МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ЗАЛУЖНИЙ Василь Вікторович

Модель контролю доступу для забезпечення безпеки «розумного будинку» / Access Control Model for Smart Home Security

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -22
В.В. Залужний

_____

Науковий керівник
д.т.н., професор М.М. Касянчук

_____

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2023 р.

Завідувач кафедри

_____ В.В.Яцків

ТЕРНОПІЛЬ – 2023

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ЗАЛУЖНИЙ ВАСИЛЬ ВІКТОРОВИЧ

1. Тема кваліфікаційної роботи:
Модель контролю доступу для забезпечення безпеки «розумного будинку» / Access Control Model for Smart Home Security
керівник роботи д.т.н., професор М.М. Касянчук
затверджені наказом по університету від «__» _____ 2022 року № _____
2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– огляд та аналіз технологій «розумного середовища» та «розумного будинку»;
– визначити основні типи загроз в системах «розумного» та прийнятні контекстні моделі контролю доступу;
– розробити архітектуру системи «розумного будинку» із контекстною моделлю доступу;
– розробити алгоритми функціонування системи «розумного будинку» із контекстною моделлю доступу;
– дослідити основні типи атак на систему «розумного будинку».

5. Перелік графічного матеріалу у роботі:

– архітектура шлюзу контролю доступу;
– формування правил контролю доступу;
– блок-схема алгоритму аналізу контексту;
– алгоритм перерозподілу рівнів;
– склад модельованої системи «розумного будинку»;
– загальна платформа системи моделювання;
– діалогове вікно програми.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз безпеки систем «Розумного будинку»	12.2022 р. – 03.2023 р.	
2	Застосування контекстної моделі контролю доступу для посилення безпеки систем «Розумного будинку»	03.2023 р. – 05.2023 р.	
3	Моделювання системи «Розумного будинку» та атак на систему	05.2023 р. – 11.2023 р.	

Студент _____ Залужний В.В.

(підпис)

Керівник роботи _____ д.т.н., професор М.М.Касянчук

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Модель контролю доступу для забезпечення безпеки «розумного будинку»” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека” освітньо-професійної програми «Кібербезпека» написана обсягом 77 сторінок і містить 23 ілюстрацій, 1 таблицю, 1 додаток та 32 джерела за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка моделі контролю доступу для забезпечення безпеки «розумного будинку».

Методи дослідження. Математичні методи моделювання та програмування, методи алгоритмізації.

Результати дослідження. Здійснено аналіз основних типів технологій «розумного середовища» та «розумного будинку», що дозволило встановити основні типи загроз на систему та способи захисту від них. Розроблено математичне та алгоритмічне забезпечення системи «розумного будинку» із контекстною моделлю доступу, що дозволило побудувати відповідні моделі «розумного будинку». На основі побудованих моделей «розумного будинку» розроблено алгоритм функціонування системи захисту, що дозволило дослідити основні методи захисту від атак. Розроблено архітектуру системи «розумного будинку» із контекстною моделлю доступу.

Результати роботи можуть успішно застосовуватися для контролю доступу для забезпечення безпеки «розумного будинку».

КЛЮЧОВІ СЛОВА: КОНТРОЛЬ ДОСТУПУ, КОНТЕКСТНА МОДЕЛЬ, ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ, «РОЗУМНИЙ БУДИНОК», МОДЕЛЮВАННЯ АТАК.

ABSTRACT

The graduate work on the topic „Access Control Model for Smart Home Security” for Master’s degree on speciality 125 "Cybersecurity " is written on 77 pages and contains 23 illustrations, 1 table, 1 suplement and 32 references.

The aim of graduate work is the development an access control model to ensure the security of a "smart home".

Research methods. Mathematical methods of modeling and programming, methods of algorithmization.

Results of the study. An analysis was made of the main types of "smart environment" and "smart home" technologies, which made it possible to establish the main types of threats to the system and methods of protection against them. Mathematical and algorithmic support of the "smart house" system with a contextual access model was explained, which made it possible to build appropriate "smart house" models. Based on the constructed models of the "smart house" an algorithm for the functioning of the protection system was developed, which made it possible to investigate the main methods of protection against attacks. The architecture of the "smart house" system with a context model of access has been developed.

The results of the work can be successfully applied for access control to ensure the security of the "smart home".

Keywords: ACCESS CONTROL, CONTEXT MODEL, SECURITY ENSURING, SMART HOME, ATTACK SIMULATION.

ЗМІСТ

ВСТУП

Актуальність теми. В даний час бурхливий розвиток переживає технологія «розумних середовищ» [1-4]. У зв'язку із молодістю цієї технології, поки що відсутнє загальновизнане визначення, однак можна виділити ряд положень, що характеризують такі середовища – це використання сенсорів та обчислювальних пристроїв, що взаємодіють у динамічному децентралізованому середовищі для досягнення єдиної мети, такої, як забезпечення безпеки чи ефективного управління [5-7]. Виділяються такі характерні ознаки таких середовищ:

- безпосередня взаємодія між пристроями;
- віддалене керування пристроями;
- складний функціонал пристроїв;
- "інтелектуальність" пристроїв;
-- різноманітність стандартів мережевої взаємодії.

Такі середовища в першу чергу знаходять своє застосування в різних системах автоматизації [8-10], надаючи хорошу основу для побудови інфраструктури. Одним з найбільш поширених прикладів використання «розумних середовищ» є системи «розумного будинку», що є розвитком автоматичних систем керування спорудами [11-12].

Системи «розумного будинку» призначені для забезпечення зручності та безпеки проживання, а також підвищення енергоефективності будівлі [13-14]. При цьому недостатньо уваги приділяється інформаційній безпеці самої системи. Для більш повного розуміння проблеми необхідно визначити ключові особливості системи та можливі проблеми безпеки, пов'язані із нею.

У класичних автоматизованих системах управління будівлею (АСУЗ), що є основою для систем «розумного будинку», виділяються три рівні автоматизації [15]:

- рівень диспетчеризації та адміністрування, на якому здійснюється взаємодія персоналу з системою, та збір статистичної інформації;

- рівень автоматичного управління, на якому реалізується автоматизація процесів у різних інженерних системах будівлі. Включає контролери та комутаційне обладнання;

- рівень кінцевих пристроїв, який включає датчики, виконавчі пристрої та безпосередньо фізичні з'єднання між компонентами.

У системі «розумного будинку» відбувається розширення рівня автоматизованого управління [16-18] та зниження ролі рівня диспетчеризації за рахунок можливості автономного прийняття рішень. Підвищений рівень автоматизації спричиняє нові проблеми безпеки. Поточні дослідження безпеки насамперед спрямовані на рішення питань, пов'язаних з приватністю, тобто тільки з конфіденційністю інформації, що збирається та обробляється в системі "розумного будинку". Для «розумних середовищ» загалом пропонується застосування моделей контролю доступу, що базується на контексті. При цьому суб'єктами доступу є користувачі системи, а об'єктами - пристрої, які складають єдину систему. Одним із перспективних напрямків досліджень є застосування контролю доступу для забезпечення безпеки при взаємодії між компонентами динамічного середовища "розумного будинку" [19-20].

Мета роботи. Метою роботи є розробка моделі контролю доступу для забезпечення безпеки «розумного будинку».

Для вирішення поставленої мети вирішуються наступні **завдання**:

– огляд та аналіз технологій «розумного середовища» та «розумного будинку»;

– визначити основні типи загроз в системах «розумного» та прийнятні контекстні моделі контролю доступу;

– розробити архітектуру системи «розумного будинку» із контекстною моделлю доступу;

– розробити алгоритми функціонування системи «розумного будинку» із контекстною моделлю доступу;

– дослідити основні типи атак на систему «розумного будинку».

Об’єкт дослідження. Процес забезпечення безпеки системи «розумного будинку» із контекстною моделлю доступу.

Предмет дослідження. Методи і засоби забезпечення безпеки системи «розумного будинку» із контекстною моделлю доступу.

Методи дослідження. Математичні методи моделювання та програмування, методи алгоритмізації.

Наукова новизна одержаних результатів.

1. Здійснено аналіз основних типів технологій «розумного середовища» та «розумного будинку», що дозволило встановити основні типи загроз на систему та способи захисту від них.

2. Розроблено математичне та алгоритмічне забезпечення системи «розумного будинку» із контекстною моделлю доступу, що дозволило побудувати відповідні моделі «розумного будинку».

3. На основі побудованих моделей «розумного будинку» розроблено алгоритм функціонування системи захисту, що дозволило дослідити основні методи захисту від атак.

Практичне значення отриманих результатів. Розроблено архітектуру системи «розумного будинку» із контекстною моделлю доступу.

Публікації та апробація КР.

1. Залужний В.В., Козбур Г.Є. Механізми контролю доступу в контекстних моделях. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.103-105 [21]

2. Залужний В.В., Моцний В.О. Моделювання атаки на систему «Розумний будинок». Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.71-74 [22].

1 АНАЛІЗ БЕЗПЕКИ СИСТЕМ «РОЗУМНОГО БУДИНКУ»

1.1 «Розумні середовища» та «розумний будинок»

«Розумне середовище» - це об'єднання пристроїв, які спільно розподіляють свої ресурси та працюючих [23-25]. Природа розумного середовища припускає виникнення конфліктів між різними пристроями та учасниками, які можуть переслідувати протилежні цілі, і мати різне поняття про поточну ситуацію, але при цьому функціонувати в загальному довіреному інформаційному просторі. Для зниження ризиків інформаційної безпеки потрібна підтримка механізму динамічного контролю доступу до загальних ресурсів. Таким чином, з'являється необхідність у моделі контролю доступу, що використовує інформацію про поточний стан середовища у формі контексту виконання операцій.

Основною метою «розумних середовищ» є отримання та аналіз інформації про навколишню реальність з метою надання користувачам середовища нових можливостей щодо взаємодії із зовнішнім середовищем. Крім цього, можуть застосовуватися механізми адаптації до потреб користувачів. Як було зазначено раніше, можна виділити наступні властивості розумних середовищ:

1) безпосередня взаємодія між пристроями;

2) віддалене керування пристроями;

3) складний функціонал пристроїв;

4) "інтелектуальність" пристроїв;

5) різноманітність стандартів мережевої взаємодії.

У «розумному будинку» широко застосовуються автоматизовані системи управління будинками або технологіями для вирішення різних завдань, що виникають під час експлуатації споруд [26].

Технологія «розумного будинку» полягає у застосуванні сучасних систем автоматизації та різноманітних периферійних пристроїв з метою забезпечення

безпеки, економії ресурсів та покращення умов проживання загалом [27]. Однією з ключових особливостей є активна взаємодія різних автоматизованих підсистем для отримання нових можливостей з розпізнавання та реагування на різні ситуації. З фізичного погляду такі системи є розвитком АСУЗ, які, у свою чергу, є адаптацією АСУ для будівель та споруд.

Сучасні розумні будинки мають доступ до конфіденційної інформації і володіють правом управління більшістю домашньої електроніки і техніки. У зв'язку з цим існує ризик, що управління системою, а також віддалений контроль над усіма підключеними пристроями, може бути перехоплено зловмисником. Найпоширенішими атаками зловмисників є віддалене перехоплення контролю над будівлею та отримання конфіденційної інформації. Предметами атаки можуть стати безпровідні модулі в мережі, такі як смарт-розетки, розумні колонки, електронні дверні замки, електронні лічильники та сервери зберігання інформації.

Аналіз інформації про різні системи автоматизації житлових приміщень та моделювання подібних умов із застосуванням технічних та програмних засобів дозволяє визначити основні вектори атаки на системи «Розумний дім» та способи їх запобігання.

Однією з основних проблем безпеки розумних пристроїв є незахищеність каналів зв'язку [28] як у зовнішній частині мережі, так і у внутрішній, включаючи канали зв'язку між розумними пристроями та датчиками, що надалі дозволяє віддалено перехоплювати управління та контролювати всі параметри та дані в розумних будинках.

Застосування методів оцінки ризиків та пошуку каналів витоку інформації, виявлення проблем конфіденційності та безпеки систем, моделювання та пропозиція методів підвищення захищеності систем призводить до поліпшення якості захисту сучасних розумних систем автоматизації.

З аналізу випливає, що сучасний розумний будинок націлений на підвищення якості життя шляхом розгортання повністю автоматизованого управління приладами та надання додаткової допомоги мешканцям. Такий будинок дозволяє підвищити енергоефективність за рахунок адаптивної експлуатації пристроїв у кожному конкретному випадку, підвищити зручність користування домашнім обладнанням, вести своєчасний облік витрати комунальних послуг, автоматично економити електроенергію шляхом керування енергоспоживанням, надавати функціональну мультимедійну базу, розширені можливості щодо забезпечення безпеки будівлі та повний віддалений контроль за технікою. Користувачі та пристрої постійно пов'язані у розширений комунікаційний мережевий комплекс.

При проведенні аналізу виявлено, що більшість існуючих систем мають розрізнені протоколи зв’язку, не використовують загальноприйнятні стандарти безпеки, мають небезпечні налаштування.

1.2 Основні технології для розумних будинків

Найактуальніші технології для розумних будинків були згруповані за такими чотирма категоріями [29]:

а) інтегрована бездротова технологія (ІБТ);

б) система управління домашньою енергією (СУДЕ);

в) розумні домашні мікрокомп'ютери (РДМ);

г) системи домашньої автоматизації (СДА).

ІБТ - це система комунікації, яка зазвичай використовується в офісній будівлі, приватному будинку або будь-якому іншому житловому приміщенні для забезпечення внутрішнього та зовнішнього ближнього зв'язку в рамках технології «розумного дому». ІБТ частіше віддають перевагу порівняно з провідними технологіями. Використання провідних рішень було б економічно та/або фізично недоцільно для багатьох застосувань "розумних мереж".

Натомість бездротові технології дають такі переваги, як нижча вартість обладнання та установки, швидке розгортання, широкий доступ та велика гнучкість.

На рисунку 1.1 показано архітектуру «розумного будинку» верхнього рівня. Вона включає сервер/шлюз/маршрутизатор як підключення до будинку та розумної мережі. Вони можуть встановлюватися за допомогою однієї або комбінації зовнішніх мереж, таких як телефонні лінії, цифрові абонентські лінії (xDSL), кабельні мережі та мережі електроживлення.

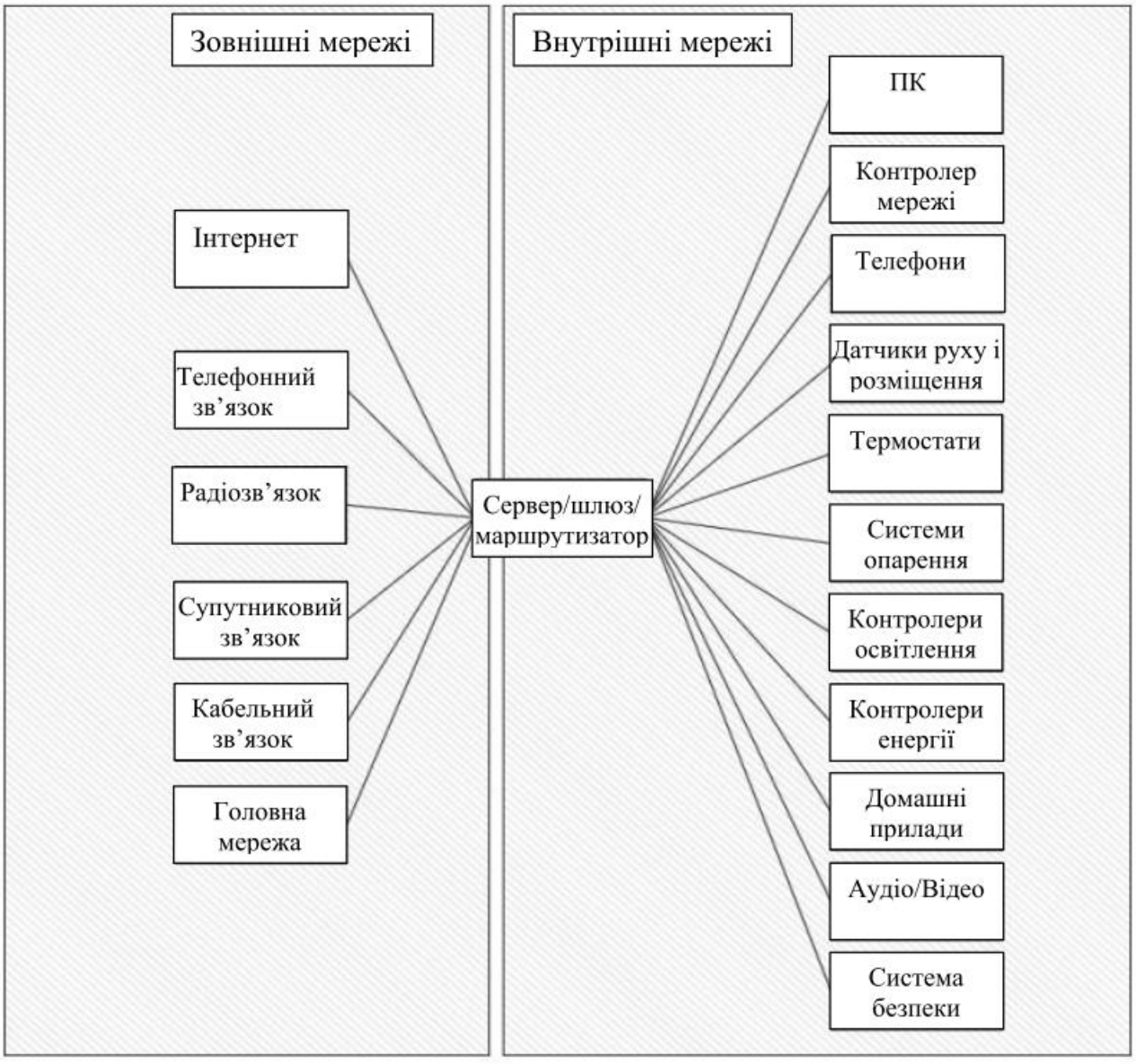

Рисунок 1.1 – Архітектура верхнього рівня типового розумного будинку

Розробки СУДЕ почалися в зв'язку з нестачею енергії та наслідками глобального потепління. З моменту її першого застосування в 1976 р. вона стала однією з найпопулярніших тем для досліджень. Система СУДЕ дозволяє автоматично керувати та контролювати енергоспоживання будівлі та допомагає знизити піковий попит на електроенергію та рахунки користувачів за електрику.

Кількість установок СУДЕ зростає в районах Північної Америки та Європи, які мають велику широту, через кількість темної доби на рік. У цих районах СУДЕ досить суттєво знижують загальний попит на електроенергію: до 30% навантаження на електроенергію припадає на години пікових навантажень. Пікове навантаження можна знизити в середньому на 30%, а експлуатаційні витрати на електроенергію – на 23%.

У «розумних» мережах використання СУДЕ стало пріоритетним для локального розподілу енергії, що необхідна споживачам, відповідно до цін на енергію, що регулюються добовими тарифами. Майбутня тенденція може полягати у використанні специфічних погодинних тарифів, тобто тарифу в реальному часі, часі використання, критичного пікового тарифу тощо.

РДМ– це невеликі комп'ютери, які підключаються до інших пристроїв для автоматизації та управління всією системою «розумного будинку». Вони складаються з мікроконтролера з додатковими компонентами, які полегшують програмування, та вбудовуються до інших схем. Важливим аспектом є їх стандартні роз'єми, які дозволяють користувачам підключатися до плати центрального процесора, а також до різних взаємозамінних додаткових модулів. Вони дозволяють користувачам створювати інтерактивні проекти та програми з навколишнім середовищем, використовуючи кілька роз'ємів, що розширюються, і отримуючи вхідні дані від багатьох датчиків та впливаючи на їх оточення, керуючи освітленням або іншими виконавчими механізмами.

СДА надає інтелектуальний інтерфейс, який відстежує та вивчає звички користувачів, а також може передбачати та полегшувати їх дії. Він зможе

зробити життя легшим і комфортнішим, забезпечити деяку економію енергії за рахунок віддаленої взаємодії з користувачами.

СДА вирішує частину завдань у системі управління розумним будинком. Однак для взаємодії з користувачами систему СДА необхідно комбінувати з неавтоматизованими пристроями. Наприклад, використання тільки СДА-систем не дасть користувачам можливості регулювати енергоспоживання. Але за умови, що кінцевим користувачам буде надано зворотний зв'язок, заснований на діях по управлінню, що виконуються в рамках системи автоматизації розумного будинку, то ця функція буде чинною.

Таку технологію можна було б включити в інтелектуальну систему, яка дозволяє економити енергію, покращувати тепловий та візуальний комфорт в будинку за рахунок реалізації як короткострокових, так і довгострокових показників теплового та зорового дискомфорту/

1.3 Датчики довкілля

Датчики цього типу не прикріплені до людей, а розміщені у навколишньому середовищі, у якому перебувають користувачі. Вони особливо цінні, тому що вони надають інформацію, не вимагаючи від людей дотримання правил в установленому порядку. Це чудовий аспект, тому що в реальних системах необхідно враховувати інші функціональні можливості, саме інвазивність обраного рішення.

Навіть незважаючи на те, що датчики середовища можуть контролювати діяльність групи людей, вони можуть відчувати труднощі з поділом рухів або дій між індивідуумами, що є частиною цієї групи.

Пасивний інфрачервоний датчик, який також називається датчиком руху, вимірює інфрачервоне світло, що випромінюється об'єктами в його полі зору. Якщо різниця у виявленому випромінюванні між декількома отворами ІЧ-датчика більша заданого порога (це відбувається, коли тепле тіло входить у

зону дії сенсора або виходить із неї), він генерує повідомлення. Людина випромінює інфрачервоне випромінювання, тому ІЧ-датчики можуть бути використані для виявлення її руху в межах зони покриття. Оскільки пасивний інфрачервоний датчик чутливий до теплових рухів, він може працювати в умовах недостатньої освітленості. З іншого боку, він може не відчувати руху, якщо об'єкт знаходиться між датчиком і людиною, що рухається. Всі об'єкти з температурою, вищою за абсолютний нуль, випромінюють теплову енергію у вигляді випромінювання, тому такого роду датчики можуть видавати повідомлення навіть у тому випадку, якщо такий пристрій, як принтер, починає друкувати великий документ у безпосередній близькості. Рисунок 1.2 ілюструє сценарій роботи ІЧ-датчика.

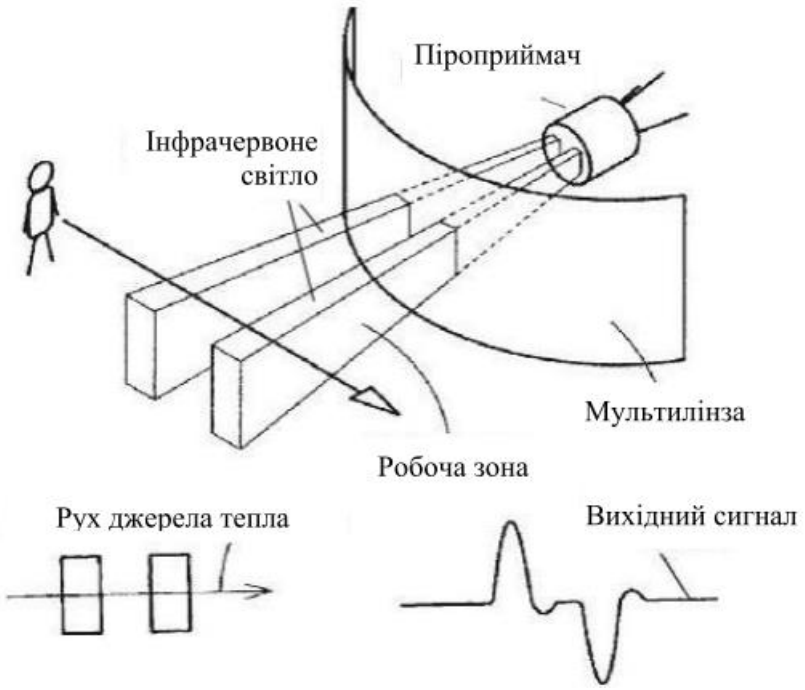

Рисунок 1.2 – Взаємодія ІЧ-датчика з людиною, яка перетинає зону виявлення

Магнітні датчики дверей складаються з двох частин, які утворюють ланцюг, коли вони розташовані паралельно один до одного. Коли хтось відкриває двері (або будь-яку деталь, що відкривається), ці дві частини розділяються та розривають ланцюг, викликаючи зміну стану датчика, який

може бути зареєстрований як подія, пов'язана з датчиком. Точно так само, коли двері зачиняються назад, ланцюг знову замикається і відбувається подія. Цей датчик корисний для визначення того, чи відкриті чи закриті двері, вікна, ящики чи шафи.

Додаткові датчики (температури, світла, вологості) можуть бути розміщені в приміщеннях для вимірювання температури навколишнього середовища, освітлення та вологості. Такі датчики можуть бути запрограмовані на періодичне повідомлення про їхній поточний стан або, коли їхнє поточне показання суттєво відрізняється від попереднього моменту часу.

Датчик тиску - це пристрій для вимірювання тиску будь-яких газів чи рідин. Тиск є виразом сили, необхідної для зупинки розширення рідини, і зазвичай вказується в одиницях сили на одиницю площі. Для контролю діяльності у конкретному середовищі тактильні датчики чутливі до дотиків чи сили. Ці датчики тиску виявляють та вимірюють взаємодію між людиною та поверхнею контакту, їх можна розмістити під або над дверними килимками, стільцями, ліжками та підлогами. Вони використовуються для контролю розташування та розподілу ваги людини на спроектованій поверхні.

Сенсори глобальної системи позиціонування (GPS) – це супутникова навігаційна система, що використовується для визначення наземного становища об'єкта. Ці пристрої засновані на зв'язку принаймні з чотирма супутниками глобальної системи позиціонування і, таким чином, не можуть використовуватись у будь-яких умовах. Більше того, так як приймачі GPS вимагають безперешкодного шляху до космосу, технологія GPS не ідеальна для використання всередині приміщень і зазвичай використовується в інших системах.

Bluetooth маяки передають універсальний унікальний ідентифікатор, отриманий сумісним додатком чи операційною системою. Ідентифікатор та кілька байтів, відправлених разом з ним, можуть бути використані для

визначення фізичного місцезнаходження пристрою, відстеження клієнтів або ініціювання дій на основі розташування пристрою.

1.4 Аналіз безпеки протоколів систем «розумного будинку»

У контексті комп'ютерних наук, існує безліч різноманітних протоколів, що застосовуються у сфері автоматизації управління будинками. На сьогоднішній день надзвичайно актуальним стає питання стандартизації мережевої взаємодії між пристроями, що складають інтегровану систему "розумного будинку". Наразі відсутні загальновизнані норми в цьому контексті. Відповідно до поточної ландшафту, приміщення розумних будинків мають багато різних пристроїв, які здатні взаємодіяти між собою, і відсутність стандартів суттєво ускладнює цей процес.

З огляду на вище викладене, виникає питання про доцільність використання технологій локальних обчислювальних мереж [30]. З цього приводу слід зазначити, що цей підхід може бути менш перспективним унаслідок їхньої надмірності та обмеженої функціональності відносно потреб сучасних розумних будинків. У зв'язку з цим, важливо визначити ключові вимоги до технологій, що використовуються в системах "розумних будинків":

- низьке споживання енергії;
- висока надійність та забезпечення безпеки передачі даних;
- доступність за ціною;
- простота фізичного розташування та інсталяції пристроїв.

Цільові вимоги до продуктивності й ефективності технологій у контексті розумних будинків можуть значно відрізнятися в залежності від конкретних сценаріїв використання. Подекуди швидкість передачі даних не має критичного значення, і основна увага зосереджується на інших аспектах, таких як стійкість і надійність.

При порівнянні провідних та безпровідних мереж, важливим критерієм стає спрощення фізичного розташування мережевих пристроїв. Відзначається сімейство конкурентоспроможних технологій провідних мереж, відомих як Power Line Communication (PLC). Суть цих технологій полягає в використанні наявності електричних мереж у приміщеннях для передачі даних. Такий підхід дозволяє створити як провідні, так і бездротові мережі, використовуючи технології, такі як X10, INSTEON, HomePlug, Lonworks для передачі даних через електричні проводи, а також Bluetooth, Z-Wave та ZigBee для організації бездротового зв'язку [31].

Значущим досягненням в цій області є протокол Z-Wave, що представляє собою комплекс стандартів, розроблених і підтримуваних організацією Z-Wave Alliance. Сьогоднішнім етапом розвитку є визнання цього протоколу одним з найбільш обіцяючих у сфері систем «розумних будинків». Наявність різних рівнів, що відповідають моделі OSI, демонструє його важливість у структурі мережевої взаємодії:

- фізичний рівень;

- канальний рівень: на цьому рівні мережевого протоколу Z-Wave відбувається важливий контроль - забезпечення цілісності та адресації пристроїв в межах зони безпосередньої видимості. Це означає, що пристрої можуть обмінюватися даними в рамках прямої лінії видимості одне до одного. Важливою на цьому рівні є можливість одночасної адресації кількох пристроїв (багатоадресність) та передачі даних для всіх пристроїв в мережі (широкомовне розсилання);

- мережевий рівень. В мережевому протоколі Z-Wave прописані докладні вказівки щодо алгоритму маршрутизації для одноадресних пакетів. Цей алгоритм використовується для передачі даних між пристроями, які знаходяться за межами безпосередньої досяжності один до одного. Усі пристрої, що постійно функціонують у мережі, беруть участь у передачі пакетів від одного до іншого. Протокол передбачає, що маршрут, яким буде йти пакет,

визначається перед відправленням пакету вузлом-відправником. Якщо неможливо знайти прямий маршрут до призначеного вузла за допомогою вже відомих маршрутів, то існує механізм пошуку шляхом відправки спеціального пакету Explorer Frame до всіх вузлів мережі;

- транспортний рівень: Транспортний рівень протоколу Z-Wave відіграє важливу роль у забезпеченні доставки даних та вирішенні можливих втрат пакетів. Кожен вузол, що бере участь у передачі, зобов'язаний підтверджувати факт отримання повідомлення. Це допомагає забезпечити надійну доставку та в разі виявлення втрати пакету - його повторну відправку. У режимі "мовчазних підтверджень" вузол, який відправив пакет на наступний вузол, спостерігає за прослуховуванням ефіру та визначає, коли пакет був успішно переданий наступному вузлу. Підтвердження надсилається лише після успішної доставки пакета до остаточного призначення;

- сеансовий рівень. Він використовується лише при активованому шифруванні для встановлення сеансового ключа. Це допомагає забезпечити безпеку обміну даними між пристроями на вищих рівнях;

- прикладний рівень: на прикладному рівні протоколу Z-Wave визначено алгоритми інтерпретації отриманих команд. Цей рівень описаний набором класів команд, і для деяких класів може існувати кілька способів інтерпретації команд в залежності від типу пристрою;

Важливо зауважити, що критичні компоненти систем автоматизації, наприклад, замки певного виду, на сьогоднішній день використовують шифрування за стандартом AES-128. Проте, шифрування є додатковим розширенням стандарту, і ранні версії деяких пристроїв можуть не підтримувати цю функцію. Деякі дослідники також виявили вразливості в імплементації протоколу під час обміну ключами, що може також інколи приводити до компрометації системи, використовуючи стандартний ключ за замовчуванням.

У контексті полегшення управління системами "розумного будинку" на базі протоколу Z-Wave, одним із рішень, сертифікованим Z-Wave Alliance, є Z-Way. Цей інструмент надає засоби взаємодії з системою через веб-інтерфейс та API. Однак, слід зазначити, що в цьому контексті відсутні механізми аутентифікації та шифрування даних. Такий підхід може створювати потенційні точки вразливості, через які атакуючий може отримати доступ та контроль над системою "розумного будинку" після компрометації локальної мережі.

ZigBee є стандартом відкритого бездротового зв'язку для систем автоматизації [32]. Він включає в себе специфікації мережевих протоколів верхнього рівня, які складаються з рівня додатків та мережевого рівня. Важливо пам'ятати, що нижні рівні, які відповідають за управління доступом до середовища та фізичний рівень, регулюються стандартом IEEE 802.15.4.

Рівень додатків визначає об'єкт конкретного пристрою ZigBee. Цей рівень включає в себе інтерфейс розробки додатків, який містить опис стандартних типів даних, дескрипторів служб, форматів пакетів. Це дозволяє розробляти прості профілі швидко, використовуючи атрибути. Об'єкти додатків - це програмні модулі, які управляють кінцевими пристроями ZigBee.

Мережевий рівень відповідає за керування мережевими адресами та маршрутизацію. Він здійснює такі функції, як запуск мережі, присвоєння мережевих адрес, додавання та видалення мережевих пристроїв, маршрутизація повідомлень, застосування політики безпеки, пошук маршрутів.

Фізичні рівні визначаються стандартом IEEE 802.15.4. Рівень керування доступом до середовища відповідає за стабільний зв'язок з безпосередніми сусідами та вирішення колізій. Фізичний рівень забезпечує інтерфейс для передачі даних через фізичне середовище.

Постачальник послуг безпеки особисто відповідає за різні механізми безпеки на рівнях комп’ютерної мережі та програмному рівні. Важливо зазначити, що мережі стандарту ZigBee можуть працювати також і в режимах

без шифрування. Стандартний рівень безпеки не забезпечує захист ключів мережі.

У контексті безпеки, механізм лічильників, які монотонно збільшуються, використовується для запобігання атакам повтору. Однак, реалізація цього механізму може призвести до проблем з функціонуванням мережі, що вимагає ручного скидання лічильників. Фреймворк KillerBee практично демонструє атаки повтору та отримання ключа з перехопленого трафіку для аналізу мереж ZigBee.

1.5 Загрози безпеки в системах «розумного будинку»

Для систем «розумного будинку» існує низка загроз безпеки, характерних для багатьох комп'ютерних мереж [8]. У роботі [9] розглянуто ряд різних атак, які призвели до можливості їх реалізації (таблиця 1.1).

Таблиця 1.1 – Основні типи атак на «Розумний будинок»

№	Тип атаки	Вразливість	Можливі наслідки
1	Атаки на центральний вузол	Підключення мережі «Розумного будинку» до Інтернету. Відсутність (неефективність) механізмів захисту периметра мережі.	Порушення роботи або вихід з ладу центрального сервера і як наслідок, всієї системи. Порушення конфіденційності, цілісності та доступності інформації.
2	Вплив вірусних та троянських програм на роботу системи.	Підключення мережі «Розумного будинку» до Інтернет. Відсутність (неефективність) механізмів захисту периметра мережі	Збої в ПЗ системи, а, отже, порушення роботи або виведення з ладу апаратури системи. Порушення конфіденційності, цілісності та доступності інформації

Продовження таблиці 1.1

3	Перехоплення інформації, переданої по дротових та бездротових каналах зв'язку	Можливість доступу зловмисника до провідних каналів або до зони стійкого перехоплення радіосигналів мережі. Відсутність (неефективність) механізмів захисту трафіку.	Порушення конфіденційності інформації, що передається по каналу. Можливе захоплення управління системою.
4	Доступ зловмисника з правами адміністратора на центральний вузол за допомогою крадіжки паролей та інших реквізитів розмежування доступу	Відсутність (неефективність) механізмів аутентифікації та ідентифікації.	Порушення конфіденційності, цілісності та доступності інформації, яка знаходиться в мережі.
5	Доступ до мережі неавторизованих користувачів	Відсутність (неефективність) механізмів аутентифікації та ідентифікації.	Порушення конфіденційності, цілісності та доступності інформації, яка знаходиться в мережі.
6	Помилки корисувача	Відсутність (неефективність) механізмів захисту системи від неправильних дій користувачів.	Порушення конфіденційності, цілісності та доступності інформації. Можливі збої у системі через неправильне використання обладнання.

Продовження таблиці 1.1

7	Поломка апаратури системи	Низька надійність обладнання, низька кваліфікація персоналу	Порушення конфіденційності, цілісності та доступності інформації
8	Помилки програмного забезпечення	Використання неліцензійного ПЗ, низька кваліфікація персоналу, відсутність (неефективність) тестування закупленого ПЗ.	Порушення конфіденційності, цілісності та доступності інформації

На основі розглянутих атак можна зробити висновки щодо загроз, яким можна запобігти шляхом використання контекстної моделі контролю доступу. На рисунку 1.3 представлені потенційні загрози безпеці системи «розумного будинку», визначені внаслідок їх аналізу.

Виходячи з поставленої мети забезпечення безпеки системи при взаємодії пристроїв, що становлять її, визначено таку множину загроз:

- шкідливий код;
- підключення зараженого пристрою;
- зараження пристроїв у мережі;
- збій пристрою;
- неправильні дані датчиків;
- помилкові команди;
- помилка конфігурування;
- неправильна поведінка системи;
- збої у режимах роботи.

На захист від цих загроз і буде націлена контекстна модель контролю доступу.

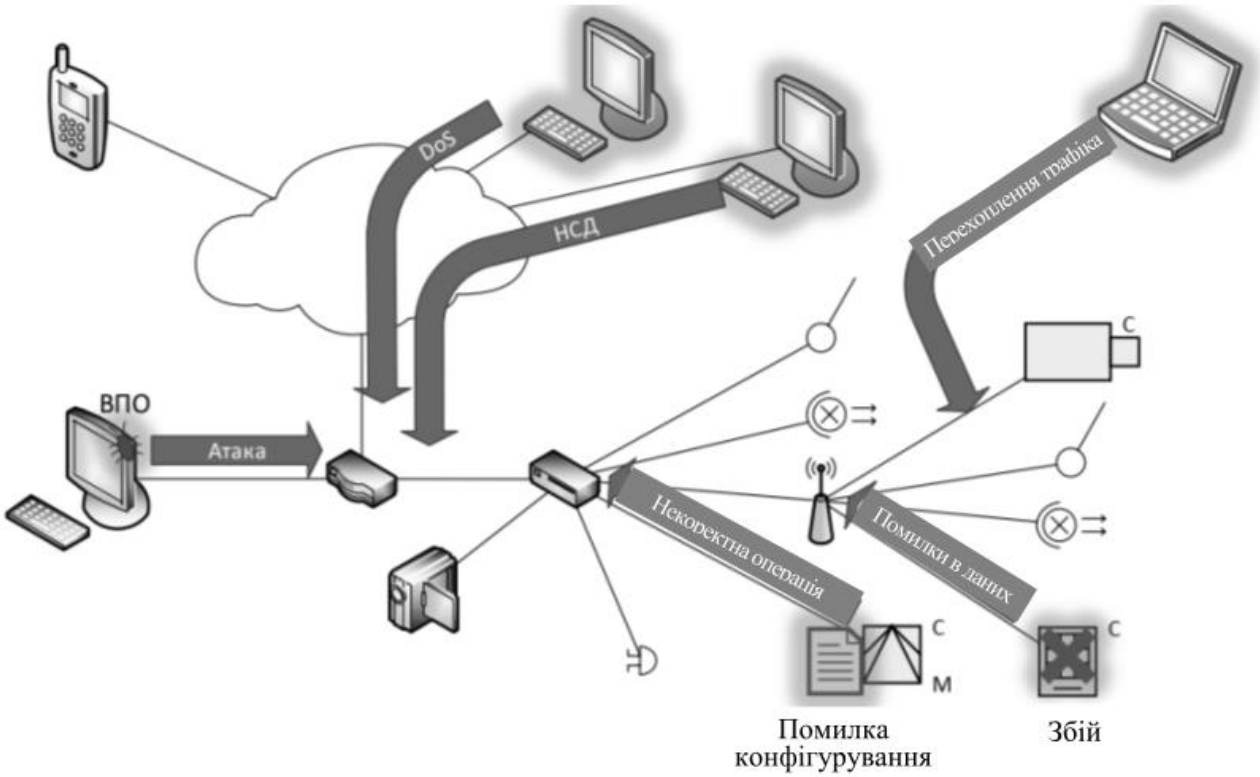

Рисунок 1.3 – Потенційні загрози безпеці системи «розумного будинку»

1.6 Контекстні моделі контролю доступу

Контекстні моделі контролю доступу відрізняються від існуючих моделей, які використовують статичну інформацію про систему, що захищається, тим, що містять методи використання інформації про стан системи в момент виконання операції, що підлягає контролю. Така інформація називається контекстом.

Контекст – сукупний стан пристроїв системи у момент виконання операції. Стан пристрою описується набором його параметрів, доступних для читання сторонніми пристроями. Таким чином, контекст складається з різнорідних елементів, що описують вимірювані параметри системи. Прикладом таких елементів може бути поточний час, розташування пристрою, завдання, що виконуються.

Також, контекст може містити історичні дані про окремі параметри. У такому разі необхідно також зберігати інформацію про зв'язок параметрів для можливості відстеження їх спільної зміни часу. Наявність історичних даних не суперечить визначенню контексту як стану системи в момент виконання операції, оскільки поточний стан, у якому знаходиться система, є результатом певних подій, що відбулися раніше і мають відображення в історії зміни контексту

Одним із важливих завдань, що стоять при розробці контекстних моделей контролю доступу є збір та аналіз контексту. Для отримання можливості застосування контексту з метою контролю доступу необхідно підготувати необроблені дані, які отримують з сенсорів. Можна виділити такі етапи підготовки даних:

- нормалізація даних. Процес приведення даних з різноманітних пристроїв до єдиної форми, придатної для обробки системою контролю доступу;

- фільтрування даних. Процес виділення даних, ознаки яких є суттєві для аналізу;

- кореляція даних. Це є початковий етап підготовки отриманих даних, який полягає у співвіднесенні різних значень цих даних, що залежать один від одного.

2 ЗАСТОСУВАННЯ КОНТЕКСТНОЇ МОДЕЛІ КОНТРОЛЮ ДОСТУПУ ДЛЯ ПОСИЛЕННЯ БЕЗПЕКИ СИСТЕМ «РОЗУМНОГО БУДИНКУ»

2.1 Формальні моделі контролю доступу

Для опису базової рольової моделі потрібно ввести поняття множин суб'єктів *S* та об'єктів *O* доступу. Нехай їх елементи $s_i \in S$, $o_i \in O$.

Суб'єктам призначається множина ролей *R*, в яку входять елементи $r_i \in R$.

Також користувачі можуть виконувати певні операції, які задаються множиною операцій *P* з елементами $p_i \in P$.

При функціонуванні рольової моделі контролю доступу використовуються такі функції:

1) функція отримання списку ролей користувача: *Roles* (s_i)={ролі, призначені користувачу s_i};

2) функція отримання списку операцій, доступних для ролі: Ops(r_i)={операції, пов’язані з роллю r_i};

3) функція отримання допустимих для ролі операцій над об'єктом: *Perms*(r_i, o_j)={операції над o_j, доступні для ролі r_i};

4) функція перевірки можливості виконання операції суб'єктом над об'єктом:

Execute(s_i, o_j, p_k)=$\exists r_m \in$ Roles(s_i): $p_k \in$ Ops(r_m), $p_k \in$ Perms(r_m, o_j).

Перші три функції використовуються для отримання інформації про поточну конфігурацію системи, що використовує дану модель контролю доступу. Остання використовується під час роботи суб'єктів доступу з системою. Саме дана функція застосовується для контролю доступу та визначення можливості виконання суб'єктом запрошеної операції.

Можливе додаткове розширення моделі шляхом додавання ієрархії ролей (рисунок 2.1). Такий механізм спрощує процедуру додавання нових ролей, дозволяючи засновувати їх на вже наявних, та розширювати їх повноваження.

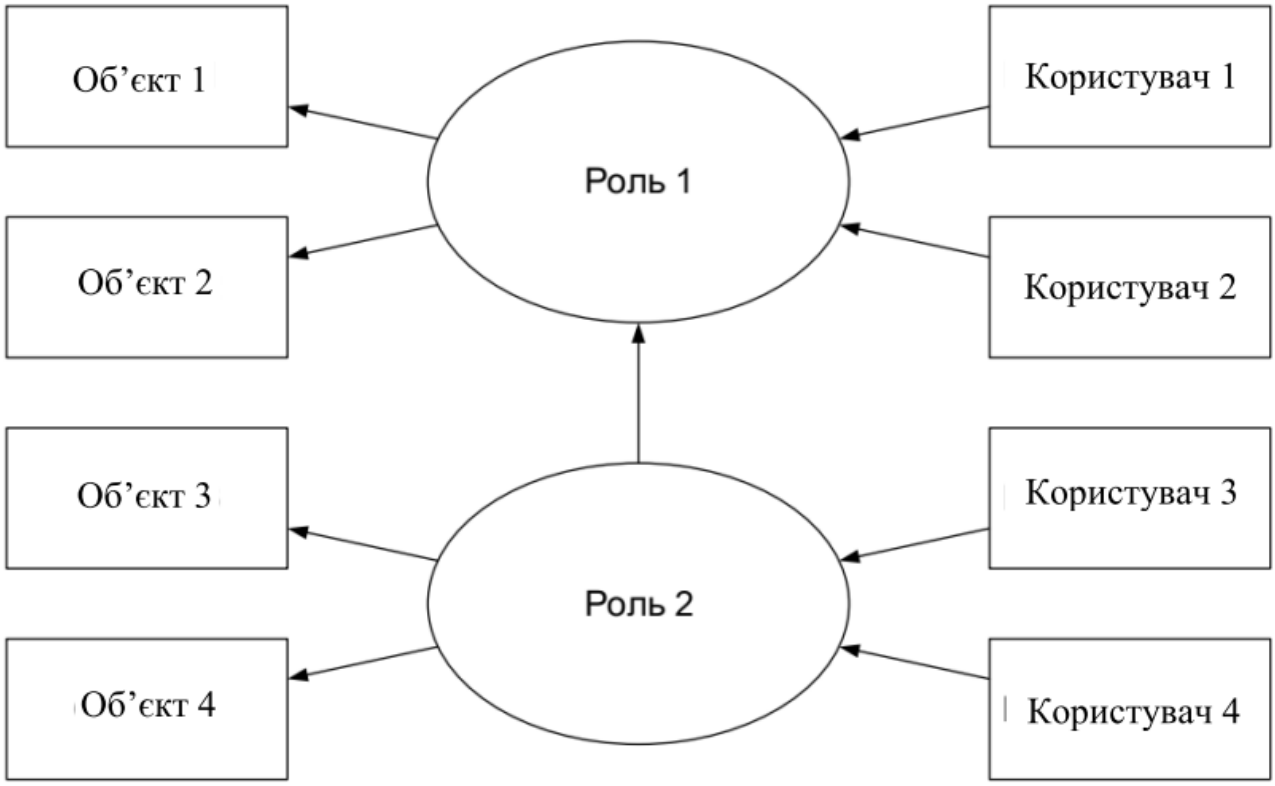

Рисунок 2.1 – Ієрархія ролей у рольовій моделі контролю доступу

На наведеному рисунку 2.1 показаний приклад можливостей, наданих механізмом ієрархії ролей. Так, на основі ролі 1 була створена роль 2. В результаті цього користувачі 3 та 4 мають доступ до об'єктів 3 та 4, а також до тих об'єктів, до яких мають доступ користувачі з призначеною роллю 1.

Для розгляду мандатних моделей були вибрані модель БеллаЛападули та модель Біба.

Модель Белла-Лападули призначена для розмежування доступу до інформації, що захищається, і заснована на правилах документообігу, прийнятих у багатьох державних установах [11].

Формальний опис моделі складається з наступних визначень:

- S – множина суб'єктів доступу, $S=\{s_1, s_2, \ldots, s_k\}$;

- O – множина об'єктів доступу, яка включає в себе множину суб'єктів, $O=\{o_1, o_2, \ldots, o_m, s_1, s_2, \ldots, s_k\}$;

- R – множина прав доступу; визначено два типи доступу – на читання і на запис, тобто R={*read*, *write*};

- L – множина рівнів безпеки, $L=\{l_1, l_2, \ldots, l_n\}$;

- Λ=(L, ≤, ·, ⊗) – сітка рівнів безпеки;

- V – множина станів системи, що складається з упорядкованих пар (F, M), де F: $S \cup O \rightarrow L$ – функція, що зіставляє з суб'єктами та об'єктами рівні секретності, M - матриця прав доступу.

Розглянемо докладніше сітку рівнів безпеки Λ. Вона включає в себе множину рівнів безпеки , оператор часткового нестрогого відношення порядку ≤, оператори отримання найменшої верхньої та найбільшою нижньою меж · і ⊗ відповідно.

Оператори · та ⊗ описуються наступним чином:

- $l_1 \cdot l_2 = l \Leftrightarrow l_1,\ l_2 \le l \wedge \forall l' \in L: (l' \le l) \rightarrow (l' \le l_1 \vee l' \le l_2)$;

- $l_1 \otimes l_2 = l \Leftrightarrow l \le l_1,\ l_2 \wedge \forall l' \in L: (l' \le l_1 \wedge l' \le l_2) \rightarrow (l' \le l)$.

На рисунку 2.2 зображено сітку рівнів безпеки, та відображені допустимі права доступу для суб'єктів різних рівнів.

Безпека моделі Белла-Лападули ґрунтується на двох наступних правилах:

- просте правило безпеки: суб’єкт з рівнем безпеки l_s має доступ *read* до об’єкта з рівнем безпеки l_0 тільки тоді, коли виконується така умова: $l_0 \le l_s$;

- ускладнене правило безпеки: суб’єкт з рівнем безпеки l_s має доступ *write* до об’єкта з рівнем безпеки l_0 тільки тоді, коли виконується така умова: $l_s \le l_0$.

При виконанні тільки цих двох умов стан системи вважається безпечним. Якщо умови виконуються для всіх станів системи, то система вважається безпечною.

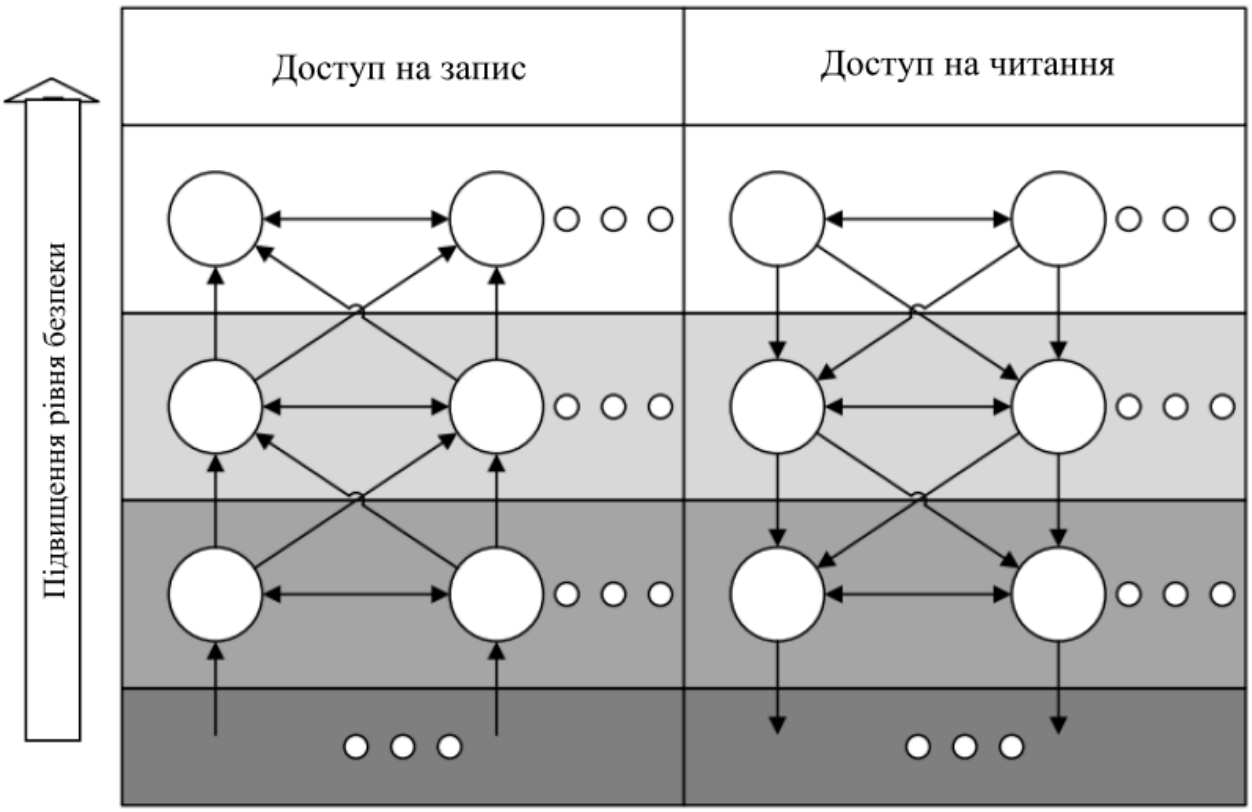

Рисунок 2.2 – Сітка рівнів безпеки

Модель Біба є модифікацією попередньої моделі і визначається аналогічно. При цьому модель орієнтована на забезпечення цілісності даних, а не конфіденційності.

Наведемо короткий опис основних визначень:

- S – множина суб'єктів, $S=\{s_1, s_2, \ldots, s_k\}$;

- O – множина об'єктів, $O=\{o_1, o_2, \ldots, o_m, s_1, s_2, \ldots, s_k\}$;

- R – множина прав доступу, $R=\{read, write\}$;

- L – множина рівнів цілісності, $L=\{l_1, l_2, \ldots, l_n\}$;

- $\Lambda=(L, \leq, \cdot, \otimes)$ – сітка рівнів цілісності.

У моделі Біба також діють два базові правила:

- просте правило цілісності: суб'єкт з рівнем цілісності l_s має доступ *read* до об'єкта з рівнем цілісності l_0 тільки тоді, коли виконується така умова: $l_s \leq l_0$;

- ускладнене правило цілісності: суб'єкт з рівнем цілісності l_s має доступ *write* до об'єкта з рівнем цілісності l_0 тільки тоді, коли виконується така умова: $l_0 \leq l_s$.

За виконання цих двох умов у всіх станах система вважається безпечною.

2.2 Механізми контролю доступу в контекстних моделях

Контроль доступу в контекстних моделях виконується на основі розширених правил, що спираються на контекст. Правила дозволяють уточнювати надані права доступу на основі відомих параметрів контексту. Прикладом мови опису контекстних правил контролю доступу є мова політик контролю доступу.

Контекстна модель розширює рольову і використовує контекст динамічного розподілу ролей. Для цього визначаються три набори правил політики контролю доступу:

1) TrustValue задає рівень довіри користувача щодо елементів контексту, виходячи з їхніх значень;

2) Assign_role виконує розподіл ролей на основі рівнів довіри до окремих елементів контексту;

3) Permissions, як і в класичній рольовій моделі, зіставляє ролі з наборами привілеїв.

Політика контролю доступу має бути складена заздалегідь, ґрунтуючись на умовах і вимогах до системи, що захищається. Особливу увагу варто приділяти складанню правил для задання рівня довіри користувачеві за значеннями контексту.

Процес надання доступу можна подати у вигляді схеми, наведеної на рисунку 2.3.

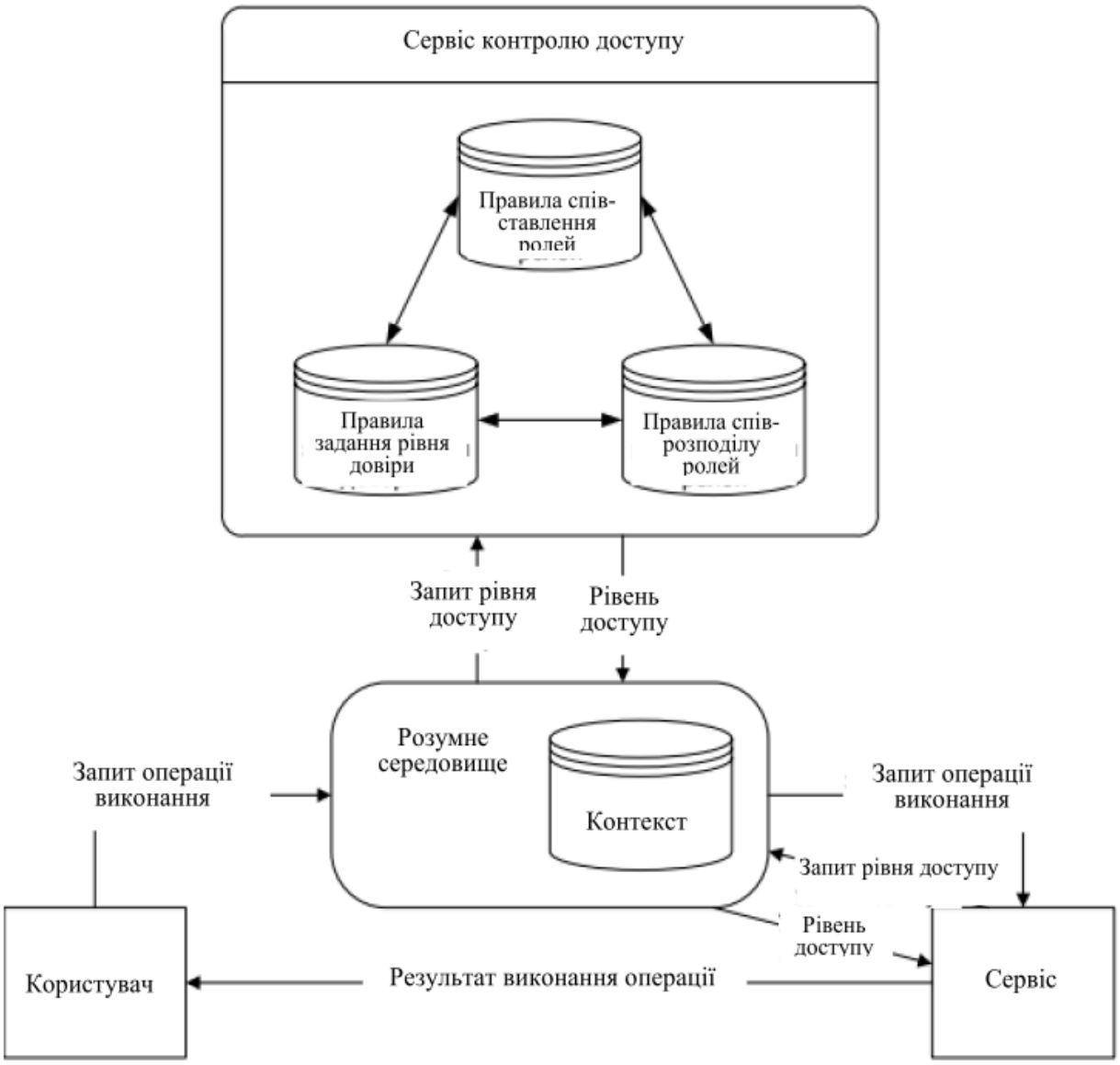

Рисунок 2.3 – Узагальнена архітектура контекстного механізму контролю доступу

На рисунку 2.3 виділені основні компоненти, що беруть участь у процесі отримання доступу. Розглядається типовий сценарій доступу користувача до сервісу, що надається одним із пристроїв, який міститься в «розумному середовищі».

Передбачається, що зв'язок між користувачем та пристроєм проводиться за допомогою спеціального обладнання, що підтримує «розумне середовище» шляхом зв'язування пристроїв у єдину мережу та збору інформації про

контекст. До складу середовища входить брокер доступу, призначений для виконання операцій з перевірки прав користувача.

Користувач сервісу надсилає запит на виконання операції, яка потребує певного рівня доступу. Перед виконанням запиту брокер запитує інформацію про поточні права доступу до сервісу контролю доступу, повідомляючи йому поточний контекст. Сервіс контролю доступу зберігає політику безпеки системи і визначає права доступу за наступним алгоритмом:

1) відбувається перевірка цифрового підпису контексту користувача. Якщо підпис правильний, то відбувається перехід до наступного кроку. В іншому випадку сервіс контролю доступу відмовляє у доступі;

2) за елементами контексту обчислюються рівні довіри користувача. Саме на цьому етапі проводиться аналіз контексту, надалі безпосередні значення елементів контексту використовуватись не будуть;

3) проводиться перевірка можливості присвоєння користувачеві ролей на основі рівнів довіри щодо елементів контексту. Визначається список ролей користувача;

4) на підставі списку ролей виконується перевірка прав доступу до сервісу, що запитується. Результат операції повертається брокеру.

Після цього за наявності доступу виконується запитувана операція. Сервіс отримує інформацію про рівень доступу користувача та повідомляє результат виконання операції.

Застосування контексту породжує нові можливості контролю доступу. Виходячи з опису розглянутої моделі контролю доступу, можна виділити такі переваги контекстних моделей контролю доступу:

- гнучкість налаштування політики контролю доступу;

- адаптація системи до навколишнього середовища.

Такі властивості моделі можуть бути повною мірою задіяні в системах «розумного будинку», оскільки значною мірою відповідають властивостям

самих систем «розумного будинку», що виділяють їх серед інших засобів автоматизації.

2.3 Архітектура системи «розумного будинку» із контекстною моделлю доступу

На цьому етапі доцільно звернути увагу на основні тенденції у побудові систем "розумного будинку", розкриваючи важливі аспекти використання протоколів, таких як Z-Wave та ZigBee. Ці протоколи служать фундаментом для ефективної комунікації між "розумними пристроями".

На сьогоднішній день стратегія, яка здійснюється в побудові систем "розумного будинку", передбачає наявність спеціалізованих центральних вузлів як ключової компоненти. Видатними прикладами таких систем є рішення, що представлені компаніями Philips і Samsung [12]. Ці рішення базуються на використанні спеціальних пристроїв, які виступають як мости між різними "розумними пристроями" та керуючими програмами, використовуючи інтерфейси, які надаються цими мостами.

Незважаючи на те, що мережі, побудовані на основі технологій, подібних до ZigBee, часто вибирається топологія "дерево", яка також підтримується цим протоколом. За такої умови вузли в мережі зазвичай поділяються на три групи:

1) центральний вузол виступає як кореневий пристрій у мережі, він забезпечує основні функції з взаємодії між пристроями та забезпечення безпеки;

2) проміжні вузли, крім виконання функцій автоматизації "розумного будинку", дозволяють розширювати мережу шляхом ретрансляції повідомлень між вузлами;

3) кінцеві вузли виконують різноманітні функції з автоматизації "розумного будинку".

Ілюстрація на рисунку 2.4 наочно демонструє таку мережеву топологію. Проміжні вузли відкривають можливість значно розширювати мережу шляхом послідовного підключення.

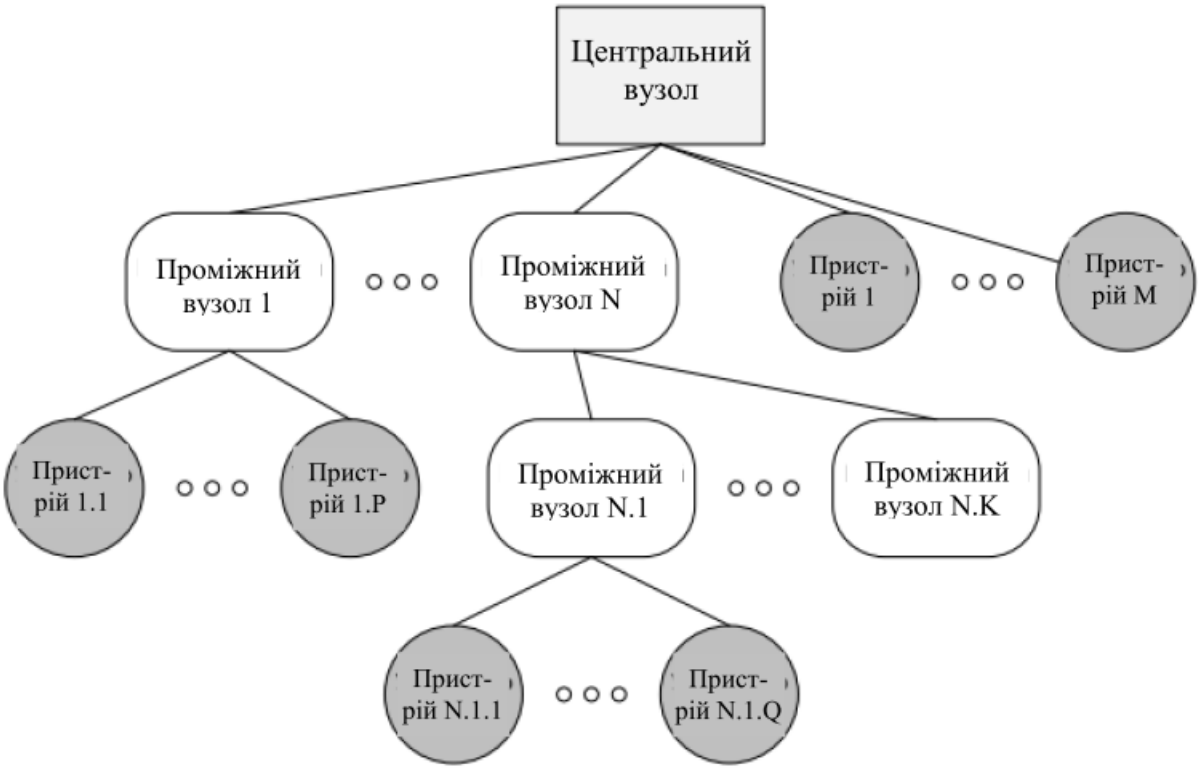

Рисунок 2.4 - Топологія мережі «розумного будинку»

Однією з застосованих концепцій, заснованою на такій топології, є використання шлюзу контролю доступу для централізованого управління доступом у системі "розумного будинку". Цей підхід значно спрощує впровадження контекстного контролю доступу, відповідаючи реальним вимогам і стандартам "розумного будинку". Ілюстрація на рисунку 2.5 показує етапи роботи системи контролю доступу:

1) аналіз мережевої взаємодії, де пристрої взаємодіють через шлюз контролю доступу, спрощуючи завдання;

2) застосування правил контролю доступу, фільтруючи запити між пристроями згідно з встановленими правилами;

3) оновлення контексту на основі попередніх запитів та прямого дослідження пристроїв. Параметри та операції зберігаються для відображення переходу до нового стану;

4) відновлення правил контролю доступу, враховуючи оновлений контекст та політику моделі, для їх подальшого застосування.

Рисунок 2.5 - Процес роботи системи контролю доступу

Щодо шлюзу контролю доступу, то для нього розроблена архітектура, представлена на рисунку 2.6. Основні компоненти шлюзу об'єднуються у трьох підсистемах: зберігання політик і контексту, контролю доступу та взаємодії з мережею.

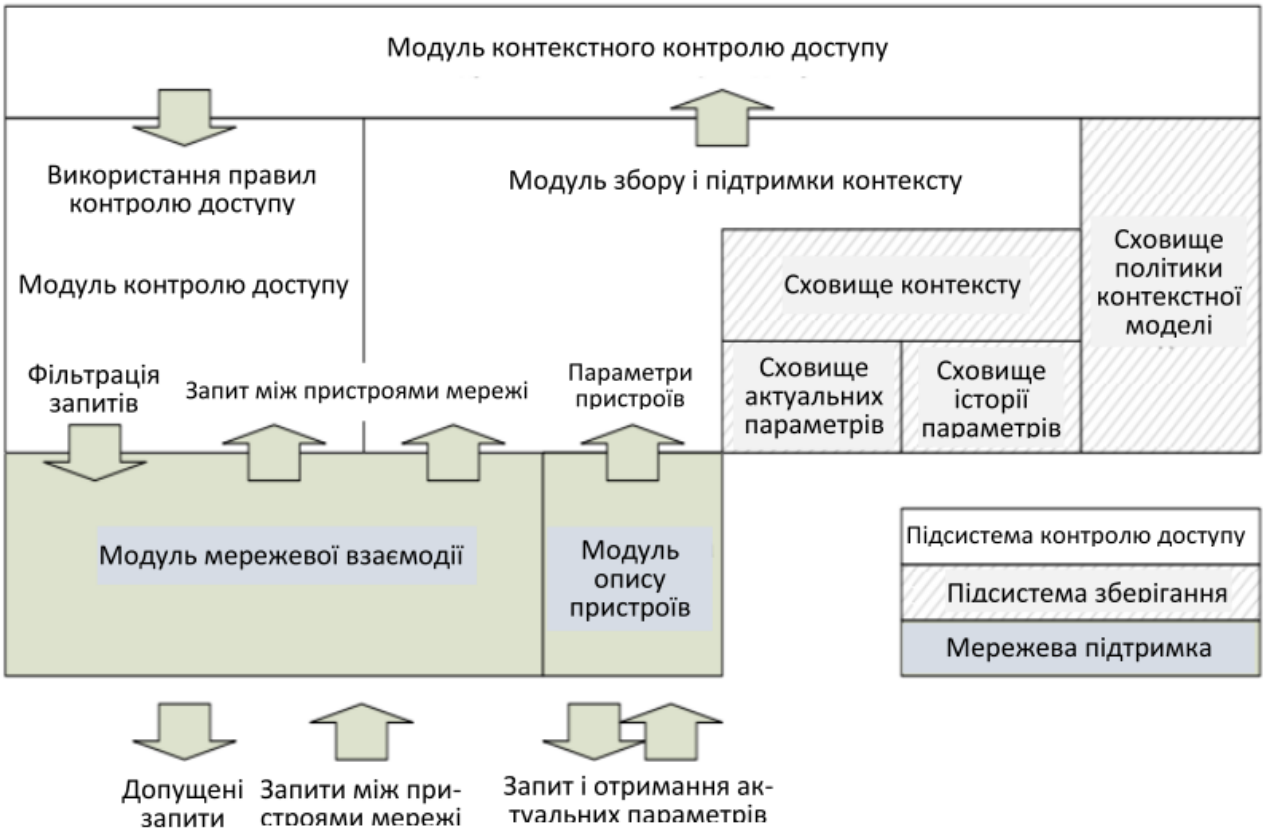

Рисунок 2.6 – Архітектура шлюзу контролю доступу

2.4 Методи збирання та зберігання контексту

Центральною складовою системи, яка впроваджує концепцію контекстної моделі під час контролю доступу, є її підсистема, яка відповідатиме за зберігання та зібрання усього контексту. Завдання, що вирішуються вказаною підсистемою, відображаються на рисунку 2.7. У рамках розглянутої архітектури для системи "розумного будинку" відкривається надзвичайно важлива низка можливостей для виконання цих операцій.

Для розробленої моделі запропоновано декілька способів збору контексту, зокрема, аналізуючи обмін запитами між пристроями; опитуючи пристрої тощо.

Рисунок 2.7 - Основні завдання збору та зберігання контексту

Рисунок 2.7 наглядно демонструє ключові завдання, пов'язані зі збором та зберіганням контексту. Перший спосіб є більш складним у реалізації, проте водночас він ефективніший з точки зору додаткового навантаження на пристрої в мережі "розумного будинку".

Він ґрунтується на тому явищі, що шлюз контролю доступу під час нормальної роботи отримує всі запити між пристроями та відповідає за їх фільтрацію відповідно до правил контролю доступу. Таким чином, шлюз контролю доступу може визначити, чи необхідно виконувати запит та отримати результат виконання. Деталі алгоритму аналізу запитів наведено на рисунку 2.8.

Другий спосіб призначений для отримання параметрів пристроїв, які змінюються без виконання будь-яких запитів. Такими пристроями є різноманітні датчики, параметрами яких можуть бути навіть вимірювані ними величини.

На відміну від першого способу, під час використання якого оновлення контексту відбувається безперервно під час роботи системи, другий вимагає періодичного виконання опитування пристроїв.

Рисунок 2.8 - Алгоритм аналізу запитів для оновлення контекста

2.5 Аналіз безпеки системи «Розумний будинок»

Для аналізу ризиків передбачається підхід з восьми кроків, об’єднаних в чотири фази (рисунок 2.9).

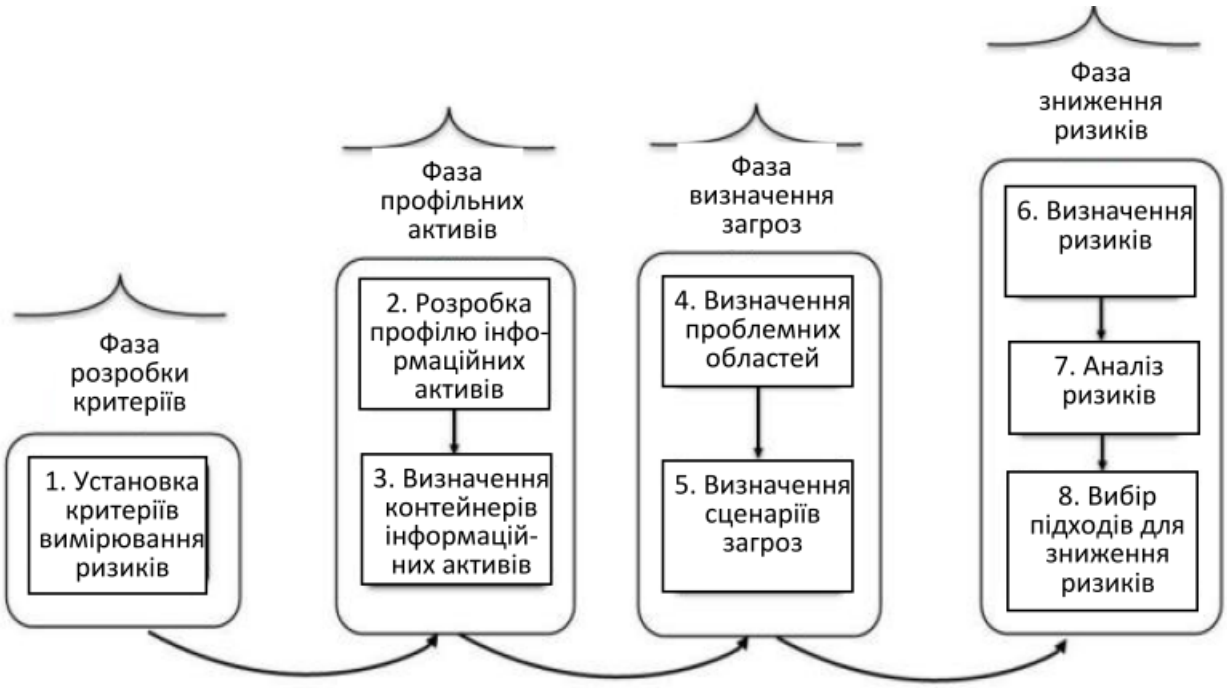

Рисунок 2.9 - Технологічна схема з восьми етапів, які поділяються на чотири основні етапи

Аналіз ризику включає наступні етапи: ідентифікацію ризику (визначення активів, визначення погроз, визначення існуючих заходів та засобів контролю та управління, виявлення вразливостей, визначення наслідків) та встановлення значення ризику (оцінка наслідків, оцінка ймовірності інциденту; встановлення значень рівня ризиків). Оцінка ризиків має ідентифікувати ризики, визначити кількість та пріоритети ризиків на основі критеріїв для прийняття ризику та цілей, значимих для забезпечення безпеки системи.

Загальний алгоритм дій групи аналізу ризиків виглядає наступним чином. На кроці 1 необхідно визначити критерії оцінки ризиків інформаційної безпеки, тобто сукупність якісних показників, які дозволять встановити значення оцінки ризику та наслідки його реалізації. Без введення таких критеріїв неможливо оцінити залежність системи від тих чи інших ризиків.

Крок 2 починається зі складання переліку інформаційних активів та визначення їхнього профілю. Профіль активу являє собою вхідні дані для наступних кроків та є основою для виявлення загроз та ризиків.

Далі виконується крок 3. Інформаційні активи можуть зберігатися не тільки в самій системі «Розумний дім», а й поза її межами. Домовласник може допускати до обслуговування своєї інфраструктури інші організації-постачальники послуг. Якщо такий постачальник послуг не виконує вимог безпеки активів, до обслуговування яких він допущений, то це само собою несе ризик. Ризик може міститися в самому факті зберігання, передачі або активації в сторонньому місці. Це порушує захист інформаційного активу. Ще більшу загрозу несе залучення таким постачальником послуг субпідрядників, про яких власник активу може і не знати. Таким чином, для отримання адекватного профілю активу важливо визначлити всі місця зберігання, передачі та обробки активу – контейнери, а також зрозуміти, чи знаходиться він у зоні прямого управління організацією. Місцем зберігання активу може бути технічний засіб, програмне забезпечення, паперовий носій чи співробітник організації. Причому люди тут особливо важливі, оскільки при отриманні інформації, що захищається, вони стають "контейнерами" активу. Такі ризики потрібно вчасно виявляти.

На кроці 4 виявляються проблемні області в інформаційній безпеці розумного будинку. Метою кроку 4 є не складання повного переліку всіх можливих загроз, а оперативне визначення тих загроз, які одночасно очевидні для аналітика.

У кроці 5, на основі виявлених проблемних областей, складаються сценарії загроз. Цей крок дозволяє врахувати ймовірність реалізації загроз, що допомагає на більш пізніх кроках розробити заходи щодо зниження ризику. Як правило, в цьому випадку використовується якісна шкала і вводиться три рівні ймовірності реалізації загрози: висока, середня і низька.

На кроці 6 після визначення загроз та виявлення наслідків їх реалізації, визначають ризики інформаційної безпеки. Необхідно визначити, як саме ризик буде впливати на систему «Розумний дім» загалом, при цьому ризик визначається для кожного активу, щоб оцінити його критичність для функціонування. Для кожного ризику визначається не менше одного наслідку.

На кроці 7 визначається кількісна міра шкоди, яка буде нанесена системі «Розумний дім» під час реалізації загрози. Це відносна оцінка, що дозволяє розставити ризики за пріоритетом.

На заключному кроці вибираються міри обробки визначених ризиків з врахуванням їх пріоритету.

3 МОДЕЛЮВАННЯ СИСТЕМИ «РОЗУМНОГО БУДИНКУ» ТА АТАК НА СИСТЕМУ

3.1 Метод та політика контролю доступу

Для розробки моделі контролю доступу вибрано модель цілісності Біба. Вибір цієї моделі був здійснений на підставі наступних вимог:

- модель контролю доступу має давати можливість групувати пристрої за різними правами доступу;

- процес зміни прав доступу окремих суб'єктів має бути простим, щоб його можна було виконати автоматично;

- початкове конфігурування системи повинно бути мінімальним, аби не ускладнювати політику контекстної моделі.

Хоча усі розглянуті моделі деякою мірою відповідають першим двом вимогам, важливо зазначити, що перерозподіл суб'єктів за ролями може виявитись більш трудомістким у випадку моделей, ніж просто призначення рівнів доступу.

Вирішальну роль у виборі моделі відіграла остання вимога. Для моделі мандатного доступу потрібно лише вказати кількість рівнів доступу та їх відношення. Рольова модель, натомість, вимагає визначення ролей, їх повноважень, конкретних випадків, ієрархії ролей, що створює значну конфігураційну навантаженість.

Із моделей мандатного доступу було обрано модель цілісності Біба. Запропонований підхід до забезпечення захисту від скомпрометованих пристроїв полягає в накладанні обмежень на окремі пристрої, щоб уникнути виконання операцій, які можуть потенційно зашкодити безпеці системи. Це вказує на можливість використання рівнів цілісності пристроїв для реалізації такого підходу.

Контроль доступу в системі реалізований на основі моделі мандатного доступу. Запропонована модель є гібридною, оскільки вона розширює мандатну

модель за рахунок додаткового механізму динамічного призначення рівнів з урахуванням контексту.

На зручність застосування моделі контролю доступу впливає підхід до задання політик контролю доступу. У запропонованій моделі політики представляються у вигляді двох груп правил:

- обмеження на параметри системи за умовами;

- допустимі операції суб'єктів над об'єктами.

Правила, що описують допустимі операції суб'єктів об'єктами, мають такий вигляд: *Execute* (*s*, *o*, *a*), де *s* - суб'єкт, *o* - об'єкт, *a* - операція.

Операція *a* входить до множини операцій *A*, допустимих до виконання над об'єктом *o*. Для отримання цієї та іншої, пов'язаної з об'єктом, інформації, визначено наступні функції:

Operations (*o*)={операції, допустимі над об'єктом *o*};

Description (*o*, *a*)={зміни параметрів *o* після операції *a*}.

Перша функція є довідковою та служить для перевірки коректності правил. Друга функція використовується для аналізу контексту для визначення конфліктів, що виявляються при потенційному виконанні операцій.

У пропонованій моделі висувається припущення, що правила доступу визначаються пристроями, що додаються в систему. Таким чином можна позбутися необхідності задання конфігурації системи контролю доступу вручну, що важливо для таких застосувань, як забезпечення безпеки «розумного дому». Для досягнення цього пристрої поділяються на попередньо задані класи з певними наборами операцій, які можуть надавати. Після цього кожен пристрій забезпечується списком правил доступу термінах класів пристроїв.

При підключенні нового пристрою до системи «розумного будинку» відбувається процес оновлення політики контролю доступу. Як показано на рисунку 3.1, процес полягає в об'єднанні списків правил пристроїв системи.

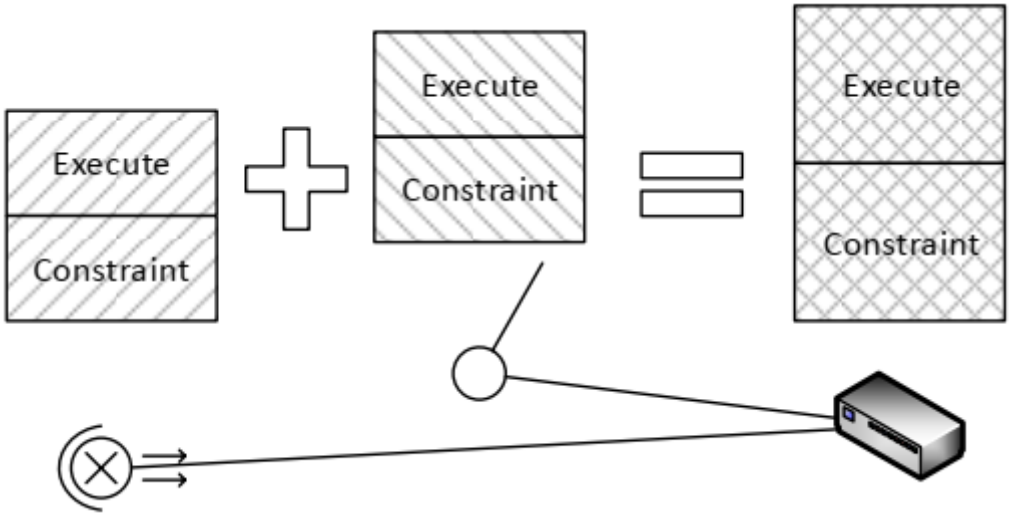

Рисунок 3.1 – Формування правил контролю доступу

Обмеження на параметри задаються однією з наступних форм:

Constraint (*context_condition*, *param*, *value_expression*);

Constraint (*context_condition*, *conditional_expression*).

Перша форма дозволяє вказувати жорстко задане значення, яке повинен приймати параметр *param* при виконанні умови *context_condition*. У цій формі правил також дозволяється визначення нових елементів контексту на основі визначених пристроями системи.

Друга форма служить для накладання довільних обмежень *conditional_expression* на елементи контексту. Обмеження на елементи контексту є фрагментами опису безпечного стану системи "розумного будинку".

3.2 Алгоритми функціонування системи

Алгоритм аналізу контексту призначений для пошуку протиріч, що виникають у системі «розумного будинку». На вхід алгоритм аналізу контексту отримує політику контролю доступу та актуальний контекст. Блок-схему алгоритму наведено на рисунку 3.2.

Рисунок 3.2 – Блок-схема алгоритму аналізу контексту

Для коректної роботи контекстної моделі контролю доступу важливі не тільки збір, зберігання та періодичне оновлення контексту. На роботу системи безпеки багато в чому впливають алгоритми подальшої обробки зібраної інформації та складання правил контролю доступу.

Основним завданням аналізу контексту у розробленій моделі контролю доступу є виявлення протиріч між потенційно можливими операціями в системі «розумного будинку» із встановленими обмеженнями на контекст. Тому алгоритм аналізу контексту служить для визначення списку чинних обмежень *Constraint* та правил типу *Execute* (*s, o, a*), які суперечать чинним обмеженням. Схематично цей процес зображений на рисунку 3.3.

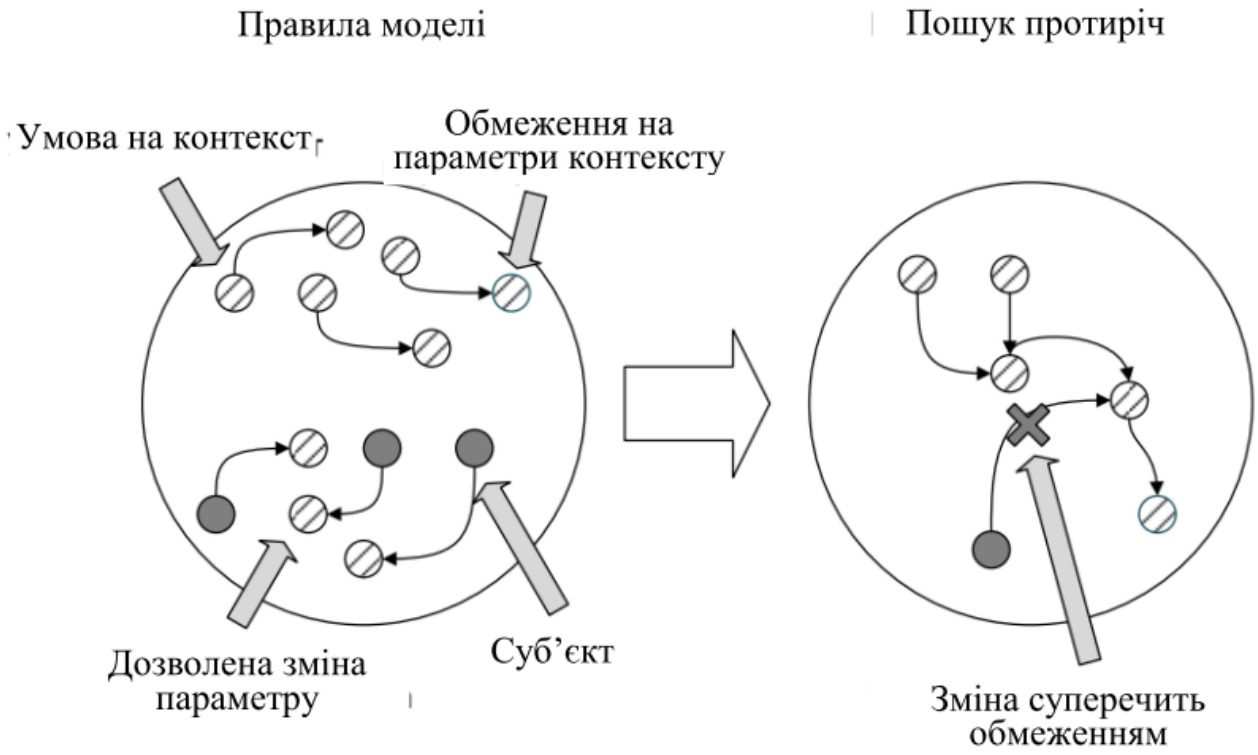

Рисунок 3.3 - Процес аналізу контекста

Важливою особливістю є те, що правила типу *Constraint* (*condition, parameter, value_expression*) дозволяють доповнювати контекст новими параметрами, що обчислюються. Така можливість дозволяє створювати складні

ланцюжки правил, які можуть доповнюватися правилами нових пристроїв, що вводяться до системи.

Цю ж особливість необхідно враховувати під час проведення аналізу контексту. Для опису алгоритму з огляду на це вводиться поняття задіяного правила *Constraint*.

На початку роботи алгоритму проводиться складання списку правил *Constraint*, що підлягають обробці. Спочатку список складається з усіх правил, присутніх у системі. Задіяним правилом *Constraint* (*condition*, *parameter*, *value_expression*) називається правило зі списку, належних до обробки, умова *condition* якого виконується у поточному контексті. Таке правило застосовується безпосередньо при залученні. Подальші дії залежить від типу правила.

Якщо це правило має вигляд *Constraint* (*condition*, *parameter*, *value_expression*), тоді в контекст додається новий параметр *parameter* із значенням, що отримується в результаті обчислення *value_expression*. Якщо такий параметр уже присутній у контексті, то нове значення додається до списку можливих значень. Також нове значення додається до списку обмежень на контекст. Суперечності на цьому етапі не визначаються, оскільки вони впливають призначення рівнів цілісності.

Якщо задіяне правило, що має вигляд *Constraint* (*condition*, *conditional_expression*), тоді умова додається до списку обмежень на контекст.

Після застосування правила воно виключається зі списку правил, що підлягають обробці. Описаний процес повторюється доти, доки на наступній ітерації у списку оброблюваних правил не будуть відсутні задіяні правила.

Подальша обробка складеного списку обмежень на контекст полягає у визначенні правил Execute, що порушують ці обмеження. Для цього для кожного правила *Execute* (*s*, *o*, *a*), що використовується в системі, виконується перевірка змін параметрів з використанням функції *Description* (*o*, *a*).

Усі правила, виконання операцій згідно яким буде порушувати умови, накладені на контекст, додаються до списке правил, що викликають протиріччя.

Результатом роботи алгоритму є список обмежень на контекст та список правил доступу, що суперечать їм.

Виконання алгоритму призначення рівнів цілісності є заключним етапом роботи розробленої контекстної моделі контролю доступу під час оновлення стану.

На вхід алгоритм отримує політику контекстної моделі та список правил доступу, що суперечать обмеженням контексту. На основі даного списку визначається множина пристроїв, яким необхідно заборонити доступ, та множина пристроїв, доступ до яких потрібно заборонити, щоб усунути протиріччя з контекстом.

Зміна правил контролю доступу вибирається на користь такої зміни, що призводить до найменшого впливу на систему у вигляді кількості заборонених операцій. Блок-схему алгоритму наведено рисунку 3.4.

3.3 Моделювання системи «розумного будинку»

Для оцінки ефективності розробленої системи забезпечення безпеки в сфері "розумного будинку" було проведено моделювання та подальше тестування цієї системи. Створена модель "розумного будинку", яка складається з пристроїв різних класів. Для реалізації моделі використано мову програмування Python. Це мова загального призначення, яка відома своєю здатністю до швидкого прототипування [13]. Для моделювання обрано бібліотеку дискретно-подійної симуляції SimPy [14]. Ця бібліотека використовує інтерфейс генераторів мови Python та дозволяє симулювати багатоагентні системи за допомогою кооперативної багатозадачності, створюючи агентів у вигляді співпрограм.

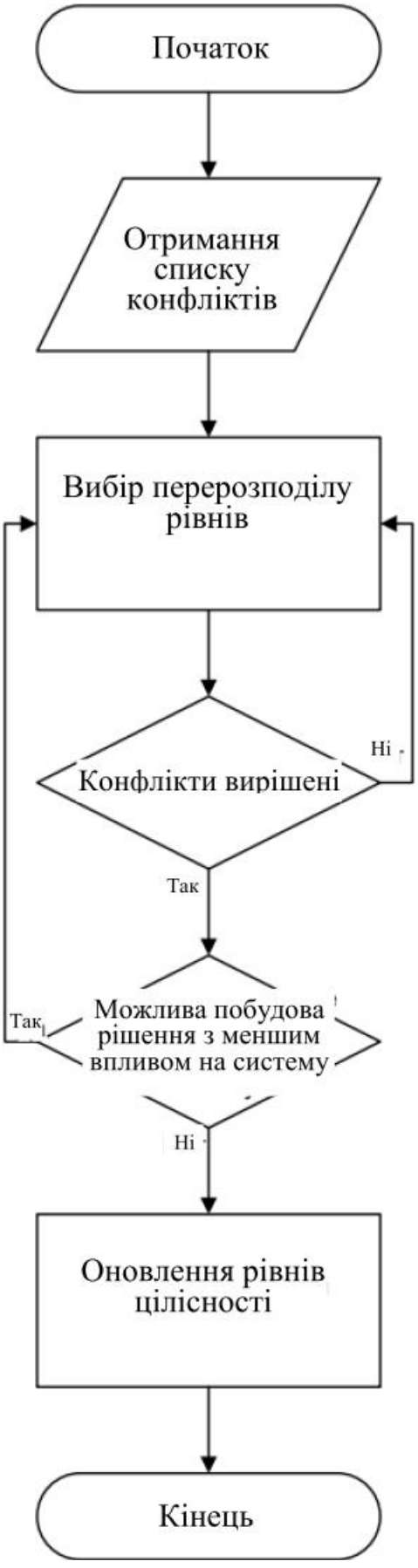

Рисунок 3.4 - Алгоритм перерозподілу рівнів

У процесі розробки системи "розумного будинку" було збережено опис цієї системи у json-форматі, де було вказано пристрої, що входять до складу системи, їх характеристики та дозволені операції над ними (Operations), включаючи опис функцій (Description) (о, а). Конфігурація модельованої системи наведена на рисунку 3.5.

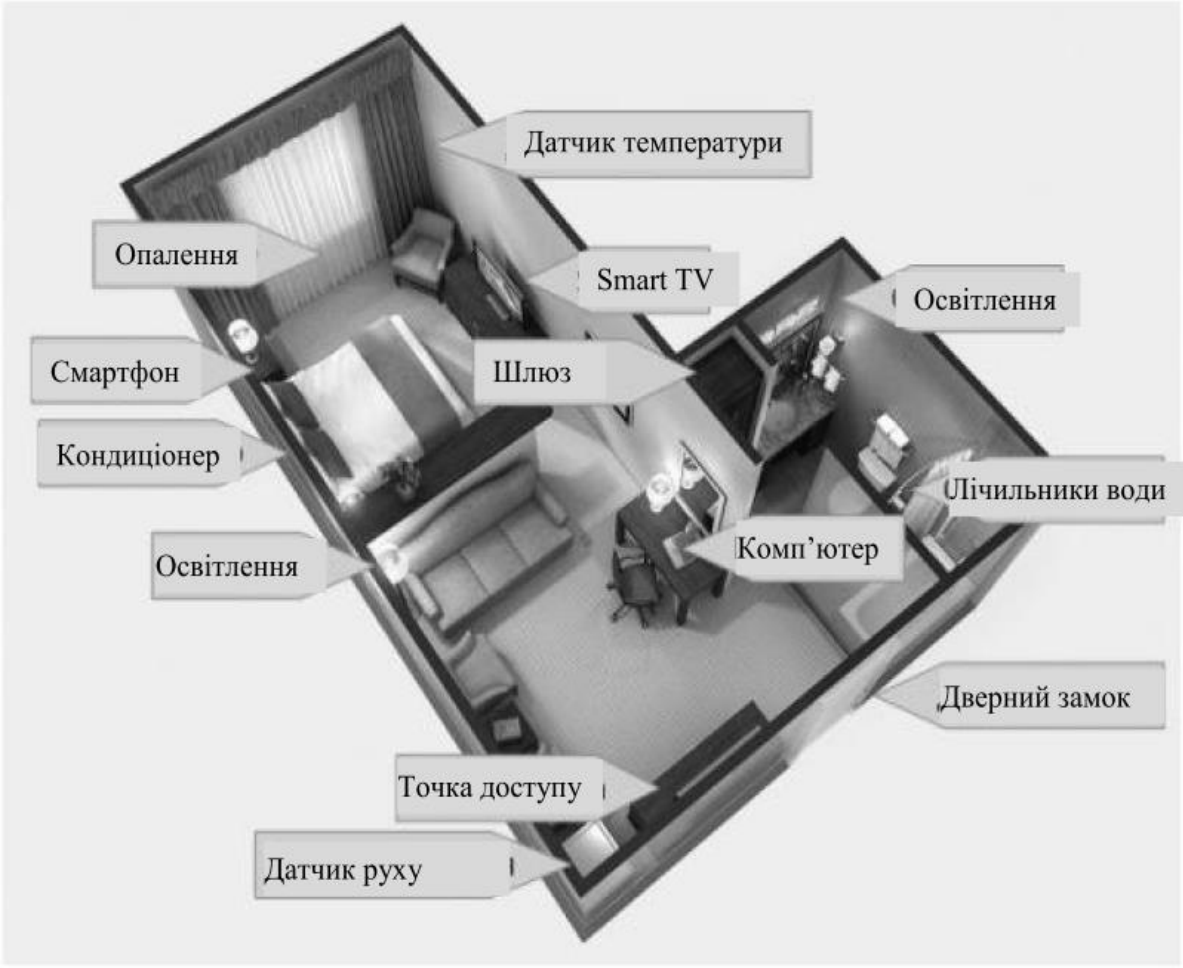

Рисунок 3.5 - Склад модельованої системи «розумного будинку»

Зазначимо, що програмний макет системи не враховує мережевий рівень. Моделюванню підлягає лише шлюз контролю доступу, який відповідає за обробку та зберігання контексту та контроль доступу. З використанням бібліотеки SimPy ми можемо відтворити сценарій, в якому відбувається обмін запитами між пристроями.

Поглибимо наше розглядання сценарію, який демонструє базові можливості захисту. Уявімо, що є скомпрометований смартфон, за допомогою якого можливе відкриття дверного замка. Щоб обмежити можливості зловмисника, було створено правило, яке передбачає підвищення рівня цілісності дверного замка в разі відповідних умов, таких як час, відсутність руху та освітлення. Таким чином, відкриття замка за допомогою скомпрометованого смартфона можливе лише для певної особи.

Під час процесу моделювання даного сценарію використовуються правила контекстної моделі, які допомагають забезпечити безпеку та визначити параметри доступу до пристроїв:

```
Constraint(світло == true, людина_в_приміщенні, true)
Constraint(рух == true, людина_в_приміщенні, true)
Constraint(людина_в_приміщенні == false and (01:00 <= час<=
07:00), двері_закриті == true)
Execute(смартфон, двері, відкрити)
Execute(смартфон, освітлення, включити)
Execute(двері, двері, відкрити)
Description(двері, відкрити) -> {двері_закриті: false}
```

Прийняте рішення, що базується на встановлених правилах, проявляється таким чином:

1) якщо освітлення вимкнене та відсутній рух, контекст зберігає інформацію про відсутність людини у приміщенні;

2) враховуючи час та відсутність людини, обмежується стан дверей. В даному контексті двері повинні бути закриті;

3) відкриття дверей викликає порушення контексту, оскільки змінює контекст недопустимим чином. Ситуація потребує вирішення конфлікту, що виникає через можливість відкриття дверей через смартфон;

4) конфлікт можна вирішити, знижуючи рівень цілісності смартфона або підвищуючи рівень цілісності дверного замка. Оскільки зниження рівня цілісності смартфона може призвести до обмеження інших дій, які не викликають конфлікту, рішення приймається на користь підвищення цілісності замка.

Також маємо інший сценарій, пов'язаний із системою керування кліматом "розумного будинку". Випадок одночасного включення опалення та кондиціонування при відсутності людей у приміщенні розцінюється як помилка управління. Рівень цілісності комп'ютера знижується з метою мінімізації наступних впливів. Для цього застосовуються наступні правила:

```
Constraint(світло == true, людина_в_приміщенні, true)
Constraint(рух == true, людина_в_приміщенні, true)
Constraint(опалення == true and людина_в_приміщенні ==false,
кондиціонер == false)
Execute(комп'ютер, опалення, включити)
Execute(комп'ютер, кондиціонер, включити)
Description(опалення, включити) -> {опалення == true}
Description(кондиціонер, включити) -> {кондиціонер == true}
```

В даному випадку прийняття рішення про роботу приладів проходить наступним чином:

1) оскільки світло вимкнене та відсутній рух, контекст фіксує відсутність людини у приміщенні;

2) враховуючи стан опалення та відсутність людини, встановлюється обмеження для кондиціонера;

3) включення кондиціонера викликає порушення контексту. У даному випадку приймається рішення знизити рівень цілісності комп'ютера.

Розроблений програмний макет системи забезпечення безпеки для "розумного будинку" демонструє її ефективність у модельних сценаріях,

пов'язаних із компрометацією пристроїв та програмними збоями. Важливо зазначити, що вплив впроваджених механізмів забезпечення безпеки на продуктивність системи контролю доступу може бути складно визначити за допомогою моделювання. Тим не менше, розроблена архітектура шлюзу контролю доступу ретельно ураховує необхідність забезпечення продуктивності системи.

Під час обробки запитів між пристроями використовуються лише правила контролю доступу, без повного аналізу контексту. Аналіз контексту виконується окремо в шлюзі контролю доступу і впливає на обробку запитів лише після оновлення правил контролю доступу.

3.4 Моделювання атак на систему «Розумний будинок»

На рисунку 3.6 представлена загальна платформа системи моделювання. Ця платформа зараз реалізує конфігурацію All in Home. У поточному розгортанні всі основні компоненти системи знаходяться на домашньому шлюзі, а хмарний сервер використовується тільки для узгодження енергоспоживання між різними розумними будинками Домашній шлюз контролює основні компоненти, які відповідають за управління розумним будинком, такі як інтеграція пристрою та Multi Agent System (MAS). Електричні пристрої з'єднані з домашнім шлюзом через спеціальні драйвери.

Далі проводиться настроювання віртуального середовища CoSSMic. В якості тестового середовища використовується Raspberry Pi 2 Моделі B. Крім Raspberry Pi, також необхідне наступне допоміжне обладнання для Raspberry Pi: блок живлення, кабель HDMI, SD карти (16 Гб), Ethernet кабель; монітор чи телевізор; клавіатура; HomeMatic бездротова смарт розетка, HM-ES-PMSw1-PI; модуль USB CC1101 V3; лампа для тестування результатів; PC, смартфон або планшетний браузер. Необхідне програмне забезпечення: підготовлений образ

Raspbian Jessie, що містить більшість оновлень, внесених до ОС; PuTTY; Win32DiskWriter. Програмні компоненти: EmonCMS; Драйвер CUL.

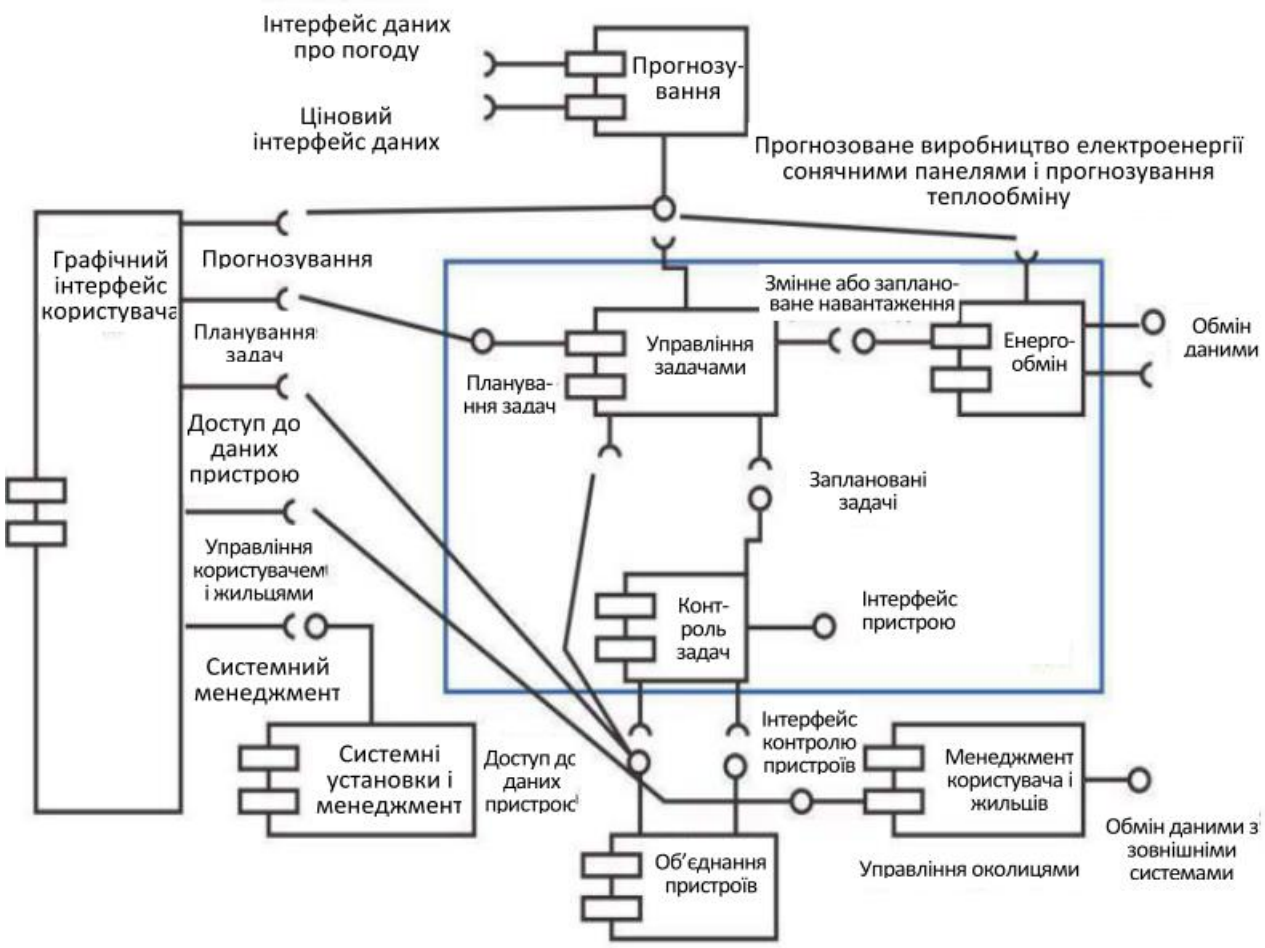

Рисунок 3.6 Загальна платформа системи моделювання

Перед підключенням вищезгаданих складових до Raspberry Pi підготовлений образ записується на SD-карту та виконуються подальші налаштування CoSSMic. Також використовується кабель для подовження живлення HomeMatic та Raspberry Pi. Це обладнання може бути підключено безпосередньо до розетки живлення. Лампа підключається до смарт-розетки HomeMatic та USB CC1101 до Raspberry Pi через його USB порт. Тепер можна отримати доступ до веб-застосунку з браузера на ПК або смартфоні, ввівши наступну URL-адреса в адресному рядку: http://129.241.208.197/emoncms.

Увійдемо в систему з ім'ям UK02 та паролем uktestpass25, які задаються під час встановлення EmonCMS.

Після налаштування обладнання та програмного забезпечення потрібно запустити систему, яка імітуватиме дії зловмисника. Для цього скористаємося наступним обладнанням та програмним забезпеченням: операційною системою Kali Linux, апаратним прийомопередатчиком на 868 МГц, сканером безпеки OWASP ZAP, для захоплення основних даних з метою здійснення основних атак використовуємо TCPDump, інструментом Wireshark як аналізатором протоколів.

Захоплення облікових даних користувача здійснюється при запуску готової моделі розумного будинку. Використовується мережевий перехоплювач Wireshark та аналізатор TCPdump. Шукана конфіденційна інформація відправляється у вигляді простого тексту по мережі. Це дозволяє зловмиснику легко перехопити ці дані, виявивши мережевий трафік і здійснивши сніффінг атаку. Результати атаки представлені нижче на рисунку 3.7.

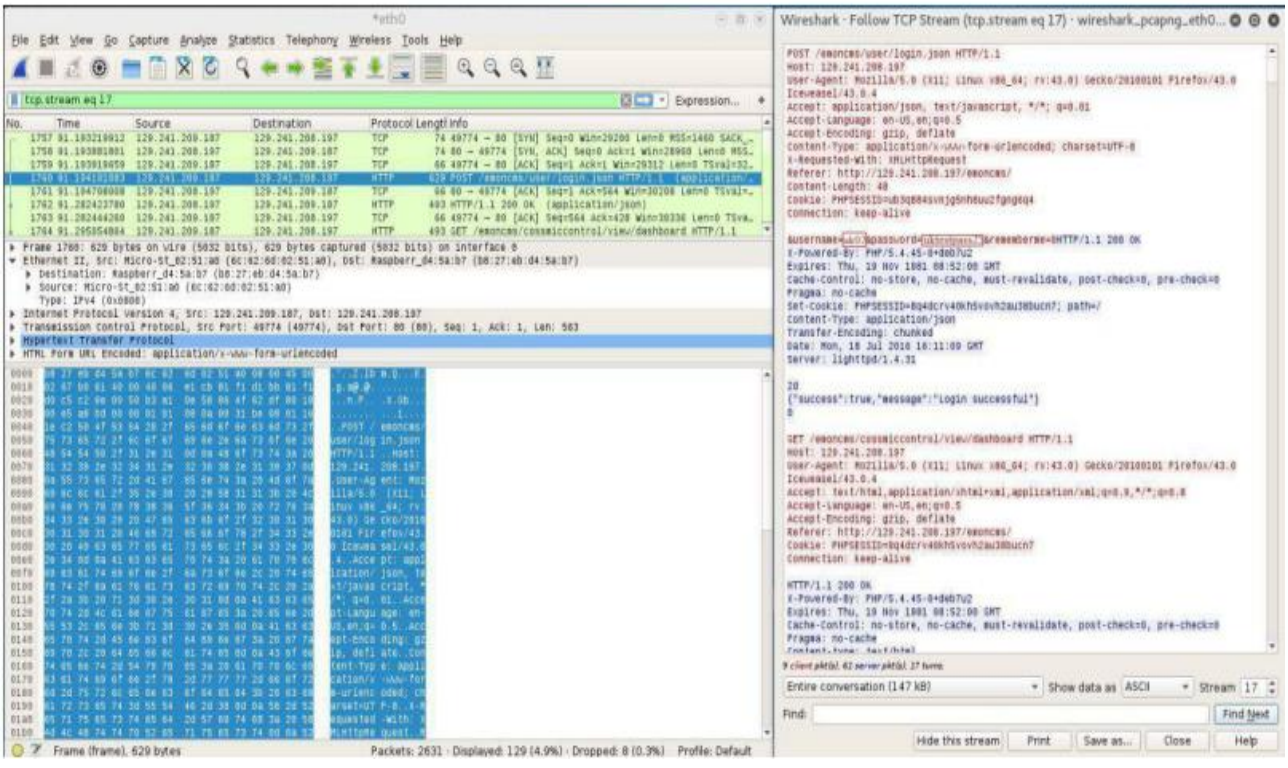

Рисунок 3.7 – Діалогове вікно програми

Тепер, після отримання знань про активний обліковий запис в системі, можна легко обійти механізм аутентифікації і ввійти в розумний будинок, не будучи санкціонованим користувачем.

Далі розглядається ClickJacking атака. Параметр X-FRAME-OPTIONS заголовка не заданий на деяких веб-сторінках згідно результатів аналізу ZAP. Змоделювати ClickJacking атаку можна шляхом запуску сценарію, як показано на рисунку 3.8.

Рисунок 3.8 - Діалогове вікно програми «Скрипт для моделювання ClickJacking атаки»

Веб-інтерфейс CoSSMic може бути вбудований в інший сайт, що робить його вразливим для ClickJacking атак.

Серед можливих вразливостей знайдена проблема віддаленого управління пристроями без авторизації. Зловмисник може легко управляти пристроями, підключеними до HomeMatic смарт-розетки, будучи неавторизованим в системі. Крім того, всіма пристроями, підключеними до смарт-розетки, можна управляти за допомогою HTTP GET запиту. Атакуючий може ввести URL в браузері (рисунок 3.9) і таким чином включити/відключити смарт-розетку.

Рисунок 3.9 – Вікно адресного рядка браузера «API-ключ доданий в URL»

Коли зловмисник введе цю URL-адресу, він зробить систему недоступною. Параметр status в URL-адресі приймає як значення символ, який є допустимим значенням для введення. Статус може приймати тільки цифри як значення. Спостереження показує, що смарт-розетка вимикається, як показано на рисунку 3.10, коли параметру status було надано значення 0, і включається, як показано на рисунку 3.11, коли параметру status було надано будь-яке інше число (не тільки 1). Авторизованому користувачеві не потрібно перемикати пристрій через URL-адресу, оскільки вона може використовувати кнопку у веб-інтерфейсі. Зловмиснику не потрібно входити в систему, оскільки він може використовувати API ключі від сніфінгу атаки. Після цього система не буде реагувати на запити користувачів і домашній шлюз потрібно фізично перезавантажити, щоб відновити функціонування та доступ до системи.

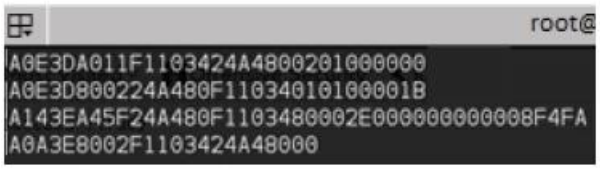

Рисунок 3.10 – Діалогове вікно програми Terminal Linux: «Пакетні дані, отримані після команди виключення»

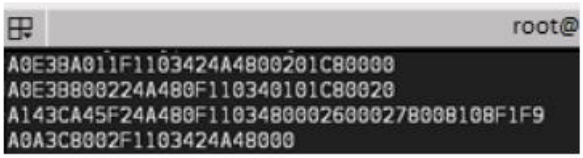

Рисунок 3.11 – Діалогове вікно програми Terminal Linux: «Пакетні дані, отримані після команди включення»

Зловмисник може легко перехопити та прослухати трафік між домашнім шлюзом (Raspberry Pi) та розумним штекером HomeMatic HM-ES-PMSw1-PI, так як з'єднання між смарт-розеткою HomeMatic та розумним будинком не

зашифровано. Пакетні дані для віддаленого керування смарт-розетками можуть бути отримані за допомогою терміналу Linux.

Продемонстровані атаки показують, як зловмисник може перехопити контроль і віддалено керувати великою частиною системи «Розумний будинок», має можливість непомітного проникнення в приміщення, управління електроенергією, може контролювати та підміняти дані в системі обліку та брати на себе несанкціоноване повне управління системою "Розумний будинок".

ВИСНОВКИ

1. Здійснено аналіз основних типів технологій «розумного середовища» та «розумного будинку», що дозволило встановити основні типи загроз на систему та способи захисту від них.

2. Розроблено математичне та алгоритмічне забезпечення системи «розумного будинку» із контекстною моделлю доступу, що дозволило побудувати відповідні моделі «розумного будинку».

3. На основі побудованих моделей «розумного будинку» розроблено алгоритм функціонування системи захисту, що дозволило дослідити основні методи захисту від атак.

4. Розроблено архітектуру системи «розумного будинку» із контекстною моделлю доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дужак І.О. Розумний будинок. Автоматизація технологічних і бізнес-процесів. Одеська національна академія харчових технологій. 2013. №13. С. 31.
2. Бондарев О. Хто в домі господар. Розумні будинки через кілька років набудуть широкої популярності. Кореспондент. 2012. №30. С. 42–46.
3. Менахем Домб. Системи розумного дому, заснованого на основі інтернет речей. URL: https://www.intechopen.com/books/internet-of-things-iot-for-automated-andsmart-applications/smart-home-systems-based-on-internet-of-things (дата звернення 03.09.2019).
4. Огляд готових рішень систем «Розумний дім». URL: https://sprut.ai/client/article/1544.
5. Saha, S., Ishraque, H., Islam, M.T., & Rahman, M.A. IoT based smart home automation and energy management. In 2019 Thesis & Report, BSc (Electrical and Electronic Engineering) (Department of Electrical and Electronic Engineering, Brac University). (2019). P. 85.
6. Jiang L., Liu D.Y., Yang B. Smart home research. Proceedings of the 2004 International Conference on Machine Learning and Cybernetics, Shanghai, China, August. 2004. Vol. 2. P.165-169.
7. Системи безпеки “Інтелектуального будинку” [Електронний ресурс]. URL: http://dim.promotion-soft.com/bud-remont-2012-07-07-5508/
8. Home Automation and Cybercrime // Trend Micro URL: http://apac.trendmicro.com/cloud-content/apac/pdfs/security-intelligence/white-papers/wp-home-automation-and-cybercrime.pdf.
9. Теслюк В.М., Березький О.М., Береговський В.В., Теслюк Т.В. Розроблення нейроконтролера для управління підсистемою освітлення інтелектуального будинку. Зб. наук. пр. ІППМЕ ім.Г.Є.Пухова НАН України, Київ. Вип. 64. 2012. С.137 – 143.

10. Паньків В. Г. Український ринок систем автоматизації та диспетчеризації. Мережі та бізнес системи, 2011. №3. С. 58–62.

11. Теслюк В.М., Теслюк Т.В., Ляпандра А.С. Модель підсистеми клімат контролю для аналізу роботи інтелектуального будинку. Науковий Вісник НЛТУ України. 2012. №22. С. 132 - 135.

12. Architecture - SmartThings Documentation 1.0 documentation. SmartThings Documentation URL: http://docs.smartthings.com/en/latest/architecture/index.html

13. Chan M., Esteve D., Escriba C., Campo E. A review of smart homes – Present state and future challenges. Computer Methods and Programs in Biomediscine. 2008. Vol. 91. P. 55-81.

14. Jiang L., Liu D.Y., Yang B. Smart home research. Proceedings of the International Conference on Machine Learning and Cybernetics, Shanghai, China, August. 2004. Vol. 2. P. 659-663.

15. Теслюк В.М., Борейко О.Ю., Сидор А.Р., Береговська Х.В. Модель телекомунікаційної мережі інтелектуального будинку. Науковий вісник НЛТУ України. 2016. №26.1. С.351-357.

16. Teslyuk V., Beregovskyi V., Pukach A. Automation of the smart house system-level design. Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska. Polish magazin. 2013. Zeszyt 4. P.81 – 84.

17. An Overview of Home Automation Systems [Електронний ресурс]. 2017. Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7791223/.

18. Granzer W.P. Security in Building Automation Systems. Munich: Appress, 2018. 578 c.

19. Борейко О.Ю., Береговська Х.В., Теслюк В.М. Модель комп’ютерної мережі інтелектуального будинку з використанням одноплатних комп’ютерів Raspberry Pi. Матеріали IV Всеукраїнської школи-семінару молодих вчених і студентів «Сучасні комп’ютерні інформаційні технології» (АСІТ-2014), 16-17 трав. 2014 р. Тернопіль: ТНЕУ, 2014. С. 48-51.

20. Teslyuk V.M., Beregovskyi V.V., Pukach A.I. Development of smart house system model based on colored Petri nets, Proc. of the XVIII-th International Seminar. Workshop On Direct And Inverse Problems Of Electromagnetic And Acoustic Wave Theory (DIPED – 2013), Lviv, Ukraine, 2013. P. 205-208.

21. Залужний В.В., Козбур Г.Є. Механізми контролю доступу в контекстних моделях. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.103-105.

22. Залужний В.В., Моцний В.О. Моделювання атаки на систему «Розумний будинок». Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.71-74.

23. Полякова О.В. Класифікація функціональних складових елементів системи інтелектуального керування середовищем при проектуванні житла. Вісник Київського національного університету технологій та дизайну. Серія: Технічні науки. 2016. № 4. С. 133–141.

24. Що таке розумний будинок? Все що потрібно знати про систему Розумний Дім [Електронний ресурс]. Режим доступу до ресурсу: https://bron.ua/article/schotake-rozumnij-budinok-vse-scho-potrbno-znati-pro-sistemu-rozumnij-dim.

25. Розумне освітлення [Електронний ресурс]. – Режим доступу до ресурсу: https://milight.com.ua/ua/

26. Котунова, Д. Г. Огляд DIY елементів для систем «Smart Home» / Д. Г. Котунова, О. М. Павловський // XIII Науково-практична конференція студентів, аспірантів та молодих вчених «Погляд у майбутнє приладобудування», 13-14 травня 2020 р., м. Київ, Україна : збірник праць конференції. – Київ : КПІ ім. Ігоря Сікорського, 2020. – С. 35–38.

27. Технологія розумного будинку: як AI створює простір, комфортний для життя [Електронний ресурс]. Режим доступу до ресурсу:

https://www.everest.ua/tehnologiya-rozumnogo-budynku-yak-ai-stvoryuye-prostirkomfortnyj-dlya-zhyttya/

28. Моніт Я.В. Система «Розумний будинок» з відкритим програмним забезпеченням. XIX науково-технічна конференція студентів та молодих учених «Гіротехнології, навігація, керування рухом та конструювання авіаційно-космічної техніки», 15-16 лютого 2016 р. К.: «Політехніка», 2016. С. 43-44.

29. Collotta M., Pau G. A Solution Based on Bluetooth Low Energy for Smart Home Energy Management. Energies. 2015. Т. 8. №. 10. С. 11916-11938.

30. Cheng J., Kunz T. A survey on smart home networking. Carleton University, Systems and Computer Engineering, Technical Report, SCE-09-10. 2009.

31. Fouladi B., Ghanoun S. Security Evaluation of the Z-Wave Wireless Protocol. Black hat USA. 2013. Т. 24.

32. Liang L., Huang L., Jiang X., Yao Y. Design and implementation of wireless Smart-home sensor network based on ZigBee protocol. International Conference “Communications, Circuits and Systems” (ICCCAS’2008), October 14-17, 2008. P. 434-438.