

Факультет _____ Комп'ютерних наук _____
(повна назва)

Кафедра _____ Програмної інженерії _____
(повна назва)

АТЕСТАЦІЙНА РОБОТА **Пояснювальна записка**

_____ другий (магістерський) _____
(рівень вищої освіти)

Дослідження методів управління в smart house та створення профілів
комфорту користувачів
(тема)

Виконав: студент 2 курсу, групи ІПЗм-17-1 _____
спеціальності 121- Інженерія програмного забезпечення
(код і повна назва спеціальності)

Освітньо-наукової програми
Інженерія програмного забезпечення _____
(повна назва освітньої програми)

_____ Степко А.Г. _____
(прізвище, ініціали)
Керівник _____ доц. Турута О.П. _____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри, проф. _____

З.В.Дудар

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Програмної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 121-Інженерія програмного забезпечення

(код і повна назва)

освітньо-наукова програма Інженерія програмного забезпечення

(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____

(підпис)

« _____ » _____ 20 ____ р.

ЗАВДАННЯ НА АТЕСТАЦІЙНУ РОБОТУ

студентові Степку Андрію Генадійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів управління в smart house та створення профілів комфорту користувачів
затверджена наказом по університету від “ ____ ” _____ 2019 р № 546СТ
заповнюється вручну після отримання наказу
2. Термін подання студентом роботи до екзаменаційної комісії: 20 червня 2019 р.
3. Вихідні дані до роботи: методи управління системами smart house, безпека систем smart house, профілі комфорту користувачів smart house. Використовувати платформи-незалежне програмне забезпечення.
4. Перелік питань, що потрібно опрацювати в роботі: мета роботи, аналіз проблемної галузі і постановка задачі, огляд підходів до управління системами smart house, методи забезпечення безпеки систем smart house, способи нівелювання різномірності апаратного забезпечення на програмному рівні smart house систем, способи забезпечення безпеки підключення нових приладів, підходи до побудови та застосування профілів комфорту користувачів як засобів інтелектуальної автоматизації.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Мета завдання, обґрунтування доцільності розроблення, постановка задачі, структурна схема системи управління smart house, структурна та функціональна схема приладу smart house, методи й підходи, діаграма послідовності початкового підключення приладу до smart house системи, демонстраційні матеріали

6 Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Спецчастина	доц. Турута О.П.		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка*
1.	Аналіз предметної галузі	19 квітня 2019р.	
2.	Огляд існуючих методів	27 квітня 2019р.	
3.	Методи управління Розумними Будинками	2 травня 2019р.	
4.	Підготовка пояснювальної записки	25 травня 2019р.	
5.	Спецчастина	26 травня 2019р.	
6.	Підготовка презентації та доповіді	28 травня 2019р.	
7.	Попередній захист	05 червня 2019р.	
8.	Нормоконтроль, рецензування	05 червня 2019р.	
9.	Занесення диплома в електронний архів	18 червня 2019р.	
10.	Допуск до захисту у зав. кафедри	18 червня 2019р.	
* заповнюється вручну після виконання чергового пункту			

Дата видачі завдання _____ 2019 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Турута О.П.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ/ABSTRACT

Пояснювальна записка до атестаційної роботи магістра: с., 7 рис., 3 додатки, 10 дж.

РОЗУМНИЙ БУДИНОК, ШЛЮЗ, СТРУКТУРНА ТА ФУНКЦІОНАЛЬНА АБСТРАКЦІЯ, ПОТОКИ УПРАВЛІННЯ, УПРАВЛЯЮЧІ КОМАНДИ, АВТОРИЗАЦІЯ, МАШИННЕ НАВЧАННЯ.

Об'єктом дослідження є системи управління Розумними Будинками. Метою роботи є дослідження методів управління системами Розумних Будинків та наробка підходів та технічних рішень, що покращували б такі системи управління. У результаті роботи проведені дослідження та розроблені підходи для систем управління Розумними Будинками, що спрощують розробку, розширення та підтримку таких систем, покращують рівень їх безпеки, а також підходи до інтелектуальної автоматизації у вигляді профілів комфорту користувачів.

SMART HOUSE, GATEWAY, STRUCTURAL AND FUNCTIONAL ABSTRACTION, MANAGEMENT FLOW, CONTROL COMMANDS, AUTHORISATION, MACHINE LEARNING

The aim of the work is the research of Smart House management systems methods and development of approaches and technical solutions which would improve such management systems. As the result researches were conducted and were suggested approaches for Smart House management systems, which simplify development, extension and support of such systems, improve their security and also for intellectual automation in the form of comfort profiles of users.

ЗМІСТ

Вступ	7
1 Огляд сфери розумних будинків та існуючих досліджень сфери управління системами розумних будинків	
1.1 Історія розвитку галузі Розумних Будинків	9
1.1.1 Технічна еволюція систем Розумних Будинків та технічні виклики на шляху розвитку цих систем	9
1.1.2 Розмаїття проектів Розумних Будинків та проекти-інтегратори	10
1.1.2.1 Різноморідність апаратних приладів	11
1.1.2.2 Шляхи розвитку проектів-інтеграторів Розумних Будинків	11
1.2 Невирішені проблеми галузі управління Розумними Будинками	12
1.2.1 Різноморідність	13
1.2.2 Безпека систем управління Розумними Будинками	14
1.2.3 Автоматизація та інтелектуалізація систем управління Розумними Будинками	15
1.3 Дослідження в галузі управління Розумними Будинками	16
1.4 Постановка задачі дослідження	17
2 Напрямок та шлях проведення досліджень	19
2.1 Обґрунтування напрямку досліджень	19
2.1.1 Доцільність дослідження різноморідності в системах управління Розумними Будинками	19
2.1.2 Доцільність дослідження безпеки систем управління Розумними Будинками	20
2.1.3 Доцільність дослідження підходів автоматизації та інтелектуалізації систем управління Розумними Будинками	21

2.2	Методика досліджень та шляхи пошуку нових технічних рішень для розв'язання поставлених задач	22
2.2.1	Шлях пошуку розв'язання проблеми різнорідності	23
2.2.2	Шлях пошуку розв'язання проблем безпеки систем управління Розумними Будинками	24
2.2.2.1	Пошук підходів до унеможливлення управління Розумним Будинком без відома користувача	25
2.2.2.2	Пошук рішення для початкового з'єднання прилада з будинком	25
2.2.2.3	Ролі та рівні доступу користувачів до управління Розумним Будинком	27
2.2.3	Шлях дослідження проблем автоматизації та інтелектуалізації	27
3	Різнорідність в системах управління Розумними Будинками	28
3.1	Проблема різнорідності апаратного забезпечення в управлінні	29
3.1.1	Типи різнорідностей	31
3.1.2	Причини різнорідності	32
3.2	Розв'язок проблеми різнорідності	33
3.2.1	Ініціювання взаємодії Шлюз-Річ	35
3.2.2	Параметр як неподільна складова структури Речі	36
3.2.3	Формулювання абстракції Розумної Речі	37
3.3	Шлюз та взаємодія Розумної Речі зі Шлюзом	39
3.3.1	Відповідальності Шлюза	39
3.3.2	Потік управління через Шлюз	40
3.3.3	Програмні адаптери на Шлюзі	41
4	Безпека систем управління Розумними Будинками	43
4.1	Авторизація запитів до Розумного Будинку	43
4.1.1	Команда з адресантом як засіб управління	43
4.1.2	Авторизація управляючих команд на Шлюзі	44

4.1.2.1	Управління ключами авторизації	44
4.1.2.2	Довіра Шлюза до початкових ключів	45
4.1.2.3	Недоліки криптографічної авторизації команд	46
4.2	Забезпечення безпеки початкового з'єднання Розумної Речі зі Шлюзом Розумного Будинку	47
5	Профілі комфорту користувачів Розумних Будинків	51
5.1	Способи використання інтелектуальної автоматизації Розумного Будинку	51
5.2	Використання профілів комфорту як основа пропозицій по управлінню Розумним Будинком	52
5.3	Забезпечення позитивного досвіду користувача під час впровадження автоматичного керування будинком	53
5.3.1	Перехід від пропозицій до повного автоматичного виконання	54
5.3.2	Безпека при управлінні Розумним Будинком засобами штучного інтелекту	55
5.4	Підхід до побудови профілю комфорту користувача	56
5.4.1	Навчання штучного інтелекту на абстрактних даних	57
5.4.2	Процедура навчання	58
5.4.3	Логістична регресія як модель навчання	59
	Висновки	61
	Перелік джерел посилання	63
	Додаток А Тези доповідей	65
	Додаток Б Слайди презентації	
	67	
	Додаток В Диск CDR	

ВСТУП

Сфера проектів Розумних Будинків має активний розвиток разом зі сферою Інтернету Речей продовж останніх років, проте має значну кількість проблем і технічних складностей досі не вирішених в існуючих проектах. Складності в цих сферах створює присутність апаратних частин у системі, що є фізично недосяжними для тих хто підтримує систему (знаходяться в будинках користувачів), а також високими вимогами до безпеки таких систем, адже часто ці системи отримують контроль над засобами забезпечення безпеки будинка.

Дослідження проведені в рамках цієї роботи спрямовані на розробку методів і підходів для прикладних програмних систем сфери Розумних Будинків, що мають на меті покращити певні властивості таких систем.

Метою роботи є розробка підходів та технічних рішень спрямованих на покращення методів управління системами Розумних Будинків зокрема та системами Інтернету Речей в цілому, а також на створення профілів комфорту користувача як засобів інтелектуальної автоматизації систем управління Розумними Будинками, що створюватиме новий позитивний досвід використання систем для користувача.

Для досягнення цих цілей необхідно вивчити підходи до методів управління, що застосовують в існуючих проектах сьогодні та що запропоновані в існуючих дослідженнях, виявити недоліки цих підходів, що створюють складності в роботі систем Розумних Будинків, а також визначити причини (початкові технічні проблеми) через які ті чи інші складності цих систем мають місце. Після такого дослідження та вивчення існуючих досліджень цієї сфери, слід розробити підходи, що дозволять нівелювати певні технічні проблеми сфери та зробити управління системами Розумних Будинків більш простим як з технічної так і з користувацької точки зору.

У роботі застосовані теоретичні методи дослідження, застосовані моделювання та формалізація певних частин в системі управління Розумними Речами з метою їх глибокого вивчення та створення підходів та конкретних технічних рішень для покращення цих систем.

В ході досліджень одержані результати, що є новими для галузі. Під час досліджень не було виявлено ані конкретних прикладних реалізацій, ані досліджень, що пропонують рішення для технічних проблем піднятих в рамках цієї роботи, або розв'язують задачі поставлені в рамках цієї роботи.

В результаті роботи напрацьовані підходи та конкретні технічні рішення застосування яких у системах управління Розумними Будинками дасть змогу спростити ці системи як з точки зору їх розробки так і з точки зору користування ними. Так технічне спрощення дасть змогу суттєво скоротити ресурси які необхідні для розробки, розширення та підтримки систем управління Розумними Будинками, особливо тих систем, які під час своєї роботи інтегрують прилади від декількох виробників. Також застосування підходів та протоколів спрямованих на забезпечення безпеки систем управління Розумними Будинками, що були розроблені в рамках цієї роботи, можуть суттєво знизити ризики атак зловмисників на системи Розумних Будинків та унеможливити захоплення контролю над Розумними Будинками.

В рамках проведених досліджень були опубліковані тези доповідей на тему боротьби з різномірністю апаратного забезпечення в системах управління Розумними Будинками.

1 ОГЛЯД СФЕРИ РОЗУМНИХ БУДИНКІВ ТА ІСНУЮЧИХ ДОСЛІДЖЕНЬ СФЕРИ УПРАВЛІННЯ СИСТЕМАМИ РОЗУМНИХ БУДИНКІВ

1.1 Історія розвитку галузі Розумних Будинків

Підґрунтям для створення й розвитку Розумних Будинків є ті основні цінності й переваги, які надають користувачам системи Розумних Будинків, а саме:

- можливість швидше та простіше виконувати певні дії в будинку, позбавляючи людини певної рутини;
- можливість автоматизувати виконання певних дій у будинку;
- можливість виконувати дії в будинку віддалено;
- оптимізувати витрати будинку на спожиті ресурси.

Отже економія ресурсів та створення додаткової зручності та комфорту є цінностями, які створюють системи управління Розумними Будинками для користувачів, а тому такі системи є цікавими й рентабельними для розробки й застосування.

1.1.1 Технічна еволюція систем Розумних Будинків та технічні виклики на шляху розвитку цих систем

Сфера Розумних Будинків розпочалася з програмно-апаратних проектів які дозволяли керування окремим приладом за певним бездротовим протоколом передачі даних. У подальшому системи ставали більш функціональними та нові вимоги до систем управління Розумними Будинками ускладнювали програмні рішення та створювали все нові й нові виклики для розробників цих систем.

Зокрема можна виділити такі вимоги до систем управління Розумними Будинками, які вплинули на дизайн цих систем, привносячи в цей дизайн певну складність:

- необхідність керувати великою кількістю приладів у будинку;
- віддалене керування Розумним Будинком – через Інтернет;
- необхідність для приладів певним чином взаємодіяти одне з одним;
- унеможливити кібератаки на Розумні Будинки з метою отримання конфіденційних даних або несанкціонованого управління будинком;

1.1.2 Розмаїття проектів Розумних Будинків та проекти-інтегратори

На ринку наразі існує велика кількість різних проектів Розумних Будинків, кожен з яких зазвичай не надає комплексного рішення для всіх сценаріїв використання Розумних Будинків. Сучасні проекти розумних будинків часто покривають лише деякі окремі сфери – такі як освітлення, опалення тощо, тож користувачі, що встановлюють різні системи Розумних Будинків в свої будинки відчують незручність протягом управління їх приладами (Розумними Речами). Необхідність управляти різними Розумними Речами в будинку в різних клієнтських додатках знижують якість досвіду користувачів та створює великий дискомфорт. Більше того, клієнтські додатки часто різноманітні, їх інтерфейс може сильно відрізнятись. Це ідея добра виражена в наступній цитаті зі статті одного дослідження: “Різнорідні сервіси приладів, згенеровані різними приладами в різних контекстах перешкоджають користувачам ефективно та коректно споживати сервіси приладів.” [1].

1.1.2.1 Різноманітність апаратних приладів

Інша проблема Розумних Приладів від різних виробників з різноманітними інтерфейсами полягає в відсутності можливості взаємодії Розумних Приладів одне з одними в будинку. Взаємодія цікава для створення сценаріїв та забезпечення роботи разом Розумних Речей, так як взаємодія Розумних Речей створює багато нових способів використання систем Розумних Будинків.

У цих умовах (різноманітні інтерфейси без стандартів чи уніфікації) взаємооперування та взаємозв'язок приладів від різних виробників досягається лише за рахунок проектів третьої сторони, які інтегрують Розумні Речі від різних виробників в єдину систему, забезпечуючи концентратор (хаб) для розумних Речей. Такі системи надбудовують ще один рівень над верхніми рівнями програмних інтерфейсів (API) проектів які ці системи інтегрують та усі взаємодія між кінцевим клієнтом та приладами відбувається через цей новий верхній рівень. Цей підхід дозволяє забезпечити користувачам єдиний додаток для управління, що використовується для всіх приладів користувача від різних систем Розумних Будинків.

1.1.2.2 Шляхи розвитку проектів-інтеграторів Розумних Будинків

Є два підходи в цих проектах-інтеграторах – 1) забезпечення програмного інтерфейсу (API) для різних апаратних приладів з якими запроваджується інтеграція; 2) реалізація інтеграції з різними апаратними приладами власноруч.

Перші не створюють інтеграції з апаратним забезпеченням, а надають програмний інтерфейс (API) з яким інтегруватися, так що апаратне забезпечення

може реалізувати інтеграцію та бути спроможним контролюватися через такий інтегратор. Інтегратори з таким підходом зазвичай створюють цінність в комфортному управлінні Розумними Речами та розробляють інтерфейси користувачів. Такими проектами-інтеграторами є наприклад Google Home [2] та Amazon Echo [3].

Другі інтегруються з різними системами Розумних Будинків та приладами самотужки. Наприклад проекти-інтегратори такі як OpenHUB[4] та Jeedom[5] використовують цей підхід.

Такі інтегруючі проекти є першими хто зтикається з різномірністю приладів Інтернету Речей. Програмні високорівневі інтерфейси розумних Речей в різних проектах не стандартизовані, що робить не тривіальною проблему в з'єднанні декількох різномірних типів приладів в єдину панель управління для кінцевого клієнта (користувача). Різномірність приладів Інтернету Речей це головна проблема, яку розв'язують такі проекти та це виявляється їх головною цінністю. Однак, деякі з таких інтегруючих проектів залишають різний, не уніфікований інтерфейс користувача для різних Розумних Речей в їх клієнтських додатках, у такий спосіб вирішуючи різномірність декількох виробників приладів, проте не вирішуючи різномірність намірів та функціональності приладів.

1.2 Невирішені проблеми галузі управління Розумними Будинками

Окрім різномірності описаної вище в підпункті про проекти-інтегратори, системи управління Розумними Будинками стикаються також із серйозними технічними виликами в контексті безпеки систем, а також зі складностями в запровадженні автоматизації процесів у будинку, що були б простими, зрозумілими та комфортними для користувача, а також цікавою та непростою є

тема інтелектуальності Розумних Будинків, якої потребує споживач подібних продуктів.

1.2.1 Різноманітність

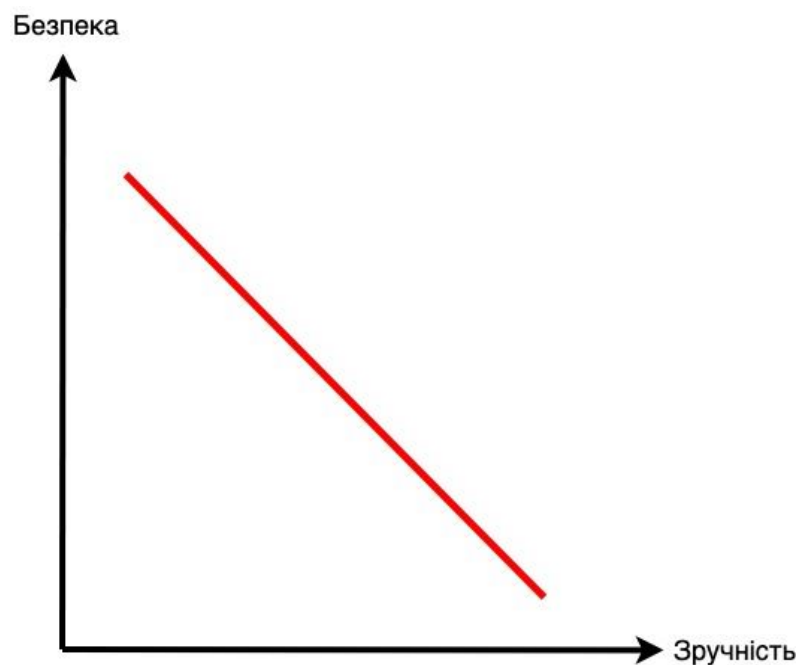
Управління розумними будинками має деяку кількість суттєвих складностей, які важко розв'язати цілком, проте можливо запропонувати відносно компромісне технічне рішення. Зокрема такою непростю проблемою систем розумних будинків зокрема та систем Інтернету Речей загалом є різноманітність апаратних приладів у таких системах. Зокрема ця проблема розглянута в даній роботі в якості дослідження методів управління систем розумних будинків.

Суть проблеми різноманітності полягає в тому, що в системах Інтернету Речей часто виникає необхідність взаємодіяти з апаратними приладами, що сильно відрізняються одне від одного, тож система має знати про специфіку роботи кожного типу таких апаратних приладів, а отже система стає різноманітною. Апаратні прилади різняться структурно та функціонально, відрізняються їх інтерфейси та способи взаємодії з ними, що зумовлено перш за все різноманіттям виробників цих приладів, які не мають уніфікації в проектуванні таких приладів, а системи Розумних Будинків часто вимушені взаємодіяти з приладами різних виробників.

Різноманітність таких систем є великою проблемою для цих систем через те, що це збільшує складність і розміри системи, що неодмінно тягне за собою ускладнення підтримки та розширення таких систем, що збільшує кількість ресурсів необхідних для розробки та підтримки систем.

1.2.2 Безпека систем управління Розумними Будинками

Для галузі управління Розумними Будинками надзвичайно критичною є вимога безпеки системи, адже успішні атаки означатимуть контроль зловмисника над приладами всередині будинку користувача, що є надзвичайно небезпечним та вкрай небажаним. Як відомо, безпека системи завжди протирічить комфорту її використання, залежність зручності від безпеки часто позначають графіком зображеним на Рисунку 1.



«Рисунок 1 – Залежність безпеки та зручності»

А так як Розумні Будинки покликані нести зручність і комфорт своїм користувачам, зручністю у таких системах не можна знехтувати. Усі ці передумови створюють непрості умови для розвитку й удосконалення безпеки систем управління Розумними Будинками та створюють необхідність знаходити нові непрості технічні рішення на стику безпеки системи та зручності її використання.

В контексті безпеки Розумних Будинків вдалих технічних рішень не було знайдено для процесу початкового підключення приладу (Розумної Речі) до системи управління Розумним Будинком, а також для організації безпеки в процесі взаємодії системи з приладами та користувача з системою, зокрема необхідно забезпечити нерозкриття даних, що передаються на всіх рівнях в рамках системи, а також забезпечити надійну авторизацію задля унеможливлення управління зловмисником будинком користувача, а також цікавою є задача унеможливлення для центральних серверів системи самотужки керувати будинком користувача без його згоди, рішень для чого також не було знайдено в процесі пошуку наукових досліджень на цю тему.

1.2.3 Автоматизація та інтелектуалізація систем управління Розумними Будинками

Процеси автоматизації рутинних процесів та залучення штучного інтелекту в системах управління Розумними Будинками мають деякі нерозв'язані проблеми, зокрема подібні процеси означають, що певна автоматизована (можливо інтелектуальна) сутність матиме доступ до керування будинком, що є ударом по безпеці системи та зазвичай при цьому користувач не матиме гнучкого та глибокого контролю над різноманітними дозволами що може та не може виконувати в його будинку автоматизована сутність.

В контексті інтелектуалізації систем управління Розумними Будинками цікавим є запровадження пропозицій автоматично виконувати дії в будинку замість користувача, проте це запровадження ускладнюється різноманіттям приладів, з якими необхідно взаємодіяти, тож такі запровадження наразі успішно реалізують тільки для відомих типів Розумних Речей (приладів) та тільки за

завчасно запрограмованою логікою. Цікавим же є дослідження можливості абстрактного інтелекту, здатного виробляти пропозиції для користувача незалежно від того, з якими приладами йде взаємодія ані з точки зору інтерфейсу цих приладів, ані з точки зору функціонального призначення приладів.

1.3 Дослідження в галузі управління Розумними Будинками

Є декілька досліджень, які намагаються знайти розв'язки для проблеми різноманітності приладів Інтернету Речей або намагаються стандартизувати інтерфейси цих приладів якимось чином. У [6] дослідженні запропоновано позбавитись різноманітності даних сенсорів шляхом пропозиції онтології приладів Інтернету Речей, що буде в змозі покрити всі прилади. Мета [6] дослідження в тому щоб запропонувати панель управління користувача, що дозволить поєднати прилади. Тож ідея в тому щоб запропонувати певну абстракцію над приладами Інтернету Речей, однак деякі атрибути відсутні та деякі зайві в контексті усунення різноманітності, що робить абстракцію непридатно для всіх приладів Інтернету Речей та зайві поля націлені на те щоби впоратись з деякими іншими проблемами, не з різноманітністю.

Інша робота пропонує фреймворк, який націлений на уможливлення для приладів користувачів взаємодіяти з різноманітними приладами [1]. Робота пропонує підхід трансформації структури реального приладу до певного віртуального приладу, підхід називається “device transformability model” (модель можливості трансформації приладу). Вони пропонують фреймворк, що також має на меті дозволити взаємодію між двома типами користувачів – постачальників приладів та споживачів приладів.

Також є дослідження, що спрямовані на стандартизацію та поліпшення безпекової частини взаємодії приладів Інтернету Речей, наприклад [7].

Це не дуже складно з технічної точки зору запропонувати стандарт для протоколів взаємодії приладів Інтернету Речей, однак дуже непросто з організаційної точки зору запровадити будь-які стандарти. Також різноманіття апаратного забезпечення приладів Інтернету Речей вірогідно залишиться та не дозволить стандартизувати цю сферу. Наступна цитата добре описує цю ситуацію: “There would be no common hardware platform that could be applied in every scenario.” (Не буде жодної загальної апаратної платформи, що може бути застосована для кожного сценарію.) [7]. У таких умовах розв’язання різноманітності шляхом приховування її в якомусь Шлюзі та розкривання тільки уніфікованого інтерфейсу зовні від Шлюза здається більш придатним до застосування для сучасної сфери.

1.4 Постановка задачі дослідження

Зважаючи на ті невирішені проблеми, що існують у галузі систем управління Розумними Будинками, задачею досліджень обрано дослідити проблему різноманітності в системах управління Розумними Будинками та запропонувати шляхи її якомога більшого нівелювання. В процесі чого слід описати інтерфейси та протоколи взаємодії на різних рівнях системи, застосування яких допоможе спростити систему знизити вплив різноманітності.

Також задачею є дослідження методів забезпечення безпеки в сучасних системах управління Розумними Будинками та розробка підходів, що дозволять покращити безпеку таких систем без суттєвого погіршення зручності користування системами – виробити способи надійної авторизації користувача

перед будинком, способи унеможливлення несанкціонованого захоплення контролю над будинком зокрема й з боку центрального сервера та способи безпечного початкового сполучення приладів з Розумним Будинком, а також безпечної передачі даних на всіх рівнях системи в процесі роботи.

А також задачею є розробка шляхів запровадження профілів комфорту користувачів, що означає залучення штучного інтелекту в систему з різнорідними різноманітними приладами, який матиме змогу надавати рекомендації користувачеві з приводу автоматизації певних дій у будинку. При цьому важливим є брати за основу ідею про те, що рекомендаційний інтелект повинен працювати в умовах необізнаності щодо приладів з якими взаємодіє, що робитиме цей інтелект дієвим будучи простим, а також дозволить йому не потребувати оновлень та знайти широке застосування, охоплюючи ширшу множину приладів.

2 НАПРЯМОК ТА ШЛЯХ ПРОВЕДЕННЯ ДОСЛІДЖЕНЬ

Проблематика систем управління Розумними Будинками є надзвичайно актуальною, адже сфера знаходить все більше й більше застосування та невпинно розширюється, тож успішні дослідження що запропонують підходи що покращать технічно такі системи стануть у нагоді багатьом.

2.1 Обґрунтування напрямку досліджень

Предметом досліджень є технічні проблеми систем управління Розумними Будинками, зокрема проблема різномірності в таких системах, проблема безпеки та проблема запровадження інтелектуального самостійного управління Розумним Будинком. Усі ці предмети досліджень є цікавими та важливими для дослідження через те що мають невирішені технічні проблеми та складності, вирішення яких може значно покращити певні властивості систем управління Розумними Будинками, а також спростити процес розробки й підтримки таких систем.

2.1.1 Доцільність дослідження різномірності в системах управління Розумними Будинками

Різнорідність притаманна сучасним системам управління Розумними Будинками на різних рівнях та ускладнює процеси розробки, підтримки та розширення цих систем через те що підтримка кожного з різномірних типів

потребує окремих незалежних зусиль, тож якщо мінімізувати різномірність хоча б на деяких рівнях систем управління, це спростить системи в цілому, що окрім зменшення витрат на розробку й підтримку, сприятиме кращій придатності до підтримки, бо, як відомо, просту систему легше підтримувати та недарма дизайн системи намагаються робити якомога простішим.

Саме тому доцільним є дослідити природу різномірності в системах управління Розумними Будинками та розробити підходи до її якомога більшого нівелювання в цих системах – це зменшить кількість ресурсів необхідних для розробки, підтримки та розширення цих систем, а також спростить їх дизайн в цілому, що обов'язково позитивно відобразиться на надійності, стабільності та передбачуваності систем управління Розумними Будинками.

2.1.2 Доцільність дослідження безпеки систем управління Розумними Будинками

Розумні Будинки є не тільки потенційним джерелом створення комфорту й зручності для жителів будинку, а й потенційним інструментом вторгнення до будинку зловмисниками у випадку успішних кібер-атак на будинок.

У разі отримання зловмисниками контролю над Розумним Будинком вони матимуть змогу потай спостерігати за тим що відбувається в будинку – отримувати доступ до камер відеоспостереження, даних про пересування мешканців всередині будинку, дані датчиків інфраструктури й тому подібне.

Більше того, у випадку заволодінням контролю над будинком зловмисниками, вони зможуть надсилати управляючі команди до будинку – керувати замками на дверях, управляти інфраструктурою, що може підірвати фізичну безпеку житла в цілому та навіть звести з розуму мешканців.

Отже, беззаперечним є факт надзвичайної важливості безпеки в сфері управління Розумними Будинками, а так як ця сфера перш за все створює вигоду користувачеві у вигляді надання зручності в користуванні будинком, впровадження найсуворіших заходів безпеки зробить користування системами менш зручним для користувача, а отже страждатиме головна вигода таких систем. Зважаючи на цей технічний конфлікт, часткове вирішення якого здатне покращити рівень безпеки систем Розумних Будинків, дослідження безпеки систем управління Розумних Будинків є надзвичайно доцільним, а також дуже цікавим з точки зору вирішення технічних протиріч.

2.1.3 Доцільність дослідження підходів автоматизації та інтелектуалізації систем управління Розумними Будинками

Автоматичне виконання певних дій у будинку та інтелектуальний помічник в системі управління Розумним Будинком – це природні шляхи розвитку цих систем, та деякі проекти Розумних Будинків уже йдуть цим шляхом. Користувачі хочуть щоб взаємодія з системою управління будинком відбувалась менш формально та більш близькою для користувачів мовою – природною мовою, а не мовою команд, а також щоб система не тільки виконувала команди, але й самостійно робила припущення які дії в який момент часу було б доцільно в будинку, а також аби інтелект розумів індивідуальну специфіку кожного користувача, будуючи в себе певний профіль комфорту кожного користувача, враховуючи поведінку користувача в будинку.

Однак залучення автоматизації та інтелектуалізації в системи управління Розумними Будинками ускладнено деякими технічними проблемами, зокрема складністю розширення штучного інтелекту з появою нових типів приладів та

складністю забезпечення безпеки та унеможливлення захоплення контролю над будинком з боку центрального сервера, адже в випадку коли інтелект управляє будинком, центральний сервер повинен мати доступ до управління будинком.

Тож цікавою та актуальною є дослідження автоматизації й інтелектуалізації та розробка підходів, що дозволять посилити безпеку та запровадити ширшу інтелектуалізацію в системах управління Розумними Будинками.

2.2 Методика досліджень та шляхи пошуку нових технічних рішень для розв'язання поставлених задач

Існуючі невирішені технічні проблеми та протиріччя слід досліджувати, ставлячи на меті виділити основні проблеми, а також корінь кожної проблеми. Під час досліджень слід визначити, що саме є основною перепорою яка досі заважала дослідникам розв'язати певні технічні проблеми в цій галузі.

Після виділення основних причин певних проблем та головних перепон боротьби з ними, слід направляти дослідження на винаходження способів, які дозволили б подолати ці проблеми та основні перепони. Можливо при застосуванні нових винайдених способів та підходів доведеться нехтувати якимись іншими властивостями системи.

Для того щоб критичні та важливі властивості системи не постраждали та не були погіршені під час змін до системи, слід завчасно сформулювати рамки за які не можна заходити в процесі розробки нових рішень – певні обмеження на властивості системи, якими не можна нехтувати, розробляючи та імплементуючи нові рішення.

2.2.1 Шлях пошуку розв'язання проблеми різномірності

Різномірність в системах управління Розумними Будинками присутня на багатьох рівнях системи, та деякого роду різномірності позбутися не вдасться – зокрема неможливо позбавити систему необхідності бути обізнаною про різномірність апаратного забезпечення з яким працює система (про специфіку взаємодії із приладами кожного типу – їх інтерфейси, протоколи і т.п.). Позбавитись такої різномірності можна лише увівши уніфікацію приладів до єдиного протоколу взаємодії, проте організаційно надзвичайно складно забезпечити використання різними виробниками приладів для Розумних Будинків єдиних уніфікованих інтерфейсів та протоколів, отже задачу позбавитись різномірності цього роду ставити не слід.

Однак, системи управління Розумними Будинками часто також мають різномірність і на усіх інших більш високих рівнях системи, така різномірність породжена різномірністю приладів та породжує паралельні, не уніфіковані шляхи управління цими приладами навіть у користувацьких інтерфейсах, тобто користувач вимушений керувати різними приладами по-різному, інтерфейс користувача відрізнятиметься.

Такого роду різномірності можливо позбутися, якщо ці високі рівні системи взаємодіятимуть з різномірними приладами однаково, тобто таким чином на цих рівнях прилади не будуть здаватися різномірними. Аби досягти на цих рівнях певної уніфікації приладів будь-якого типу до єдиного вигляду можна ввести деяку абстракцію на певному достатньо низькому рівні системи, за якою ховатиметься різномірність приладів.

Той рівень системи, на якому буде введена така абстракція буде обізнаним про різномірність приладів, проте не розкриватиме назовні (для верхніх рівнів системи) деталі цієї різномірності, роблячи для верхніх рівнів системи всі ці

прилади уніфікованими. Введена абстракція має запропонувати певний уніфікований інтерфейс та протокол взаємодії з приладом (Розумною Річчю).

Такий підхід не дозволить позбавитися різноманітності в системі управління Розумним Будинком повністю, проте дозволить викоринити різноманітність на більшості високих рівнів системи, забезпечуючи простоту системи на цих високих рівнях, а також полегшуючи розробку, підтримку й розширення цих рівнів системи.

2.2.2 Шлях пошуку розв'язання проблем безпеки систем управління Розумними Будинками

Слідуючи вимозі до систем управління Розумними Будинками про можливість управління будинком віддалено – через Інтернет, класичною архітектурою системи є наявність всередині будинку фізично деякого комп'ютера – Шлюза. Уся взаємодія користувача з Розумними Речами (приладами) будинку відбувається через цей Шлюз, та цей Шлюз є єдиною сутністю, що безпосередньо взаємодіє з приладами Розумного Будинку. Таку архітектуру обирають через складність та недоцільність забезпечення кожній Розумній Речі самостійного доступу в Інтернет, а також для наявності в системі серйозного обчислювача всередині будинку.

Логічно, що місцем проведення авторизації запитів до Розумного Будинку в системі управління мають виступати саме ці Шлюзи, адже робити це окремо на кожному приладі не доцільно. Це є недоцільним по-перше через надмірну складність (як програмно так і апаратно) цих приладів у такому випадку, що складно, неефективно й дорого, а по-друге через те що Шлюз по суті є єдиною

точкою доступу до будинку зовні через Інтернет. Тому логічно авторизацію проводити саме на рівні Шлюза.

2.2.2.1 Пошук підходів до унеможливлення управління Розумним Будинком без відома користувача

Отже, так як Шлюз доцільно робити єдиним місцем авторизації запитів до Розумного Будинку, і так як Шлюз сам по собі є комп'ютером, що потенційно забезпечує його достатньою обчислювальною потужністю для проведення криптографічних операцій, можна зробити Шлюз базою для забезпечення унеможливлення управління будинком з боку центрального сервера без відома користувача.

Слід спробувати вирішити цю задачу за допомогою асиметричної криптографії та цифрових підписів. Цифрові підписи нададуть змогу посвідчувати автора управляючої команди, що надходить на Шлюз, таким чином Шлюз як контролюючий пункт Розумного Будинку зможе пересвідчуватись, що управляюча команда надходить з довіреного джерела. Такий підхід надасть змогу унеможливити управління будинком користувача навіть з центрального сервера.

2.2.2.2 Пошук рішення для початкового з'єднання прилада з будинком

У процесі початкового підключення будь-якого прилада (Розумної Речі) до будинка за бездротовими протоколами є ризик захоплення управління над приладом з боку зловмисника. У існуючих системах безпека початкового

підключення зазвичай ґрунтується лише на припущенні, що в момент початкового підключенні Розумної Речі до будинку (конкретно Шлюза) поруч не буде зловмисника в активному пошуку приладів. Проте, очевидно цей шлях не є надійним.

Конкретно проблема полягає в тому, що важко побудувати надійну лінію довіри, аби прилад при початковому підключенні міг знати напевне кому з абонентів бездротового протоколу передачі даних навколо довіряти. Тому в момент підключення зловмисник має змогу вдати з себе Шлюз та змусити прилад підключитися до нього та довіряти йому в подальшому. Більше того, зловмисник може при цьому ще й вдати з себе прилад над яким захоплює контроль та під'єднатись до Шлюза, таким чином провівши так звану атаку MITM (Man In The Middle) – Людина посередині, у цьому випадку користувач навіть не помітить, що контроль над його Розумною Річчю був захоплений.

Абсолютно надійним шляхом побудови ліній довіри між Шлюзом та Розумною Річчю під час її початкового підключення є застосування апаратного з'єднання між Шлюзом та приладом у процесі початкового з'єднання (наприклад через дрiт або штекером) – цей процес означатиме, що Шлюз і прилад точно фізично поєднані та що прилад з'єднується за бездротовим протоколом саме з тим абонентом, до якого під'єднаний у цей момент фізично. Проте цей шлях є не економічним, адже вимагає додавання нового апаратного інтерфейсу до кожної Розумної Речі, який буде використовуватись виключно під час початкового з'єднання.

Для побудови надійної лінії довіри між Шлюзом і приладом програмно, без залучення апаратних інтерфейсів, слід зважати на те що фактично обмін даними під час цього процесу фактично проходить через публічні канали передачі даних, тобто слід покладати, що злочинці здатні прочитати всі передані дані. У такому випадку жодні ключі не можна передавати у відкритому вигляді, а також напевне має бути певний ключ, що Шлюз дізнається від Розумної Речі не через канал

передачі даних бездротовим протоколом – бажано фізично писати ключ на Речі, покладаючи що зловмисник не має фізичного доступу до Речі (приладу).

2.2.2.3 Ролі та рівні доступу користувачів до управління Розумним Будинком

Підхід ролей користувачів у системах не є новим, проте його використання в системах управління Розумними Будинками не було помічене. Функціонал ролей передбачає або завчасно задані ролі, кожна з яких має чітко визначений спектр дозволів у системі, та певна роль визначається для кожного користувача, або визначений окремий перелік дозволів для кожного користувача особисто.

Функціонал ролей ефективно та нескладно вирішує деякі потреби користувачів Розумних Будинків, зокрема надає користувачеві можливість дозволити іншому управляти своїм будинком неповністю (наприклад гостю можна дозволити керувати тільки приладами в одній кімнаті, або дитині дозволити керувати всім окрім критичної інфраструктури будинку).

Підхід надання ролей користувачам добре поєднується з підходом авторизації всіх запитів до Розумного Будинку з перевіркою запитів на Шлюзі, бо надання певному користувачеві деяких прав проходитиме через запит до Шлюза.

2.2.3 Шлях дослідження проблем автоматизації та інтелектуалізації

Проблема запровадження інтелектуального помічника, що надавав би рекомендації користувачеві, враховуючи його індивідуальні особливості та

будуючи профіль комфорту користувача полягає в складності реалізації такого інтелекту для будь-яких типів Розумних Речей будинку, без необхідності конфігурувати логіку та шлях навчання інтелекту окремо для кожного типу. Слід створити такий підхід до навчання інтелекту для Розумних Будинків, який не буде необхідності розширювати під кожний новий тип Розумних Речей.

Для досягнення цієї мети слід створити таку процедуру навчання, яка не обізнана про функціональні особливості та характер Розумних Речей. Це частково пов'язано з абстракцією запровадження якої покликане розв'язати проблему різнорідності приладів – інтелект слід навчати на абстрактному уявленні про Розумні Речі не надаючи йому інформації про те які функції ці Розумні Речі виконують.

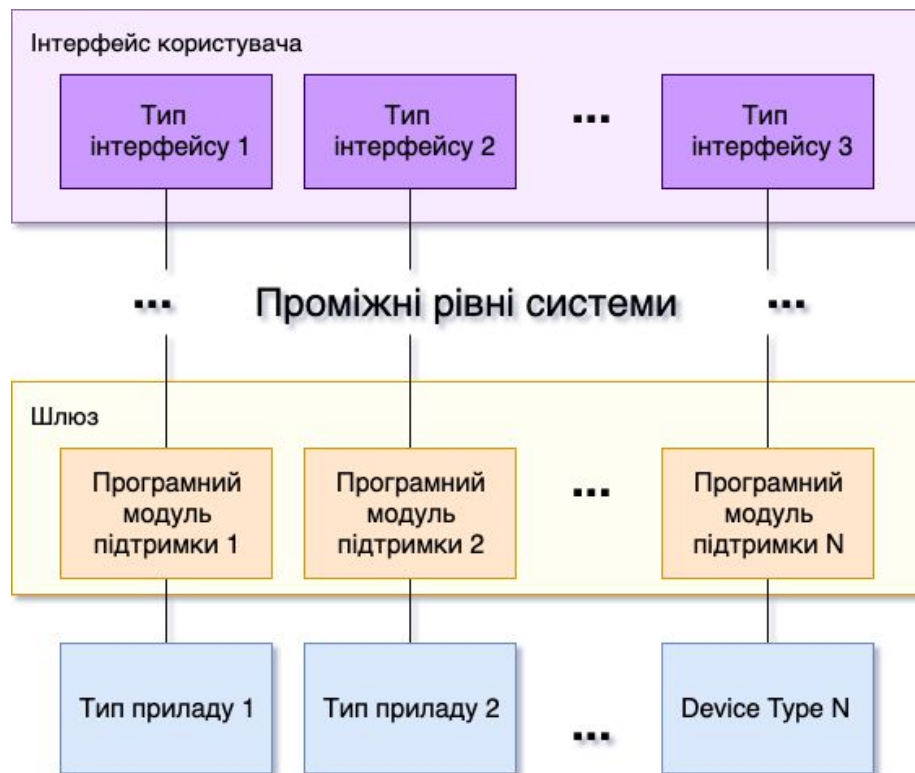
3 РІЗНОРІДНІСТЬ В СИСТЕМАХ УПРАВЛІННЯ РОЗУМНИМИ БУДИНКАМИ

3.1 Проблема різнорідності апаратного забезпечення в управлінні

Більшість підходів в управлінні системами Інтернету Речей використовують свого роду Шлюз, що несе відповідальність за під'єднання до декількох апаратних приладів (включаючи прилади різної структури та прилади від різних виробників) одночасно та за надання єдиної кінцевої точки для управління всіма приладами, які під'єднані до цього Шлюза. Шлюз також уможлиблює взаємодію між приладами Інтернету Речей. Цей підхід зазвичай досягається шляхом додавання на Шлюзі специфічних програмних адаптерів для кожного типу апаратних приладів, що до нього під'єднуються.

Тож Шлюзи зазвичай успішно рятують від необхідності під'єднуватися до декількох приладів одночасно з кінцевого клієнтського приладу користувача для управління цими приладами. Шлюзи беруть цю відповідальність на себе, залишаючи своїм програмним клієнтам єдину точку під'єднання для роботи під час управління декількома приладами.

Однак, проблема різнорідності приладів таким чином станом на зараз повністю не розв'язана. Проблема полягає в тому, що різниці, що існують в структурі різноманітних приладів та в принципах їх взаємодії, змушують потік управління бути різним для цих приладів, що означає що потоки управління цими приладами є паралельними (не мають спільних ділянок). Відсутність уніфікації приладів змушує інтерфейси управління бути різними та мати широку горизонтальну структуру на кожному рівні системи управління Розумними Будинками, з шириною рівною кількості типів різнорідних приладів, що підтримуються системою (Рисунок 2).



«Рисунок 2 – Структура різномірної системи управління»

Така широка структура на кожному рівні спричиняє велику кількість зусиль для додавання нового потоку управління (як наприклад почати управляти новими приладами, якими не управляли в системі до цього), тому що новий модуль має бути доданий до горизонтальної ієрархії на кожному рівні абстракції системи. Це робить процес розробки більш дорогим, а результат більш різномірним, що породжує більше місць для потенційних помилок та робить підтримку системи більш складною. Інша складність широкої горизонтальної ієрархії на кожному рівні - це необхідність оновлювати кожен рівень у системі для того щоб розпочати підтримувати новий тип приладів, це стає особливо складно для оновлення програмного забезпечення на фізичному апаратному забезпеченні, що встановлено в користувачів, а отже не отже недоступне інженерам (таке забезпечення як Шлюзи).

3.1.1 Типи різнорідностей

Існує декілька джерел різнорідності приладів Інтернету речей:

- прилади використовують різні безпроводні протоколи та модулі для комунікації;
- прилади використовують різні особливі високорівневі протоколи та інтерфейси взаємодії;
- прилади призначені для різного і надають різну функціональність, а отже взаємодіють по-різному;

Різниця безпроводних протоколів передачі даних, що використовують прилади ефективно розв'язується використанням Шлюзів, що здатні взаємодіяти з приладами за різними безпроводними протоколами, використовуючи різні програмні та апаратні модулі для різних безпроводних протоколів (таких як Bluetooth, Wi-Fi, ZigBee та тому подібні). Отже різнорідність такого роду може бути просто прихована в Шлюзи без відкриття цих деталей для більш високих рівнів абстракції в системі, так що більш високі рівні не обізнані про цю різнорідність.

Однак, різнорідність програмної структури приладів, їх функціональності та способів їх взаємодії зазвичай не уніфікована, тож Шлюзи зазвичай не можуть абстрагувати високі рівні абстракції в системі від різнорідності Розумних Речей такого роду, залишаючи високі рівні абстракції системи також широкими (горизонтально різноманітними бо мають окремо підтримувати кожен тип) та складними. Отже, високорівневі програмні модулі системи, включаючи інтерфейс користувача, вимушені також бути широкими та різнорідними, підтримуючи усі типи приладів окремо.

3.1.2 Причини різнорідності

Отже є 2 основні причини різнорідності, які сучасні Шлюзи в системах Інтернету Речей не ховають:

- різні виробники використовують різні програмні інтерфейси для взаємодії з їх приладами;
- різні прилади мають різне призначення та функціональність, а отже й різні інтерфейси;

Говорячи про різницю виробників, це важко вирішити та уніфікувати, поки є багато виробників, та ніякий спільний уніфікований стандарт не запропоновано та не застосовано. Уніфікація в цьому випадку – це єдиний шлях, що я організаційною а не технічною проблемою, тому в рамках даного дослідження не розглядається.

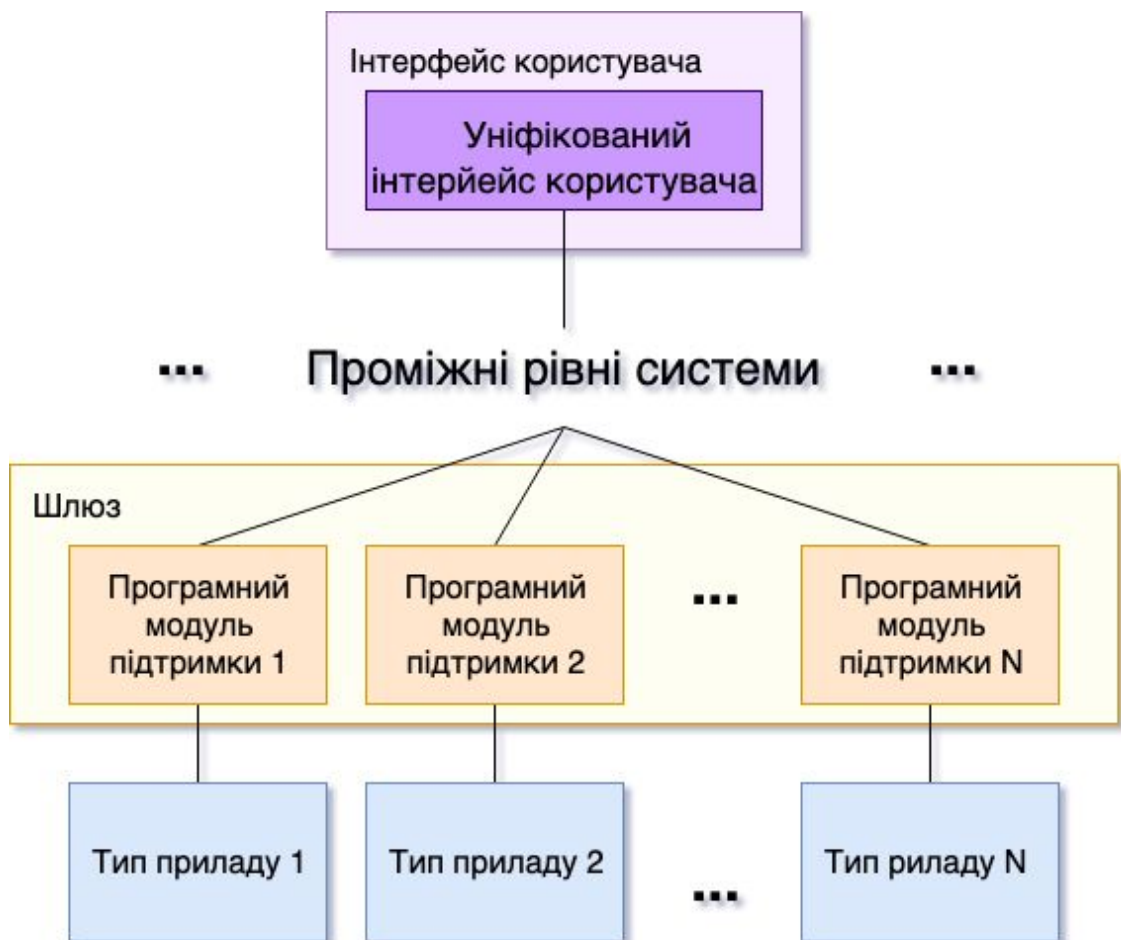
Однак розв'язання різнорідності, що спричинена різноманітністю призначення приладів та їх функціональності, є більш технічною задачею, отже теоретично може бути розв'язана засобами технічних рішень. Функціональність приладів Інтернету Речей в системах Розумних Будинків дійсно сильно різниться – деякі прилади є сенсорами та дозволяють лише зчитування даних з себе, деякі прилади дозволяють тільки запис даних в себе та деякі з них комбінують атрибути для читання та запису. Це дослідження зокрема пропонує розв'язок для цієї конкретної різнорідності, пропнуючи підхід для абстракції для управління приладами Інтернету Речей, що дозволяє уніфікувати високорівневі програмні інтерфейси приладів до єдиного інтерфейсу. Так інтерфейс будь-якого можливого існуючого пристрою міг би бути адаптованим до цього уніфікованого абстрактного інтерфейсу без втрати функціональності управління приладом.

3.2 Розв'язок проблеми різнорідності

Неможливо уникнути широкої горизонтальної структури на Шлюзі повністю, поки різнорідність приладів повністю не зникла, що не очікується в найближчому майбутньому. Однак, широка горизонтальна структура може бути прихована в Шлюзі та єдиний уніфікований програмний інтерфейс взаємодії з приладами може бути розкритий назовні Шлюза.

Для того щоб надати змогу вищим рівням системи (над Шлюзом) ставитися та обробляти управління приладами в уніфікований спосіб, має бути запропонована абстракція, що покриває все можливе різноманіття різнорідних приладів. Абстракція має покрити не тільки існуючі на даний момент типи приладів, але будь-які можливі прилади, що можуть з'явитися в майбутньому. Так щоби абстракція не потребувала будь-яких змін та адаптери від інтерфейсів специфічних приладів до абстракції могли залишатися незмінними.

Це дозволить вищим рівням системи комунікувати з приладами через цю абстракцію, приховуючи деталі різнорідності та інтерфейси певних приладів всередині Шлюза. Система управління має абстрагувати (відокремити) високі рівні системи управління приладами від деталей інтерфейсів приладів, так щоб програмне забезпечення на вищих рівнях системи управління залишалось уніфікованих для приладів всіх типів, доступних функціональностей та виробників. Перш за все цінність такої абстракції в усуненні необхідності робити будь-які зміни в високорівневих частинах системи коли якийсь нове апаратне забезпечення (Розумні Речі) додається до системи. Також абстракція що покриває всі прилади допоможе виконати це розділення та знизити зв'язність між вищими та нижчими рівнями системи, аби комунікація між рівнями відбувалась через цю абстракцію. Схему системи з такою абстракцією наведено на Рисунку 3.



«Рисунок 3 – Структура системи управління з абстракцією»

Для того щоб побудувати уніфіковану абстракцію для всіх типів приладів Інтернету Речей, побудуємо математичну модель приладу (Розумної Речі) в загальному вигляді. Під Розумною Річчю розумітимемо Абстрактну Річ, що є об'єднанням всіх можливих Розумних Речей (існуючих зараз та таких що може бути створені у майбутньому) – така Річ всі можливі атрибути всіх можливих Речей.

Для того щоб описати таку Абстрактну Річ, дослідимо всі можливі обміни даними які Річ потенційно може проводити під час усього свого життєвого циклу під час комунікації, а також структуру всіх Речей, що існують зараз та потенційно можуть існувати.

3.2.1 Ініціювання взаємодії Шлюз-Річ

Так як ми будемо абстракцію для інтерфейсу взаємодії(комунікації) з приладом, перш за все нам необхідно визначити усі можливі потоки даних між Шлюзом та Річчю та ініціаторів усіх передач даних. В запропонованій архітектурі Шлюз – це єдина сутність з якою взаємодіє Річ. Тож обидва Шлюз та Річ можуть бути ініціаторами передачі даних, таким чином:

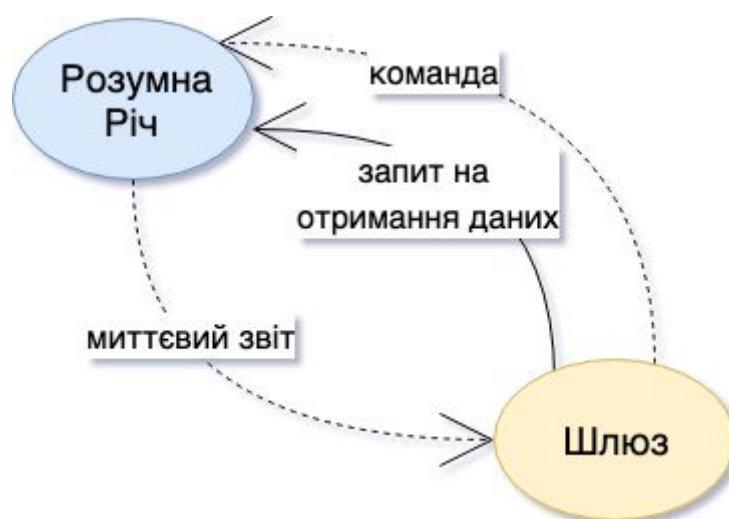
а) Шлюз ініціює комунікацію виключно з двох причин:

- 1) запит даних від Речі (наприклад дані з сенсорів) – зчитати з Речі (обов'язково для Речі);
- 2) змусити Річ змінити якесь значення чи виконати якусь дію (наприклад увімкнути лампу) – записати в Річ (опціонально);

б) Річ ініціює комунікацію виключно з метою:

- 1) сповістити про Подію що сталася(наприклад відкрилися двері або змінилось значення певного сенсора) (опціонально).

Ці 3 способи ініціювання взаємодії відображені на Рисунку 4.



«Рисунок 4 – Ініціювання взаємодії між Річчю та Шлюзом»

Ми покладаємо, що немає ніяких інших шляхів комунікації між Річчю та Шлюзом та ніколи не може бути запропоновано, тож комунікація що описана вище покриває всі потенційні способи використання комунікації з Розумною Річчю.

Такий підхід також покриває Речі з безперервним потоком даних (наприклад камери/мікрофони – постачальники та дисплеї/динаміки – споживачі), для Речей що є постачальниками даних потік даних є потоком миттєвих звітів, у той час як для споживачів даних потік даних це потік команд.

Шлюзові не знадобляться ніякі інші засоби комунікації з Розумними Речами окрім як зчитувати(отримувати) дані Речі або записувати(управляти) в Річ. Речі також ніколи не знадобиться ніякі інші засоби комунікації ініційованих Річчю окрім як відправлення даних – миттєві звіти. У цій архітектурі Річ – це свого роду slave(ведений), у той час як Шлюз це master(ведучий), отже ми не очікуємо від Речі відправки будь-яких команд управління чи запитів на зчитування будь-яких даних зі Шлюзу, отже цих описаних шляхів комунікації буде достатньо, бо ніякі інші способи ініціювання передачі даних в принципі неможливі. Таким чином, описані на Рисунку 4 взаємодії Шлюза з Розумною Річчю є вичерпним переліком потенційних взаємодій.

3.2.2. Параметр як неподільна складова структури Речі

Будь-яка Річ може бути розділена на набір неподільних значень, називатимемо такі неподільні значення Параметрами. Наприклад спільний сенсор температури та вологості має рівно 2 значення – температура та вологість, отже це є Параметри цієї Речі-сенсора. Дійсно будь-яка Річ може бути розділена на кінцеву кількість неподільних значень.

Можливими типами даних значень Параметру є:

- бінарний (true/false);
- число (ціле або дробове);
- масив чисел (може використовуватись для файлів, зображень, або кадрів відео);
- рядок.

Не існує ніякого іншого простого типу даних, тож цих можливих типів має бути достатньо для Параметрів. Нам не потрібні складні вкладені рекурсивні Параметри (які складаються з інших параметрів), бо будь-які вкладені структури можна представити як плоскі структури без будь-якої втрати функціональності чи можливостей для взаємодії. У якості виняткового випадку, якщо фізичний прилад має декілька логічних груп значень-Параметрів та ці групи є логічно пов'язаними одне з одними – цей фізичний прилад можна представити як декілька Речей (по Речі на кожен логічно пов'язану групу значень).

3.2.3. Формулювання абстракції Розумної Речі

Спираючись на ті дані, що будуть передаватися між Шлюзом та Розумною Річчю (функціональна схема Розумної Речі) та Параметр-складову Речі (структурна схема Розумної Речі), буде сформована абстракція для Речі, що покриє всі можливі структурні та поведінкові типи й різновиди Розумної Речі. Отже, буде сформована структура Речі – це набір Параметрів, кожен з унікальним ідентифікатором. Структура Параметра в свою чергу має описувати всі потенційні дії, що Параметр можуть бути виконані над параметром – структура певного Параметра має давати повне розуміння всіх можливих шляхів взаємодії з Параметром.

Приклад структури Параметру описаний в наступному JSON об'єкті:

```
{
  "title": "switch",
  "type": "bool",
  "min_value": 0,
  "max_value": 1,
  "is_settable": true,
  "is_firable": false
}
```

Кожен Параметр повинен мати наступні поля:

- ім'я Параметра;
- тип даних;
- мінімальне значення;
- максимальне значення;
- чи може це значення бути задане;
- чи може значення бути вистрілене (чи може виробляти миттєві звіти про Події, як наприклад відкриття дверей).

Така структура Параметра цілком опише Параметр згідно зі сформованою раніше абстракцією та уможливить будь-яку комунікацію з Параметром (через Річ у якій він знаходиться) згідно з абстракцією. Така структура дозволить розуміти які дані можливо зчитати чи записати в Параметр. А також атрибути “is_settable” та “is_firable” (чи може значення бути задане та вистрілене) дозволять Шлюзу розуміти які способи взаємодії дозволені для цього Параметра.

Тож запропонована структура Речі, що складається з Параметрів описаної вище структури дає повний структурний та функціональний опис Розумної Речі згідно з абстракцією.

3.3. Шлюз та взаємодія Розумної Речі зі Шлюзом

Отже, спираючись на абстракцію, що описана вище, сформулюємо процеси які мають відбуватися в Шлюзі системи управління Розумним Будинком, що взаємодіє з Розумними Речами за цією абстракцією, а також опишемо взаємодію Шлюза з Розумними Речами.

3.3.1 Відповідальності Шлюза

Шлюз є єдиною точкою доступу до Розумного Будинку, уся внутрішня структура мережі Розумних Речей у Розумному Будинку має бути відома лише Шлюзу, зовнішній споживач програмного інтерфейсу який надає Шлюз має бути обізнаний лише про перелік Розумних Речей будинку та можливі способи взаємодії з цими Речами (перелік та структуру всіх Параметрів кожної Речі). Отже Шлюз є єдиною сутністю, з якою взаємодіє Розумна Річ всередині будинку протягом усього життєвого циклу Речі. Цей життєвий цикл має складатися зі стартового підключення Розумної Речі, тимчасових відключень і підключень Речі до Шлюза, штатного режиму роботи Речі (надання даних та миттєвих звітів на Шлюз та прийому управляючих команд від Шлюза), а також відключення Розумної Речі від будинку.

Виведемо перелік відповідальностей Шлюза, спираючись на цей життєвий цикл, адже Шлюз у архітектурі системи управління Розумним Будинком що буде запропонована, не виконує інших функцій окрім об'єднання в єдину точку доступу декількох Розумних Речей та взаємодії з Речами продовж їх життєвого циклу.

Відповідальності покладені на Шлюз:

- початкове сполучення з Розумною Річчю;
- надсилання управляючих команд на Річ за запросом або за завчасно заданим сценарієм;
- зчитування й відправка на центральний сервер даних з Речі за запросом або по періоду;
- надання авторизованого програмного інтерфейсу для надсилання запитів з приводу Речей (забезпечення авторизації запитів).

3.3.2 Потік управління через Шлюз

Так як специфічна реалізація взаємодії із кожною окремою Річчю відома лише Шлюзові, управління Речами на всіх рівнях системи які знаходяться над Шлюзом має відбуватись виключно через запропоновану абстракцію Розумної Речі. Споживачі програмного інтерфейсу Шлюза знають перелік Розумних Речей будинку та їх структуру з функціональними можливостями згідно абстракції. Отже управляючі запити користувачів (або глобального сервера безпосередньо), де б не були створені, в кінці неминуче досягають Шлюза, де запити стосуються певних (одного або декількох) Параметрів Речі в абстрактному вигляді (через запропоновану абстракцію). Наприклад запит може включати освітлення, або просити надіслати дані датчика температури. Такий запит специфікує якої Речі та її Параметру запит стосується, вказуючи їх ідентифікатори, а також що саме необхідно зробити (зчитати чи задати значення, та яке власне це значення в другому варіанті).

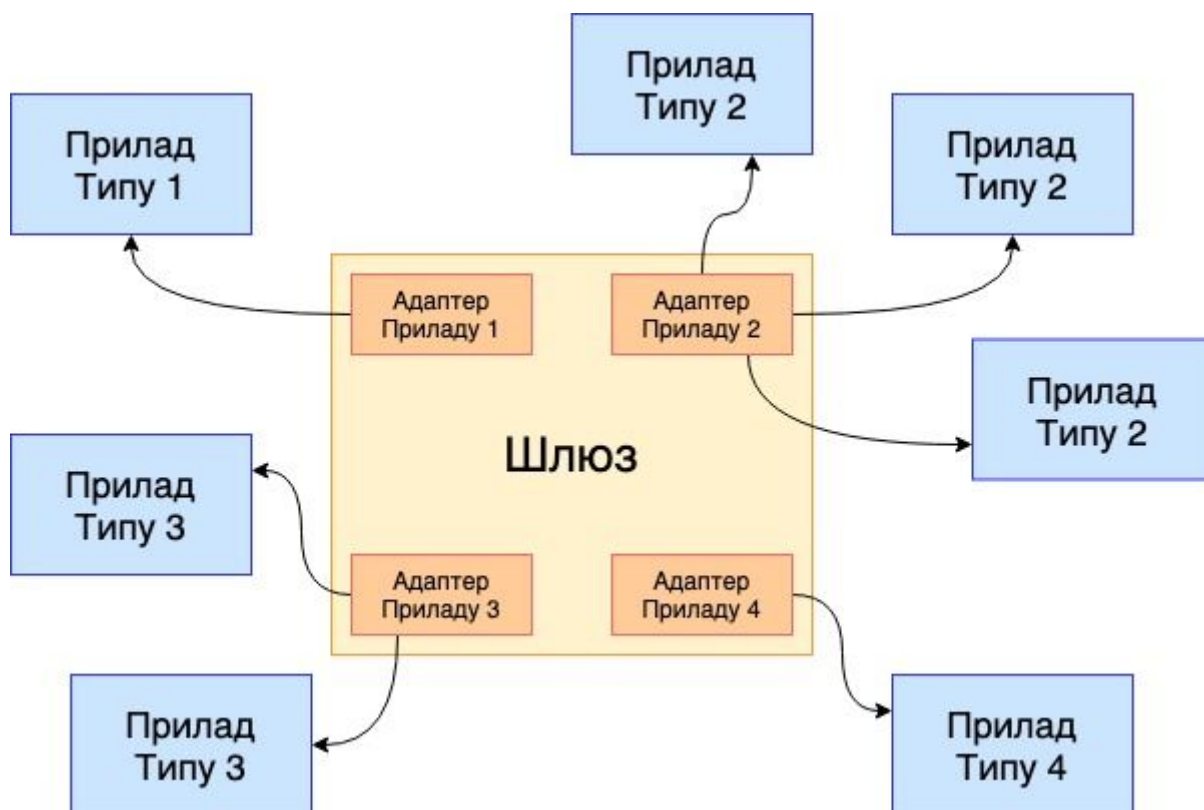
3.3.3. Програмні адаптери на Шлюзі

Шлюз отримує управляючі команди щодо певних Параметрів в абстрактному вигляді, після чого повинен донести команду до Речі. Для того щоб це було можливо, програмне забезпечення на Шлюзі має забезпечувати реалізації певного інтерфейса окремі для кожного типу Розумних Речей. Цей інтерфейс має описувати всі можливі дії над Речами, запити на які надходять в управляючих командах на Шлюз.

Цей інтерфейс у псевдокодi може виглядати наприклад наступним чином:

```
interface Thing {
    func GetCurrentValue (parameterID)
    func SetValue (parameterID, value)
    func RegisterListener (parameterId, listener) // для
миттєвих звітів (наприклад відкрилися двері)
}
```

А під кожного виробника Розумних Речей в Шлюзі необхідне існування програмної реалізації цього інтерфейсу – адаптера. І тільки ця реалізація всередині Шлюза буде обізнана про деталі комунікації між Шлюзом та Розумною Річчю цього виробника. Реалізація(адаптер) буде імплементувати функції задані в інтерфейсі, використовуючи певні бездротові протоколи передачі даних для взаємодії з Розумними Речами та певні програмні інтерфейси й протоколи взаємодії з приладами Розумних Речей задані виробниками Розумних Речей. Таким чином деталі взаємодії Шлюзу з Речами будуть приховані виключно в цих реалізаціях(адаптерах). Програмна структура Шлюза з адаптерами зображена на Рисунку 5.



«Рисунок 5 – Програмні адаптери Шлюза»

Саме створення чергової реалізації цього інтерфейсу (нового адаптеру) – це єдине що необхідно додати в програмному забезпеченні Шлюза аби додати підтримку нових Розумних Речей від нового виробника в системі управління Розумного Будинку. Тобто розширення системи новими виробниками Розумних Речей що підтримуються полягатиме тільки в створенні чергової реалізації цього інтерфейсу.

4 БЕЗПЕКА СИСТЕМ УПРАВЛІННЯ РОЗУМНИМИ БУДИНКАМИ

4.1 Авторизація запитів до Розумного Будинку

4.1.1 Команда з адресантом як засіб управління

На шляху уможливлення управління Розумними Речами через Шлюз із різних джерел-суб'єктів управління слід враховувати необхідність сприймання Шлюзом управляючих команд від різних сутностей – безпосередньо користувача, центрального сервера від імені користувача в реалізації сценаріїв тощо. Таким чином, впровадивши в публічний інтерфейс Шлюза управління в вигляді команд, що мають відправителя та авторизуються цим відправителем, можна забезпечити гнучкість управління та незалежність Шлюза від джерел управляючих команд що до нього надходять.

Такий підхід зокрема цікавий і з точки зору безпеки системи управління Розумним Будинком, тому що підхід дозволяє забезпечити неможливість центрального сервера без відома користувача управляти його Будинком (у випадку якщо дозвіл не був наданий явно з метою наприклад забезпечення автоматизації) – через криптографічні підписи управляючих команд що йдуть на Шлюз. Після цього можна забезпечити механізм добровільної передачі користувачем права на управління будинком іншим користувачам а також центральному серверу (для запровадження автоматизованого управління, наприклад через сценарії). Підхід управління через команди з адресантом та криптографічною авторизацією дозволить реалізувати всі описані вище потенційні способи управління системою та забезпечить необхідну гнучкість управління – дозволить ефективно авторизовувати управляючі команди та гнучко передавати контроль над будинком іншим сутностям.

4.1.2 Авторизація управляючих команд на Шлюзі

Основна ідея криптографічної авторизації управляючих команд, що приходять на Шлюз полягає в застосуванні асиметричної криптографії для підписування цифровими підписами кожної команди яка йде до Розумного Будинку. У відповідальність Шлюза входить перевірка цих підписів, і так як Шлюз апаратно реалізований як повноцінний комп'ютер – його обчислювальної потужності має вистачити для операцій перевірки цифрових підписів асиметричного шифрування.

Ідея асиметричної криптографії полягає в тому, що в двох абонентів різні ключі – приватний та публічний, при чому з приватного можна отримати публічний, а з публічного неможливо отримати приватний. При використанні асиметричної криптографії, приватний ключ використовують для підписання певних даних, утворюючи блок даних – підпис, а публічний ключ використовують для достовірної перевірки підпису – того що цей підпис був утворений при підписанні саме певного блоку даних приватним ключем, що відповідає публічному ключу.

4.1.2.1 Управління ключами авторизації

Очевидно, що є потреба в тому, щоб одним Розумним Будинком мали змогу керувати декілька сутностей (користувачі, центральний сервер для автоматизації, і т.п.). Також очевидно, що кожна з цих сутностей повинна надсилати на Шлюз управляючі команди самостійно та використовуючи свій власний окремий ключ для цього. Логічно, що в такому випадку, на Шлюзі має бути декілька ключів,

яким довіряє Шлюз – тобто Шлюз має авторизувати команди підписані будь-яким з ключів, до яких в нього є довіра. З початку Шлюз повинен мати один або декілька початкових ключів, до яких Шлюз матиме довіру, та які матимуть змогу надсилати Шлюзові команди про додавання інших ключів, яким Шлюз теж повинен буде довіряти.

При такому підході процедура додавання нових ключів для довіри Шлюзу та навіть заміна існуючих початкових ключів технічно не є великою проблемою – необхідно буде просто надсилати на Шлюз команду певного виду, що робитиме на Шлюзі запит на додавання нового ключа (з указанням його повноважень), або заміну одного існуючого ключа іншим новим відповідно. Проте технічно цікавою є проблема довіри Шлюза до початкових ключів – необхідно забезпечити надійність передачі на Шлюз початкових ключів, слід побудувати цей шлях таким чином, щоб унеможливити злочинну атаку впродовж цього процесу, що підмінить справжній ключ власним, або додасть власний злочинний ключ до списку початкових довірених ключів.

4.1.2.2 Довіра Шлюза до початкових ключів

Для забезпечення довіри до найперших (корінних) ключів для підписання управляючих команд слід передати ці ключі на Шлюз не тим же шляхом, яким на Шлюз надходять команди. Так як ми криптографічно підписуємо команди – то довіри до середовища передачі даних, яким передаються ці команди немає, отже початкові ключі не можуть бути передані через це середовище. Більше того, середовище яким слід передати початкові ключі повинне бути довіреним і надійним. Так як необхідне надійне середовище передачі даних, це не може бути передача даних через глобальну мережу.

Виходячи зі сформованих вище вимог до середовища передачі даних для передачі початкових ключів на Шлюз, можна прийти до висновку, що ця передача має пройти через якийсь локальний канал передачі даних – або напряму дротовим з'єднанням зі Шлюзом, або через локальну мережу. Найбільш простим для користувача способом цю передачу можна провести через локальну мережу, у якій буде Шлюз та прилад користувача. Для додаткової довіри Шлюза можна при цьому використовувати секрет, написаний фізично на Шлюзі, правильне вказання користувачем цього секрету означатиме, що користувач фізично знаходиться поруч зі Шлюзом. Для того щоб не змушувати користувача вводити ключі для Шлюза вручну, можна використовувати певний сервер з ключами, який зберігатиме ключі, а достовірність ключів отриманих з цього сервера можна перевіряти симетричним паролем, який Шлюзові сповістить користувач під час занесення в Шлюз початкових ключів.

Таким чином, Шлюз зможе бути впевненим в достовірності початкових ключів які йому предані, та матиме довіру до них.

4.1.2.3 Недоліки криптографічної авторизації команд

Важливо зазначити, що підхід криптографічних підписів для авторизації управляючих команд Розумного Будинку має певні недоліки, зокрема непростою проблемою є втрата користувачем приватного ключа для підписання команд. Втрата ключа є небезпечною, бо призводить до втрати контролю користувачем над своїм будинком, що означатиме для користувача необхідність робити перезавантаження Шлюза фізично в будинку та налаштування будинку з нуля.

Проте як і з аналогічними проблемами в інших системах де присутній цифровий підпис на основі асиметричної криптографії, цю проблему можна

вирішити шляхом надання користувачу додаткових запасних ключів, які він зберігає окремо, бажано офлайн.

4.2 Забезпечення безпеки початкового з'єднання Розумної Речі зі Шлюзом Розумного Будинку

Безпекова проблема початкового з'єднання Розумної Речі зі Шлюзом полягає в ризику захоплення контролю над Розумною Річчю зловмисником. Річ сполучається зі Шлюзом за певним бездротовим протоколом передачі даних у відкритому, а отже незахищеному, просторі. З цієї причини дані по мережі під час початкового сполучення Розумної Речі та Шлюза не можна передавати у відкритому вигляді, а також необхідно забезпечити надійні засоби довіри в Розумній Речі до Шлюза. Під час їх початкового сполучення необхідно створити умови на стороні Розумної Речі, що надасть Речі можливість пересвідчитись у тому, що з'єднання проходить саме зі Шлюзом Розумного Будинку, а не що це є атакою зловмисника.

Логічним рішенням цієї технічної проблеми є використання Шлюзом певного секретного ключа при початковому запиті до Розумної Речі, який завчасно відомий Розумній Речі та був переданий на Шлюз певним каналом передачі даних, який не є основним каналом передачі даних між Шлюзом та Річчю та точно є захищеним від перехоплення даних зловмисниками. Надійним каналом для передачі секретного ключа від Речі до Шлюза точно не може бути якийсь бездротовий канал передачі даних, бо умови задачі передбачають початкове сполучення Речі з Будинком в умовах повного прослуховування будь-ким будь-якого радіохвильного каналу для передачі даних, тобто середовище передачі даних слід вважати повністю публічним.

З такими обмеженнями є тільки два способи передати дані секрету:

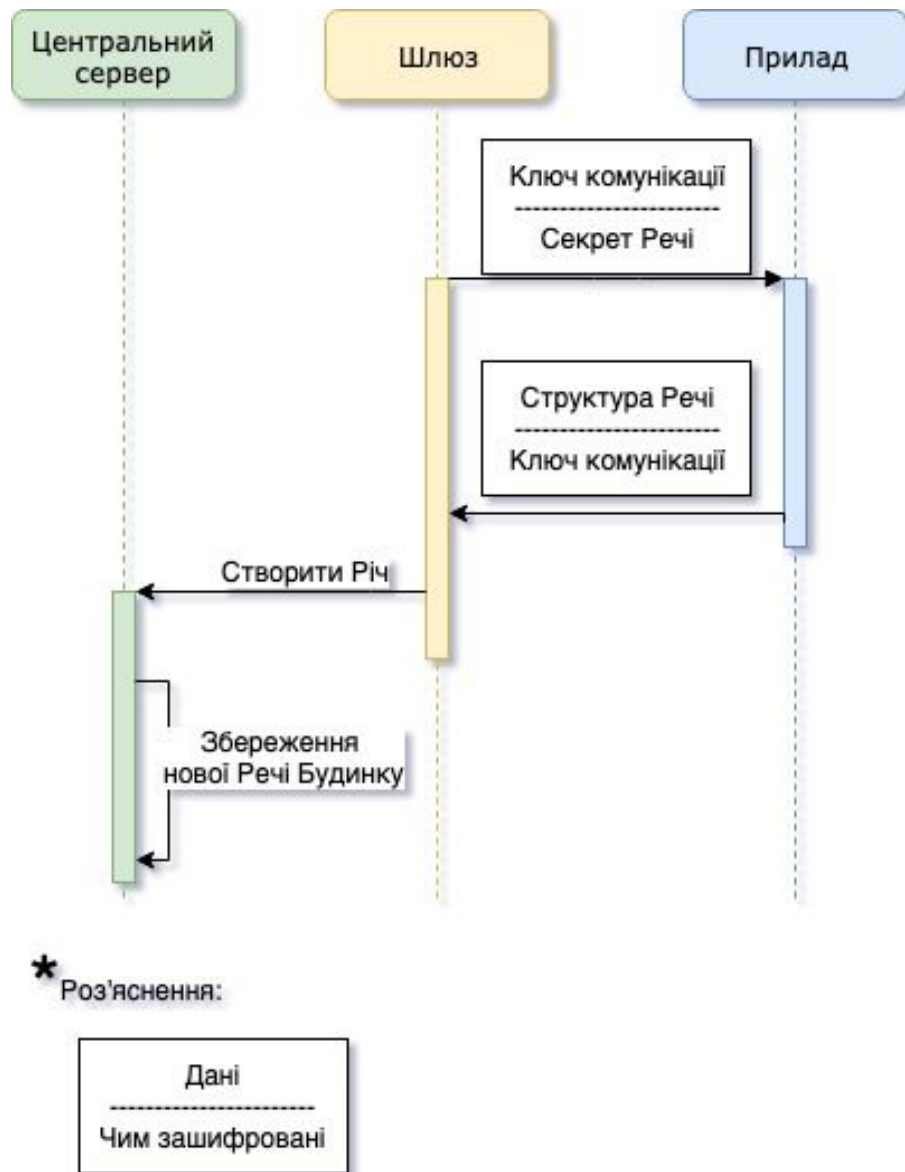
- апаратне фізичне з'єднання Розумної Речі зі Шлюзом (по дротах, або через спеціальний апаратний інтерфейс);
- користувач вводитиме певні дані в Шлюз, які він фізично офлайн прочитає (наприклад на корпусі Розумної Речі).

Розумна Річ в цілому не потребує будь-яких апаратних інтерфейсів окрім як для початкового сполучення, тож слід спробувати вирішити цю технічну проблему без залучення додаткових апаратних інтерфейсів, встановлення яких необґрунтовано збільшуватиме ціни прилада.

Отже обрано шлях, у якому користувач фізично офлайн сприймає певні дані (секрет), які передає Шлюзу через інтерфейс Шлюза по захищеному каналу. Після цього Шлюз повинен сповістити цей секрет Речі для того щоб авторизуватись та отримати довіру Речі. Так як канал передачі даних Шлюз-Річ є відкритим, передавати секрет у відкритому вигляді недопустимо. Теоретично можливо зробити секрет Розумної Речі динамічним, проте в такому випадку існує складність для Речі фізично відобразити свій секрет – наприклад знадобиться встановлення дисплею на Розумну Річ, що також є економічно недоцільним рішенням, тому покладемо що секрет є статичним для всіх підключень Речі.

Отже Шлюзові треба знайти спосіб запевнити Розумну Річ у тому що йому відомий секрет, проте не передавати цей секрет каналом передачі даних у відкритому вигляді. Аби цього досягти, слід симетрично зашифрувати цим секретом дані в найпершому повідомленні від Шлюза до Речі. Більше того, усі наступні повідомлення каналом передачі даних теж слід шифрувати, проте для цього має використовуватись інший ключ (або ключі).

Зважаючи на всі ці описані вимоги, пропоную протокол початкового сполучення Розумної Речі зі Шлюзом, який виконає поставлені вимоги та забезпечить необхідний рівень безпеки передачі даних. Протокол описано в діаграмі послідовності на Рисунку 6.



«Рисунок 6 – Діаграма послідовності початкового сполучення Розумної Речі»

На діаграмі Шлюз виконує початкове сполучення з Розумною Річчю, та після успіху сполучення, надсилає на Центральний Сервер запит про додавання нової Розумної Речі. Стрілки на діаграмі послідовності що супроводжуються прямокутником з двома половинками, розділеними горизонтально, передбачають передачу певного блоку даних зашифрованих певним ключем (зображено в роз'ясненні внизу діаграми).

Розумна Річ приймає перше початкове повідомлення та розшифровує отримані дані симетричним ключем, який жорстко в неї закодований та очікує

побачити повідомлення певної структури. Якщо структура розшифрованого повідомлення співпадає зі структурою, що очікується, авторизація Шлюза успішно проведена, та можна сполучатися із цим абонентом. Початкове повідомлення несе в собі ключ симетричного шифрування, що має використовуватись для подальшої комунікації. У відповідь на перше повідомлення Шлюза Розумні Річ повинна надіслати повідомлення, що несе в собі опис структури цієї Розумної Речі, щоби Шлюз розумів яка взаємодія з цією Річчю можлива та за яким протоколом.

Для додаткової безпеки та надійності під час подальшого спілкування Шлюз-Річ можна використовувати різні ключі шифрування – змінювати їх кожне наступне повідомлення, або кожні N повідомлень. Реалізація таких динамічних ключей не є складною технічною проблемою – просто слід надсилати нові ключі шифрування в повідомленнях комунікації та перевіряти, що адресат успішно отримав новий ключ та готовий працювати використовуючи його.

Слід використовувати саме симетричні ключі шифрування через те, що обчислювач Розумних Речей може бути не дуже потужним – Розумні Речі повинні використовувати мікроконтролер, а не комп'ютер у якості обчислювача.

5 ПРОФІЛІ КОМФОРТУ КОРИСТУВАЧІВ РОЗУМНИХ БУДИНКІВ

Гарною основою для застосування штучного інтелекту та індивідуального підстроювання Розумного Будинку під конкретного користувача є описані вище підходи до побудови архітектури системи управління Розумними Будинками та до використання управляючих команд з адресантом та авторизацію в процесі управління будинком. Інтелектуалізація та створення профілів комфорту користувачів зокрема має на увазі автоматичне надсилання управляючих команд Розумному Будинкові від імені Центрального Сервера відповідно до тих повноважень в рамках яких користувач дозволить Центральному Серверу автоматизувати певні дії в будинку, самостійно приймаючи рішення про надсилання певних команд. Авторизовані команди з адресантом є гнучким і зручним інструментом у цьому процесі, адже дозволяють безпечно керувати Розумним Будинком користувача, а користувачеві обмежувати чим саме інтелект може керувати.

5.1 Способи використання інтелектуальної автоматизації Розумного Будинку

Користувач Розумного Будинку схильний повторювати певні поведінкові патерни та робити однакові дії в певних умовах. Наприклад, включати світло повертаючись ввечері додому, або включати світло коли стає темно, вмикати опалення, коли стає холодніше певної температури комфорту тощо. В цілому багато з дій які користувач схильний робити в Своєму Розумному будинку залежать напряду від певних конкретних параметрів у момент часу. Наприклад

вмикання світла залежить від рівня освітленості, а вмикання опалення – від температури. Отже, так як зазвичай дії користувача напряму залежать від певних параметрів, ці дії можна передбачити, знаючи ці параметри.

Отже, дії користувача, що можливо передбачити, можна програмно передбачати та пропонувати користувачеві виконати їх, або виконувати їх автоматично замість користувача, надаючи таким чином користувачеві додаткову зручність управління Розумним Будинком.

Очевидно, що поведінка кожного окремого користувача в Розумному Будинку може сильно відрізнятися, тобто є суто індивідуальною, а отже й автоматизація яка має бути запропонована кожному окремому користувачу має відрізнятися, тобто бути індивідуальною для кожного користувача.

5.2 Використання профілів комфорту як основа пропозицій по управлінню Розумним Будинком

Кожен користувач має свій особистий індивідуальний певний профіль комфорту, адже комфорт для кожної людини є різним. Проте цей профіль є відносно статичним, тобто в різні моменти часу він не дуже відрізняється, бо зазвичай користувачеві комфортно при одних і тих же умовах. І саме ці умови, що є комфортними для користувача, він прагне створити у себе в будинку.

Аби робити користувачеві пропозиції по автоматизації певних його рутинних дій у будинку, система має розуміти профіль комфорту користувача, тобто бути обізнаною про конкретні умови, які користувач скоріш за все вважає в своєму будинку комфортними. Отже, система має будувати та оновлювати, підтримуючи в актуальному стані, профіль комфорту користувача.

Спостерігаючи за діями, які користувач робить у себе в будинку, певний штучний інтелект системи управління Розумним Будинком повинен будувати та підтримувати в себе профіль комфорту користувача, який допоможе штучному інтелекту повторювати поведінку користувача та певні його поведінкові патерни в будинку автоматично.

Наприклад, запам'ятавши в який час чи за яких умов користувач робить ті чи інші дії в будинку – система може пропонувати виконати їх самостійно, передбачаючи наступні дії користувача в Розумному Будинку завчасно. Зафіксувавши що користувач вмикає світло в кімнаті в певний час доби, або після відкриття дверей кімнати або будинку, або при певних значеннях рівня освітленості в кімнаті, система може пропонувати користувачеві увімкнути світло автоматично, коли умови за яких користувач вмикає світло повторяться знову.

5.3 Забезпечення позитивного досвіду користувача під час впровадження автоматичного керування будинком

Запровадження автоматичного управління Розумним Будинком користувача тягне за собою певні властивості, які багатьма користувачами можуть сприйматись негативно. Отже важливим аспектом при запровадженні автоматичного керування Розумним Будинком є ретельна розробка підходів, спрямованих на забезпечення позитивного досвіду використання системи управління Розумним Будинком користувачем. Слід ретельно продумати шляхи нівелювання негативного досвіду користувача системи.

Зокрема користувачі наприклад можуть негативно сприймати недостатній рівень безпеки в системі, відсутність повного контролю користувача над тим що відбувається в системі та Розумному Будинку, а також надмірну нав'язливість у

спілкуванні інтелекту Розумного Будинку з користувачем через повідомлення чи нотифікації.

Можна виділити наступні негативні для досвіду використання аспекти запровадження автоматичного інтелектуального керування Розумним Будинком:

- контроль певною сутністю над будинком користувача;
- занадто широкі повноваження та спектр приладів якими може керувати штучний інтелект;
- можливість критичних приладів інфраструктури змінити свій стан внаслідок дій, що не залежать від користувача;
- нав'язливість пропозицій по автоматичному управлінню;
- недоречні управляючі команди автоматично подані на Розумний Будинок;
- недостатній контроль користувача над логікою поведінки штучного інтелекту Розумного Будинку.

Розглянемо можливі підходи при запровадженні інтелектуальної автоматизації управління Розумним Будинком, що покликані нівелювати описані вище аспекти.

5.3.1 Перехід від пропозицій до повного автоматичного виконання

Аби досвід користувача не був невдалим, слід перші автоматичні дії в Розумному Будинку робити тільки в вигляді пропозицій користувачеві, які той особисто вручну схвалюватиме чи відхилятиме. Таким чином, користувач на перших етапах, коли він ще особливо невпевнений в ефективності штучного інтелекту, не відчуватиме незручності від того, що його будинок управляється сторонньою сутністю.

Також аби створити приємний досвід використання, кожний користувач повинен мати змогу обрати персональний рівень нав'язливості повідомлень із пропозиціями (запитами його підтвердження на виконання дій) – як часто отримувати пропозиції по виконанню якихось дій.

Тільки після певного етапу роботи в режимі “з підтвердженнями”, коли користувач особисто підтверджує всі пропозиції штучного інтелекту в Розумному Будинку, слід запропонувати користувачу надати штучному інтелекту дозвіл працювати в повністю автоматичному режимі. Однак це не означає, що якісь пропозиції нового плану, що ще не були схвалені користувачем вручну або пропозиції щодо яких інтелект не має повної впевненості, не можуть бути додатково надіслані користувачеві на ручне схвалення. Як показчик того, що можна переходити на повністю автоматичний режим, щодо тих дій, які користувач вже неодноразово схвалював вручну, може бути факт того, що декілька разів під ряд користувач схвалював пропозиції надані штучним інтелектом.

5.3.2 Безпека при управлінні Розумним Будинком засобами штучного інтелекту

Вирішуючи проблему негативного досвіду використання користувача з приводу того, що контроль над його будинком має певна стороння сутність, можна запропонувати імплементувати опцію обмеження доступу до управління Розумним Будинком для штучного інтелекту. Можливо реалізувати надання інтелекту доступу тільки до певних Розумних Речей в будинку, або ввести певні інші обмеження. Таким чином, користувач буде впевнений, що штучний інтелект

управлятиме в будинку тільки тими приладами, доступ до управління якими інтелекту було надано.

Для технічної реалізації лімітованого доступу штучного інтелекту до управління Розумним Будинком слід імплементувати команди спеціального типу, що передаватимуть управління будинком, чітко зазначаючи якими саме приладами та в якій мірі надається доступ на управління.

Також, якщо рівень стурбованості з приводу передачі управління в користувача ще вищий, слід запровадити функціонал, що не передбачає контролю над управлінням будинком у штучного інтелекта. Натомість інтелект може тільки пропонувати певні дії в будинку, а користувач підтверджуватиме їх. При цьому фактично саму дію в будинку виконуватиме саме користувач, а інтелект доступу до управління не матиме.

Ще однією проблемою автоматизованого управління Розумним Будинком є низький рівень контролю користувача над логікою прийняття рішень штучним інтелектом всередині будинку. Для вирішення цієї проблеми, слід надати користувачеві можливість продивлятися та вручну коригувати той профіль користувача, який про нього побудує штучний інтелект. Наприклад, коригувати порогові значення температури (встановлені під час навчання штучного інтелекту) для автоматичного увімкнення опалення.

5.4 Підхід до побудови профілю комфорту користувача

Отже, зрозуміло які сценарії використання інтелектуальної автоматизації заснованої на профілях комфорту користувача, проте пока відкритим залишається питання процедури побудови цього профілю комфорту. Профіль комфорту має бути заснований на індивідуальних особливостях користувача, на поведінкових

патернах та особливостях його поведінки в будинку. Отже, єдиний шлях для побудови такого профілю комфорту користувача – це проводити спостереження за поведінкою користувача.

Для того щоб оброблюючи дані про поведінку користувача в будинку створити певний профіль його комфорту, слід в автоматичному режимі знаходити взаємозв'язок між станом будинку та діями які робить у будинку користувач. Штучний інтелект має навчитися на поведінці користувача, і для цього має бути застосоване машинне навчання. Штучний інтелект має постійно проводити пошук кореляції між усіма даними, які є в його наявності та діями які робить у будинку користувач.

Розумний Будинок має наступні типи приладів (Розумних Речей):

- сенсори (постачальники даних про будинок);
- прилади управління (Розумні Речі, що сприймають та виконують певні управляючі команди).

Інтелект слід навчати шляхом пошуку кореляцій від даних сенсорів і подій що відбуваються в будинку (наприклад відкриття дверей чи поява руху людини в кімнаті) до дій (управляючих команд), які користувач виконує в будинку.

5.4.1 Навчання штучного інтелекту на абстрактних даних

Важливим моментом процедури навчання штучного інтелекту на поведінці користувача є навчання виключно на абстрактних даних. Під абстрактними даними мається на увазі те, що інтелект у процесі навчання не повинен знати дані функціонально яких саме приладів він оброблює. Тобто процес навчання має бути не обізнаний про функціональні призначення Розумних Речей на даних з яких навчається інтелект.

Наприклад інтелект не повинен розуміти де дані сенсорів температури, а де вологості чи освітлення, інтелект не повинен знати де дані про увімкнення освітлення, а де про увімкнення вентилятора для провітрювання. Тобто інтелект повинен розуміти які саме прилади були задіяні та які дані було отримано, проте не повинен бути обізнаним що це за прилади за функціональним призначенням.

Таким чином, в процесі навчання штучний інтелект шукатиме кореляції між усіма наявними даними, що допоможе йому виявляти надійні та стабільні кореляції, які однак можуть бути нелогічними з першого погляду, та людині запропонувати це як можливу закономірність було б дуже важко.

Завдяки такому підходу, інтелекту не потрібно початково закладати ніякі потенційні зв'язки (наприклад між сенсорами рівня освітленості та вимикачами ламп освітлення), а його навчання проводитиметься без додаткових попередніх конфігурацій, які потенційно були б динамічним та потребували б оновлення. Таким чином, такий абстрактний штучний інтелект готовий до обробки даних та до навчання на них з будь-яких існуючих Розумних Речей, а також з будь-яких Розумних Речей що коли-небудь існуватимуть. Отже, з появою Розумних Речей нового типу або нового функціонального призначення, такий абстрактний штучний інтелект не потребуватиме оновлень процесу навчання.

5.4.2 Процедура навчання

В розробці підходів до навчання інтелектуальної системи для Розумних Будинків важливо брати до уваги те, що закономірності, які штучний інтелект покликаний виявити в даних про поведінку користувача можуть бути відсутніми насправді. Тобто слід враховувати, що якісь дії користувача можуть бути спонтанними та не залежати від якихось параметрів у будинку, а значить

справжньої кореляції в даних за таких обставин бути не може. Отже, вибірку для навчання сформувати в такому випадку неможливо, бо взаємозв'язку між входами та виходами підсумкового інтелекту може не бути серед даних зібраних продовж спостерігання за діями користувача. Тому неможливим є застосування навчання з учителем для цієї задачі.

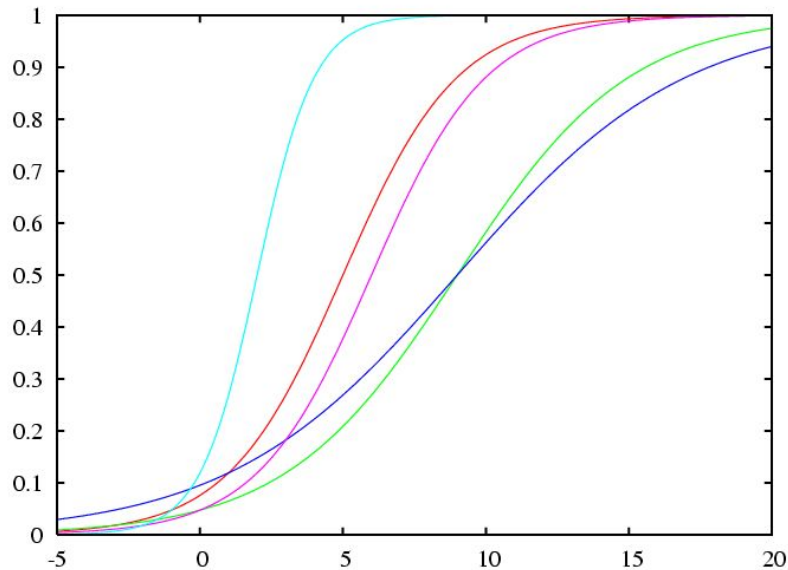
Так як неможливо навчати штучний інтелект на навчальній вибірці – слід шукати кореляції серед даних та використовувати ці кореляції, застосування нейронних мереж за таких умов неможливе. Для того щоб відокремити дані серед яких необхідно проводити пошук кореляцій, слід брати для аналізу дані про події та дані з сенсорів продовж певного невеликого часу безпосередньо перед дією користувача в будинку. Серед цих даних слід за допомогою регресії шукати кореляцію між даними сенсорів та дією яку зробив користувач. Очевидно, що не всі вхідні параметри матимуть вплив на ту чи іншу дію користувача (вихідний параметр), аналіз має виявити ті параметри, які корелюють з вихідним параметром, а після цього шукати порогові значення на яких вихідна подія вважатиметься прогнозованою.

5.4.3 Логістична регресія як модель навчання

Навчена підсумкова модель повинна визначати кореляції де залежна змінна є бінарною (дія користувача відбулась чи не відбулась). Для таких змінних побудова звичайної лінійної регресії є некоректною, тож у якості моделі для прогнозування виконання користувачем дій у будинку слід використовувати логістичну регресію [8]. Логістична регресія використовується для прогнозування вірогідності виникнення певної події (де виникнення певної події по суті є бінарним результатом), а власне математичним очікуванням в моделі є

вірогідність того, що залежна змінна (у нашому випадку факт виникнення певної дії користувача) дорівнює одиниці.

Результатом логістичної регресії є логістична функція, приклади графіків логістичної функції [9] зображено на Рисунку 7.



«Рисунок 7 – Графіки логістичної функції»

У ідеальному випадку спектр значень, для яких вірогідність (математичне очікування) не дорівнює ані нулю ані одиниці, прямуватиме до нуля, при цьому швидкість набору висоти графіком буде вищою. Тобто впевненість моделі в прогнозі на значення залежної змінної буде найвищим.

ВИСНОВКИ

Під час роботи були проведені дослідження сучасних систем управління Розумними Будинками. Внаслідок дослідження прикладних реалізацій сучасних проектів систем Розумних Будинків та розгляду досліджень в цій галузі, були виявлені деякі невирішені проблеми галузі та сформульовані задачі, які необхідно вирішити в рамках дослідження.

За допомогою теоретичних методів досліджень, моделювання та формалізації певних частин систем управління Розумними Будинками були розроблені підходи та конкретні технічні рішення, що здатні покращити такі системи. Під час досліджень були виділені корені певних технічних проблем галузі, досліджені основні перепони що заважають розв'язати ці технічні проблеми. Після цього сформульовані обмеження, якими не можна знехтувати під час винаходження нових технічних рішень, що здатні розв'язати проблеми галузі, та винайдені підходи, які не виходячи за сформульовані обмеження вирішують певні технічні проблеми.

В ході досліджень були одержані результати, що є новими для галузі, напрацьовані підходи та конкретні технічні рішення, застосування яких у системах управління Розумними Будинками дасть змогу спростити ці системи як з точки зору їх розробки так і з точки зору користування ними. Підходи розроблені під час досліджень дають змогу суттєво нівелювати проблеми різномірності апаратного забезпечення в системах управління Розумними Будинками, забезпечити безпеку передачі команд управління до Розумного Будинку та створити ефективну гнучку інтелектуальну автоматизацію управління Розумними Будинками.

Результати цих досліджень можуть бути застосовані в системах управління Розумними Будинками, що значно спростить процес розробки, розширення та

підтримки таких систем, а також покращить рівень безпеки процесу управління Розумними Будинками та надасть змогу гнучко запровадити інтелектуальні пропозиції по управлінню Розумними Будинками користувачам на основі побудованих на їх індивідуальних даних профілів комфорту користувачів.

Подальші дослідження цієї теми слід вести в напрямку проведення випробувань напрацьованих підходів на реальному апаратному забезпеченні з перевіркою повноцінної працездатності цих підходів під час реального використання системи як Розумного Будинку. Особливу увагу при цьому слід звернути на досвід користувача від використання системи в якій запроваджено розроблені підходи та порівняти досвід користувачів. Також підходи з приводу покращення безпеки систем управління Розумними Будинками після перевірки в реальних умовах слід перевірити шляхом проведення перевірки безпеки через тестування системи на проникнення. Розроблені підходи для побудови профілів комфорту користувачів слід перевірити на реальних системах та зафіксувати ефективність від застосування такої інтелектуальної автоматизації, використовуючи як метрику оцінку користувачів позитивності досвіду використання системи управління Розумним Будинком з інтелектуальною автоматизацією такого роду.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Guangyi Xiao, Member, IEEE, Jingzhi Guo, “User Interoperability With Heterogeneous IoT Devices Through Transformation” // IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 10, NO. 2, MAY 2014 URL: http://www.cis.umac.mo/~jzguo/pages/pub/14_TII.pdf (дата звернення: 25.05.2018).
2. Google Home main page // Google Home URL: https://store.google.com/us/product/google_home?hl=en-US (дата звернення: 20.04.2018).
3. Amazon Echo article // Wikipedia URL: https://en.wikipedia.org/wiki/Amazon_Echo (дата звернення: 20.04.2018).
4. Welcome page OpenHUB // OpenHUB URL: <https://www.openhab.org/> (дата звернення: 20.04.2018).
5. Welcome page Jeedom // Jeedom URL: <https://www.jeedom.com/site/en/index.html> (дата звернення: 20.04.2018).
6. Hoan-Suk Choi, Jun-Young Lee, Na-Ri Yang, Woo-Seop Rhee, “User-centric Service Environment for Context Aware Service Mash-up” // 2014 IEEE World Forum on Internet of Things (WF-IoT) URL: https://www.researchgate.net/profile/Hoan_Suk_Choi/publication/269309102_User-centric_service_environment_for_context_aware_service_mash-up/links/5718ed4208ae986b8b7b2bde.pdf (дата звернення: 26.05.2018).
7. Leandro Marin, Marcin Piotr Pawlowski, and Antonio Jaram “Optimized ECC Implementation for Secure Communication between Heterogeneous IoT Devices” // Sensors 2015 URL: <http://www.mdpi.com/1424-8220/15/9/21478/htm> (дата звернення: 28.05.2018).
8. Логістична регресія // Wikipedia URL: <https://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D1%96%D1%81%D1%8>

[2%D0%B8%D1%87%D0%BD%D0%B0_%D1%80%D0%B5%D0%B3%D1%80%D0%B5%D1%81%D1%96%D1%8F](https://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D1%96%D1%81%D1%82%D1%8C) (дата звернення: 04.06.2019).

9. Логістична рівність // Wikipedia URL:
https://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D1%96%D1%81%D1%82%D0%B8%D1%87%D0%BD%D0%B0_%D1%80%D1%96%D0%B2%D0%BD%D1%96%D1%81%D1%82%D1%8C (дата звернення: 04.06.2019).