – Vol. 103. – pp. 72 – 83 // Access mode [site] : sciencedirect.com, 2022.

8. Kyas, O. To Smart Home: A Step by Step Guide for Smart Homes & Building Automation [Text] : Monograph / O. Kyas. – New York: Key Concept Press, 2017. – 337 p.

9. Miller, M. My Smart Home for Seniors [Text] : Monograph / M. Miller. – Que Publishing, 2017. – 384 p.

10. Vandome, N. Smart Homes in easy steps: Master smart technology for your home [Text] : Monograph / N. Vandome. – In Easy Steps Limited, 2018. – 192 p.

11. Pinto, G. Transfer learning for smart buildings: A critical review of algorithms, applications, and future perspectives [Web resource] / G. Pinto [et al.]. // Advances in Applied Energy. – 2022. – Vol. 5. – pp. 1 – 23 // Access mode [site] : sciencedirect.com, 2022.

12. Radha, R. K. Flexible smart home design: Case study to design future smart home prototypes [Web resource] / R. K. Radha // Ain Shams Engineering Journal. – 2022. – Vol. 13. – Iss. 1. – pp. 1 – 17 // Access mode [site] : sciencedirect.com, 2022.

13. Nasir, M. Enabling automation and edge intelligence over resource constraint IoT devices for smart home [Web resource] / M. Nasir [et al.]. // Neurocomputing. – 2022. – Vol. 491. – pp. 494 – 506 // Access mode [site] : sciencedirect.com, 2022.

14. Imran. IoT Task Management Mechanism Based on Predictive Optimization for Efficient Energy Consumption in Smart Residential Buildings [Web resource] / Imran, N. Iqbal, D. H. Kim // Energy and Buildings. – 2022. – Vol. 257. – pp. 1 – 23 // Access mode [site] : sciencedirect.com, 2022.

15. Azrour, M. IoT and Smart Devices for Sustainable Environment [Text] : Monograph / M. Azrour, A. Irshad, R. Chaganti. – Cham: Springer, 2022. – 188 p.

16. Home Networking & Smart Devices [Text] : Monograph / BDM. – Papercut Limited, 2022. — 100 p.

17. Chelliah, P. R. Applied Learning Algorithms for Intelligent IoT [Text] : Monograph / P. R. Chelliah, U. Sakthivel, S. Nagarajan. – CRC Press, 2022. — 369 p.

18. Neustein, A. Advances in Ubiquitous Computing: Cyber-Physical Systems, Smart Cities and Ecological Monitoring [Text] : Monograph / A. Neustein. – Elsevier Inc., 2020. – 336 p.

19. Rodrigues J. Cyber-Physical Systems for Next-Generation Network [Text] : Monograph / J. Rodrigues, A. Gawanmeh. – IGI Global, 2018. – 308 p.

20. Ranjan, R. Handbook of Integration of Cloud Computing, Cyber Physical Systems and Internet of Things [Text] : Monograph / R. Ranjan [et al.]. – Springer, 2020. – 337 p.

21. Mittal, S. Complexity Challenges in Cyber Physical Systems: Using Modeling and Simulation (M&S) to Support Intelligence, Adaptation and Autonomy [Text] : Monograph / S. Mittal, A. Tolk. – Wiley, 2020. – 432 p.

22. Liu, Y. Smart Sensors and Systems: Technology Advancement and Application Demonstrations [Text] : Monograph / Y. Liu, C.-M. Kyung, H. Yasuura. – New York: Springer, 2020. – 207 p.

23. Khajeh, H. Flexibility Potential of a Smart Home to Provide TSO-DSO-level Services [Web resource] / H. Khajeh, H. Firoozi, H. Laaksonen // Electric Power Systems Research. – 2022. – Vol. 205. – pp. 1 – 12 // Access mode [site] : sciencedirect.com, 2022.

24. Arab, M. B. Suitable various-goal energy management system for smart home based on photovoltaic generator and electric vehicles [Web resource] / M. B. Arab, M. Rekik, L. Krichen // Journal of Building Engineering. – 2022. – Vol. 52. – pp. 1 – 22 // Access mode [site] : sciencedirect.com, 2022.

25. Qureshi, K. N. Trust aware energy management system for smart homes appliances [Web resource] / K. N. Qureshi [et al.]. // Computers & Electrical Engineering. – 2022. – Vol. 97. – pp. 1 – 13 // Access mode [site] : sciencedirect.com, 2022.

26. Kumar, T. An Emergy-based Approach to Evaluate the Effectiveness of Integrating IoT-based Sensing Systems into Smart Buildings [Web resource] / T. Kumar [et al.]. // Sustainable Energy Technologies and Assessments. – 2022. – Vol. 52. – Part C. – pp. 1 – 15 // Access mode [site] : sciencedirect.com, 2022.

27. Teslyuk, V. Neural controller for smart house security subsystem [Web resource] / V. Teslyuk [et al.]. // Procedia Computer Science. – 2019. – Vol. 106. – pp. 394 – 401 // Access mode [site] : sciencedirect.com, 2022.

28. Chohan, A. H. Development of smart application for house condition survey [Web resource] / A. H. Chohan [et al.]. // Ain Shams Engineering Journal. – 2022. – Vol. 13. – Iss. 3. – pp. 1 – 9 // Access mode [site] : sciencedirect.com, 2022.

29. Sung, W.-T. The application of thermal comfort control based on Smart House System of IoT [Web resource] / W.-T. Sung, S.-J. Hsiao // Measurement. – 2020. – Vol. 149. – pp. 1 – 12 // Access mode [site] : sciencedirect.com, 2022.

30. Hosseinihaghighi, S. Discovering, processing and consolidating housing stock and smart thermostat data in support of energy end-use mapping and housing retrofit program planning [Web resource] / S. Hosseinihaghighi [et al.]. // Sustainable Cities and Society. – 2022. – Vol. 78. – pp. 1 – 15 // Access mode [site] : sciencedirect.com, 2022.

31. Dahal, K. Internet of Things and Its Applications: Select Proceedings of ICIA 2020 [Text] : Monograph / K. Daha [et al.]. – Springer, 2022. – 457 p.

32. Guarda, T. Information and Knowledge in Internet of Things [Text] : Monograph / T. Guarda [et al.]. – Springer, 2022. – 483 p.

33. James, A. IoT System Design: Project Based Approach [Text] : Monograph / A. James, A. Seth, S. C. Mukhopadhyay. – Springer, 2022. – 291 p.

34. Mangla, M. Real-Life Applications of the Internet of Things [Text] : Monograph / M. Mangla [et al.]. – CRC Press/Apple Academic Press, 2022. – 516 p.

35. Кукунін, С. В. Розробка цілісної методології організації систем типу «розумний будинок» в рамках парадигми «інтернету речей» [Електронний ресурс] / С. В. Кунін // Комп’ютерно-інтегровані технології: освіта, наука, вир-

во. – 2020. – Вип. 38. – С. 40-45. – Режим доступу [сайт] : cit-journal.com.ua, 2022.

36. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки [Текст] : ДСТУ (Державний стандарт України) / Технічний комітет зі стандартизації «Інформаційні технології» (ТК 20). – Київ: ДП «УкрНДНЦ», 2018. – 44 с.

37. Тарасюк, А. В. Теоретико-правові основи забезпечення кібербезпеки України [Текст] : Дисертація на здобуття наукового ступеня доктора юридичних наук зі спеціальності 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право; 08 – Право / А. В. Тарасюк. – Інститут інформації, безпеки і права Національної академії правових наук України. – Київ, 2021. – 461 с.

38. Веселова, Л. Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни [Текст] : Дисертація на здобуття наукового ступеня доктора юридичних наук зі спеціальності 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право; 08 – Право / Л. Ю. Веселова. – Одеський державний університет внутрішніх справ. – Одеса, 2021. – 500 с.

39. Проценко, О. Б. Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку [Текст] : Збірник матеріалів наукового круглого столу. м. Маріуполь, 26 квітня 2018 р. / О. Б. Проценко, К.В. Меркулова. – Маріуполь: Маріупольський державний університет, 2018. – 145 с.

40. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект [Текст] : Підручник / В. Л. Бурячок [та інш.]. – Київ: ДУТ, 2015. – 288 с.

41. Бойко, В. О. Державно-приватне партнерство у сфері кібербезпеки: кейс Німеччина [Текст] : Аналітична записка / В. О. Бойко. – К.: Національний інститут стратегічних досліджень, Відділ інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень 2018. – 18 с.

42. Дубова, Д. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України [Текст] : Аналітична доповідь / Д. Дубова. – Київ : НІСД, 2018. – 84 с.

43. Alexandrou, A. Cybercrime and Information Technology: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices [Text] : Monograph / A. Alexandrou. – CRC Press, 2022. – 455 p.

44. Mangesh, G. M. Cyber Security and Digital Forensics: Challenges and Future Trends [Text] : Monograph / G. M. Mangesh, P. Sabyasachi. – Wiley-Scrivener, 2022. – 432 p.

45. Goyal, D. Cyber-Physical Systems and Industry 4.0: Practical Applications and Security Management [Text] : Monograph / D. Goyal [et al.]. – Apple Academic Press Inc., CRC Press, 2022. – 290 p.

46. Khanna, K. Cyber Security and Digital Forensics [Text] : Monograph / K. Khanna, V. V. Estrela, J. J. P. C. Rodrigues. – Springer, 2022. – 623 p.

47. Lehto, M. Cyber Security: Critical Infrastructure Protection [Text] : Monograph / M. Lehto, P. Neittaanmäki. – Springer, 2022. – 486 p.

48. Maglaras, L. Cybersecurity Issues in Emerging Technologies [Text] : Monograph / L. Maglaras, I. Kantzavelou. – CRC Press, 2022. – 227 p.

49. Мужанова, Т. М. Інформаційна безпека держави [Текст] : Навчальний посібник / Т. М. Мужанова. – Київ: Державний університет телекомунікацій, 2019. – 131 с.

50. Бобало, Ю. Я. Інформаційна безпека [Текст] : Навчальний посібник / Ю. Я. Бобало [та інш.]. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.

51. Ахрамович, В. М. Курс лекцій з навчальної дисципліни Кібербезпека банківських та комерційних структур [Текст] : Навчальний посібник / В. М. Ахрамович. – Київ: ДУТ, 2019. – 163 с.

52. Зернецька, О. В. Глобальна комунікація [Текст] : Монографія / О. В. Зернецька. – Київ : Наукова думка, 2017. – 350 с.

53. Pal, S. IoT: Security and Privacy Paradigm [Text] : Monograph / S. Pal, V. G. Diaz, D.-N. Le. – CRC Press, 2020. – 398 p.

54. Wu, C. Security of Cyber-Physical Systems: State Estimation and Control [Text] : Monograph / C. Wu [et al.]. – Springer, 2022. – 293 p.

55. Skillicorn, D. B. Cyberspace, Data Analytics, and Policing [Text] : Monograph / D. B. Skillicorn. – CRC Press, 2022. – 274 p.

56. Santos, H. M. D. Cybersecurity: A Practical Engineering Approach [Text] : Monograph / H. M. D. Santos. – CRC Press, 2022. – 340 p.

57. Priyadarshini, I. Artificial Intelligence and Cybersecurity: Advances and Innovations [Text] : Monograph / I. Priyadarshini, R. Sharma. – CRC Press, Taylor & Francis Group, LLC, 2022. – 223 p.

58. Abaimov, S. Machine Learning for Cyber Agents: Attack and Defence [Text] : Monograph / S. Abaimov, M. Martellini. – Springer, 2022. – 235 p.

59. Maleh, Y. Machine Intelligence and Big Data Analytics for Cybersecurity Applications [Text] : Monograph / Y. Maleh [et al.]. – Springer, 2021. – 533 p.

60. Pascal, A. Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment [Text] : Monograph / A. Pascal. – Packt Publishing, 2021. – 800 p.

61. Fiedelholtz, A. The Cyber Security Network Guide [Text] : Monograph / A. Fiedelholtz. – Springer, 2020. – 97 p.

62. Tony, T. Machine Learning Approaches in Cyber Security Analytics [Text] : Monograph / T. Tony, V. Athira, E. Sabu. – Springer, 2020. – 217 p.

63. Stolojescu-Crisan, C. Access control and surveillance in a smart home [Web resource] / C. Stolojescu-Crisan, C. Crisan, B.-P. Butunoi // High-Confidence Computing. – 2022. – Vol. 2. – pp. 1 – 9 // Access mode [site] : sciencedirect.com, 2022.

64. Hammi, B. Survey on smart homes: Vulnerabilities, risks, and countermeasures [Web resource] / B. Hammi [et al.]. // Computers & Security. – 2022. – Vol. 117. – pp. 1 – 24 // Access mode [site] : sciencedirect.com, 2022.

65. Mahmood, A. A Solution to the Security Authentication Problem in Smart Houses Based on Speech [Web resource] / A. Mahmood // Procedia Computer Science. – 2019. – Vol. 155. – pp. 606 – 611 // Access mode [site] : sciencedirect.com, 2022.

66. Albany, M. A review: Secure Internet of thing System for Smart Houses [Web resource] / M. Albany [et al.]. // Procedia Computer Science. – 2022. – Vol. 201. – pp. 437 – 444 // Access mode [site] : sciencedirect.com, 2022.

67. Adamu, Z. M. Green Internet of Things Sensor Networks: Applications, Communication Technologies, and Security Challenges [Text] : Monograph / Z. M. Adamu [et al.]. – Springer, 2020. – 135 p.

68. Nayak, P. IoT Applications, Security Threats, and Countermeasures [Text] : Monograph / P. Nayak, N. Ray, P. Ravichandran. – CRC Press, 2022. – 279 p.

69. Qinghao, T. Internet of Things Security: Principles and Practice [Text] : Monograph / T. Qinghao, D. Fun. – Springer, 2021. – 292 p.

70. Sovacool, B. K. Knowledge, energy sustainability, and vulnerability in the demographics of smart home technology diffusion [Web resource] / B. K. Sovacool, M. Martiskainen, D. D. Furszyfer Del Rio // Energy Policy. – 2021. – Vol. 153. – pp. 1 – 18 // Access mode [site] : sciencedirect.com, 2022.

71. Hodges, D. Cyber-enabled burglary of smart homes [Web resource] / D. Hodges // Computers & Security. – 2021. – Vol. 110. – pp. 1 – 21 // Access mode [site] : sciencedirect.com, 2022.

72. Hughes, R. Smart plugs invite cyber criminals into the home [Web resource] / R. Hughes // Network Security. – 2021. – Vol. 2021. – Iss. 11. – pp. 9 – 12 // Access mode [site] : sciencedirect.com, 2022.

73. Heartfield, R. A taxonomy of cyber-physical threats and impact in the smart home [Web resource] / R. Heartfield [et al.]. // Computers & Security. – 2018. – Vol. 78. – pp. 398 – 428 // Access mode [site] : sciencedirect.com, 2022.

74. Базилевич, В. М. Захищена система розумного будинку з використанням Internet of Thsings [Електронний ресурс] / В. М. Базилевич [та

інш.] // Технічні науки та технології. – 2020. – № 2 (20). – С. 218 – 228 // Режим доступу [сайт] : tst.stu.cn.ua, 2022.

75. Рибак, Л. Я. Інтелектуальна інформаційна система «розумний замок» для захисту приміщень [Електронний ресурс] / Л. Я. Рибак, П. О. Кравець // Information systems and networks. – 2019. – № 6. – С. 41 – 51 // Режим доступу [сайт] : science.lpnu.ua, 2022.

76. Кукунін, С. В. Розробка цілісної методології організації систем типу «розумний будинок» в рамках парадигми «інтернету речей» [Електронний ресурс] / С. В. Кукунін // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2020. – № 38. – С. 40 – 45 // Режим доступу [сайт] : orcid.org, 2022.

77. Бєлов, О. Моделювання кіберзагроз для Інтернет речей [Електронний ресурс] / О. Бєлов, М. Делембовський, В. Шкляр // Transfer of Innovative Technologies. – 2021. – Vol. 4. – № 1. – pp. – 92 – 94 // Access mode [site] : tit.knuba.edu.ua, 2022.

78. Chantzis, F. Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things [Text] : Monograph / F. Chantzis [et al.]. – San Francisco : No Starch Press, 2021. – 464 p.

79. Jbair, M. Threat modelling for industrial cyber physical systems in the era of smart manufacturing [Web resource] / M. Jbair [et al.] // Computers in Industry. – 2022. – Vol. 137. – pp. 1 – 14 // Access mode [site] : sciencedirect.com, 2022.

80. Nweke, L. O. Threat Modelling of Cyber–Physical Systems Using an Applied π-Calculus [Web resource] / L. O. Nweke, G. K. Weldehawaryat, S. D. Wolthusen // International Journal of Critical Infrastructure Protection. – 2021. – Vol. 35. – pp. 1 – 11 // Access mode [site] : sciencedirect.com, 2022.

81. Zibak, A. A success model for cyber threat intelligence management platforms [Web resource] / A. Zibak, C. Sauerwein, A. Simpson // Computers & Security. – 2021. – Vol. 111. – pp. 1 – 14 // Access mode [site] : sciencedirect.com, 2022.

82. Al-Fawa'reh, M. Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior [Web resource] / M. Al-Fawa'reh [et al.]. // Egyptian Informatics Journal. – 2021. – pp. 1 – 13 // Access mode [site] : sciencedirect.com, 2022.

83. Zhao, J. Cyber threat prediction using dynamic heterogeneous graph learning [Web resource] / J. Zhao [et al.]. // Knowledge-Based Systems. – 2022. – Vol. 240. – pp. 1 – 24 // Access mode [site] : sciencedirect.com, 2022.

84. Tundis, A. A Feature-driven Method for Automating the Assessment of OSINT Cyber Threat Sources [Web resource] / A. Tundis, S. Ruppert, M. Mühlhäuser // Computers & Security. – 2022. – Vol. 113. – pp. 1 – 13 // Access mode [site] : sciencedirect.com, 2022.

85. Yevseiev, S. Synergy of building cybersecurity systems [Text] : Monograph / S. Yevseiev [et al.]. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

86. Ngoy, S. P. A Mathematical Modeling Approach in Cybersecurity using Deep neural Learning [Web resource] / P. S. Ngoy, K. Musumbu, D. K. Gathungu // International Journal of Advanced Research in Science, Engineering and Technology. – 2021. – Vol. 8. – Iss. 6. – pp. 1 – 18 // Access mode [site] : ijarset.com, 2022.

87. Valizadeh, M. H. Cybersecurity Games: Mathematical Approaches for Cyber Attack and Defense Modeling [Web resource] : Doctoral Dissertations / M. H. Valizadeh. – University of Connecticut, 2019. – 188 p. // Access mode [site] : opencommons.uconn.edu, 2022.

88. Chowdhury, F. Modelling cyber attacks [Web resource] / F. Chowdhury, M. S. Ferdous // International Journal of Network Security & Its Applications (IJNSA). – 2017. – Vol. 9. – № 4. – pp. 13 – 32 // Access mode [site] : aircconline.com, 2022.

89. Mishra, B. K. Mathematical model on distributed denial of service attack through Internet of things in a network [Web resource] / B. K. Mishra [et al.]. // Nonlinear Engineering. – 2019. – Vol. 8. – Iss. 1. – pp. 486 – 495 // Access mode [site] : degruyter.com, 2022.

90. Білова, А. О. Методи забезпечення безпеки розумного будинку [Електронний ресурс] / А. О. Білова, В. В. Онищенко // Кібербезпека: освіта, наука, техніка. – 2019. – № 2. – С. 134 – 141 // Режим доступу [сайт] : nbuv.gov.ua, 2022.

91. Адамов О. С. Блокчейн інфраструктура для захисту кіберсистем [Електронний ресурс] / О. С. Адамов [та інш.]. // Радіоелектроніка та інформатика. – 2018. – № 4. – С. 64 – 85 // Режим доступу [сайт] : openarchive.nure.ua, 2022.

92. Ebrahim, M. Blockchain as privacy and security solution for smart environments: A Survey [Web resource] / M. Ebrahim [et al.]. // arXiv:2203.08901v1 [cs.CR]. – 2022. – pp. 1 – 22 // Access mode [site] : arxiv.org, 2022.

93. Moniruzzaman, Md. Blockchain for smart homes: Review of current trends and research challenges [Web resource] / Md. Moniruzzaman [et al.]. // Computers & Electrical Engineering. – 2020. – Vol. 83. – pp. 1 – 17 // Access mode [site] : sciencedirect.com, 2022.

94. Ammi, M. Customized blockchain-based architecture for secure smart home for lightweight IoT [Web resource] / M. Ammi, S. Alarabi, E. Benkhelifa // Information Processing & Management. – 2021. – Vol. 58. – Iss. 3. – pp. 1 – 15 // Access mode [site] : sciencedirect.com, 2022.

95. Ren, Y. Multiple cloud storage mechanism based on blockchain in smart homes [Web resource] / Y. Ren [et al.]. // Future Generation Computer Systems. – 2020. – Vol. 115. – pp. 1 – 21 // Access mode [site] : sciencedirect.com, 2022.

96. Samuel, O. Towards sustainable smart cities: A secure and scalable trading system for residential homes using blockchain and artificial intelligence [Web resource] / O. Samuel [et al.]. // Sustainable Cities and Society. – 2021. – Vol. 76. – pp. 1 – 15 // Access mode [site] : sciencedirect.com, 2022.

97. Mukherjee, A. Unified smart home resource access along with authentication using Blockchain technology [Web resource] / A. Mukherjee [et al.]. //

Global Transitions Proceedings. – 2021. – Vol. 2. – Iss. 1. – pp. 29 – 34 // Access mode [site] : sciencedirect.com, 2022.

98. Zhang, S. A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain [Web resource] / S. Zhang, J. Rong, B. Wang // International Journal of Electrical Power & Energy Systems. – 2020. – Vol. 121. – pp. 1 – 25 // Access mode [site] : sciencedirect.com, 2022.

99. Minoli, D. Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach [Web resource] / D. Minoli // Internet of Things. – 2020. – Vol. 10. – pp. 1 – 6 // Access mode [site] : sciencedirect.com, 2022.

100. Lee, Y. A blockchain-based smart home gateway architecture for preventing data forgery [Web resource] / Y. Lee [et al.]. // Human-centric Computing and Information Sciences. – 2020. – Vol. 10. – pp. 1 – 14 // Access mode [site] : hcis-journal.springeropen.com, 2022.