Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Комп'ютерних наук
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

магістр
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: Функціональні складові інтелектуального керування та підсистема захисту "розумного будинку"

Виконав: студент (ка) 5 курсу, групи СТм-61
спеціальності (напряму підготовки)
126 „Інформаційні системи та технології"
(шифр і назва спеціальності (напряму підготовки))

(підпис) Цубера В.І. (прізвище та ініціали)

Керівник (підпис) Мацюк О.В. (прізвище та ініціали)

Нормоконтроль (підпис) Мацюк О.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

м. Тернопіль – 2019Міністерство освіти і науки України

Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

Факультет Комп'ютерно-інформаційних систем і програмної інженерії

Кафедра Комп'ютерних наук

Освітній ступінь магістр

Напрям підготовки
(шифр і назва)

Спеціальність 126 „Інформаційні системи та технології"
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри *к.т.н., доцент Боднарчук І.О.*

«_____» _____ 2019 р.

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Цубера Віталія Іванівна
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Функціональні складові інтелектуального керування та підсистема захисту "розумного будинку"

Керівник проекту (роботи) Мацюк О.В., к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «_____» _____ 201__ року №_____

2. Термін подання студентом проекту (роботи)

3. Вихідні дані до проекту (роботи)

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Обгрунтування економічної ефективності	Матійчук Л.П., к.е.н., доцент		
Охорона праці та безпека в	Стадник І.Я., д.т.н., професор		
надзвичайних ситуаціях	Дмитроца Л.П., к.т.н., доцент		
Екологія	Лясота О.М., к.т.н., доцент		
Спеціальна частина	Шимчук Г.В., старший викладач		

7. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка

Студент _____ Цубера В.І.
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ Мацюк О.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

«Функціональні складові інтелектуального керування та підсистема захисту “розумного будинку”» // Дипломна робота ОР «Магістр» // Цубера Віталія Іванівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СТм-61 // Тернопіль, 2019 // Стор. , рис. – , додат. – , бібліогр. – .

Ключові слова: БУДИНОК, СИСТЕМА, ДОСЛІДЖЕННЯ, АНАЛІЗ, ІНТЕЛЕКТ.

У дипломній роботі проведено дослідження по функціональних складових інтелектуального керування та підсистем захисту “розумного будинку”».

У першому розділі було проведено аналіз наукових статей та публікації по темі дипломної роботи. Розглянуто основні терміни та концепцію «розумного будинку».

Під час виконання другого розділу було проведено аналіз основних програм інтелектуальної системи «розумного будинку», а саме: апаратні та програмні рішення щодо безпеки та комфорту користувачів в середовищі «розумного будинку».

ANNOTATION

Functional components of intelektual control and security of «smart house» // Diploma thesis Master degree // Tsubera Vitaliia Ivanivna // Ternopil' Ivan Pul'uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science, group STm-61 // Ternopil, 2019 // Pages___, Fig.____, Appendixs____, Bibliograms._____.

Keywords: HOUSE, SYSTEM, RESEARCH, ANALYSIS, INTELLECT.

The diploma work conducted research on the Intelligent Control Functional Components and Smart Home Subsystems.

The first section of the analysis of scientific articles and publications on the topic of diploma work was carried out. The basic terms and concepts regarding «smart house».

During the implementation of the second section, the main programs of the intelligent System of "smart home", namely: hardware and software solutions for user safety and comfort in a «smart home» environment.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПК – персональний комп’ютер.

Розумний дім – будинок з мікроконтроллерами, що керують всіма або більшою частиною пристроїв всередині.

Атака – загальна назва спроби заподіяти шкоду інформаційному носію.

RSA (Rivest, Shamir, Adleman) – асиметричний шифр.

Zigbee – це бездротовий стандарт передачі даних, що дозволяє передавати пристрій на пристрій з низькою вартістю, а також з низькою швидкістю передачі даних та низьким енергоспоживанням.

HiperLAN – стандарт бездротової локальної мережі, опублікований Європейським інститутом телекомунікаційних стандартів.

Bluetooth – це відкрита стандартна специфікація, яка дозволяє скоротити бездротові з'єднання для широкого кола портативних та / або стаціонарних пристроїв.

GCP (Google Cloud Platform) – інтегрованийхмарний сервер надається компанією Google, що побудований на такій же інфраструктурі, Google Search і YouTube.

GLSHCS (GL SmartHome Cloud Solution) — це готовий продукт, що дає можливість автоматизувати роботу великої кількості функцій «розумного будинку» або для цілого «розумного міста».

IFTTT (If This Then That) – модуль, що об’єднує прилади які раніше не могли працювати в одному середовищі, тобто прилади від різних фірм і виробників.

AVS (Amazon Alexa Voice Service) – це категорія пристроїв, створених за допомогою голосової служби Alexa, які мають мікрофон та динамік.

ЗМІСТ

ВСТУП

Актуальність теми роботи. «Розумний будинок» – являється інтелектуальною системою автоматики, яка керує всіма інженерними системами. Кожна людина хоче відчувати комфорт та безпеку, будучи в квартирі чи в офісі. Комфорт та безпека являються основними цілями розумного будинку, а також ектетика вигляду приладів.

На сьогоднішній день інтеграція сучасних комунікаційних та інформаційних технологій у житло призвела до появи «Смарт–домів». Ці технології полегшують створення умов для «розумного будинку», в яких пристрої та системи можуть взаємодіяти один з одним і можуть контролюватися автоматично. Тим не менш, багато проблем з безпекою викликає те що він завжди пов'язаний з зовнішнім світом через Інтернет і «відкриті задні двері» безпеки, отримані від користувачів. Нарешті, переглянувши наявну літературу про «розумні будинки» та питання безпеки, які існують у середовищі, передбачається забезпечити базу для розширення досліджень у сфері безпеки «розумного будинку» [1].

Протягом останніх десятиліть концепція «розумного будинку» почала стрімко розвиватися, але стикається з винятковими проблемами. Проте нещодавні події в інформаційно–комунікаційних технологіях призвели до розвитку інтелектуального будинку на хорошому рівні зрілості. «розумний дім» – це середовище для життя, яке включає в себе відповідну технологію, яка називається технологією «розумного будинку», для досягнення цілей комфортного проживання, безпеки життя, безпеки та ефективності [1].

Технологія «розумного будинку» досягає цих цілей, створюючи середовище, яке складається з різноманітних домашніх систем. «Розумний будинок» охоплює чотири типи систем «розумного будинку»:

– побутова техніка, система освітлення та управління кліматом;

– система домашніх розваг;

– система домашньої комунікації;

– система домашньої безпеки [1].

Кожна з вищеописаних систем характеризується різними вимогами на основі програм, що підтримує. Таким чином, різні фізичні носії є прийнятними для різних систем «розумного будинку».

Вагомий внесок у розробку систем захисту для «розумнго будинку» внесли: K.Westerlund, D. G. Hill,L. Hollis, M. Kurita, C. Lemin, K. Macfii, K. Matti, A. Miimy, C. Pula та інші.

Метою дослідження є пошук та проведення аналізу функціональних складових інтелектуального керування та підсистем захисту «розумного будинку», що має допомогти зрозуміти призначення «розумного будинку» в даний час.

На сьогодні існує велика кількість програм для інтелектуального середовища «розумного будинку» які треба проаналізувати та згідно аналізу обрати кращі.

Задача дослідження:

– здійснити аналіз літературних джерел щодо «розумних будинків»;

– проведення загального огляду основних програм інтелектуального середовища «розумного будинку, а саме: розширену систему управління та безпеки, вдосконалену систему управління домом віддалено;

– аналіз існуючих систем захисту для «розумного будинку»;

– розглянути питання забезпечення працездатності пристроїв.

Об'єктом дослідження є функціональні складові інтелектуального керування та підсистема захисту «розумного будинку».

Предметом дослідження являється сукупність теоретично-практичних досліджень та основних питань щодо розвитку системи «розумного будинку».

Науковою новизною роботи є новий підхід щодо опрацювання матеріалу, вирішення поставлених задач. Оцінка та аналіз літературних джерел щодо актуальності дослідження, а також питання забезпечення безпеки будинку.

Практичне значення: в ході виконання дипломної роботи було проведено загальний аналіз функціональних складових інтелектуального керування та підсистем захисту «розумного будинку», який допоможе визначити головні переваги та недоліки в даній області.

Результати дипломної роботи магістра представлялися на Міжнародних наукових конференціях, за результатами яких опубліковані:

1. Цубера В.І., Програмні аспекти «Розумного будинку». Аналіз існуючих програм захисту / Цубера В.І, Янковська Д.А., Квач С.М., // Збірник тез конференції II Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання» , 25-26 квітня 2019 року. — Т. : ТНТУ, 2019. — С. 53-54.

2. Цубера В.І., Аналіз існуючих розумних парковок для розумного міста / Цубера В.І., Янковська Д.А, Квач С.М., // Збірник тез конференції II Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання», 25-26 квітня 2019 року. — Т. : ТНТУ, 2019. — С. 59-60.

1 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ «РОЗУМНОГО БУДИНКУ»

1.1 Історія створення «розумного будинку»

1980–ті принесли програмовані термостати та домашні обчислення. Американська асоціація будівельників будинків ввела термін «розумний будинок» у 1984 році. Фільми почали відображати наші уявлення про те, що це означає. Kissimmee Xanadu House був створений архітектором Роєм Мейсоном, щоб створити серію «розум–роботів», які допоможуть вам провести свій день з комфортом. Був комп'ютер для приготування їжі та один, щоб стежити за станом здоров'я, садівник, погодний репортер тощо. Цей проект передбачався на 1000 будинків, але його так і не реалізували [1].

З переходом у 1990–ті електронні пристрої стали розумнішими. Walkman став портативною приставкою для компакт–дисків. Комп'ютери "зжалися", а мобільні телефони стали більш самостійними. Тоді, в 1999 році, Microsoft представила своє бачення «розумного будинку». Дім працював Pocket PC і включав в себе все, від розумних замків, освітлення та контролю навколишнього середовища, системи моніторингу домашнього відеоспостереження та навіть сканер, що провіряє штрих–код, для можливості здійснення покупок онлайн. Таке бачення, безумовно, було вперше, коли компанія розуміла те, що буде мати майбутнє [1].

Але з часом почали розроблятися «розумні будинки», обладнані різними приладами, які працюють в одній системі. Розробники почали приділяти увагу не цільки комфорту користувачів, вони старалися зробити все можливе для економії ресурсів. Кошти, яких потребувала розробка нової технології, були дуже великими. На початку 1978 року, розробники добилися того, що електричні побутові прилади могли працювати через дроти, вони мали напругу 110В [2]. На той час це був справжній прорив, що дозволяв надалі праювати за даною схемою.

Саме Американська Асоціація Забудовників (ААЗ) вигадада термін «розумний будинок» у 1984 році, та ввела у вжиток. Саме в ті роки і почали падати

ціни на електроприлади, що робило можливим побудову офісів з високою функціональністю[3].

Процес автоматизації трохи важко уявити без різних сенсорів чи датчиків, тому особливий розвиток системи «розумного будинку» почався в дев'яностих роках. Сучасні «розумні будинки» втілили у собі купу інноваційних розробок, які роблять їх унікальними з боку комфортності та головне безпеки. Завдяки наявності всіх розробок дає власнику житла можливість не перейматися через будинок, так як він постійно під контролем. На даний момент є багато компаній, що можуть запропонувати свої послуги з проектування «розумного будинку», але при виборі компанії користувач має бути впевненим у професіоналізмі працівників, щоб уникнути проблем з пристроями [4].

1.2 Конценція «розумного будинку»

Для архітектурної моделі «розумного дому» дуже важливо висначитисяз списком основних компонентів для того, щоб зрозуміти що саме впливає на рівень безпеки помешкання, а також реалізацію технологій безпеки, що дає можливість мінімізувати ризик небезпечних атак [5].

Можна вважати що «розумний будинок» складається з трьох основних компонентів:

– внутрішня мережа;

– зовнішня мережа;

– мережевий шлюз.

Ці три компоненти представлені на рисунку 1.1.

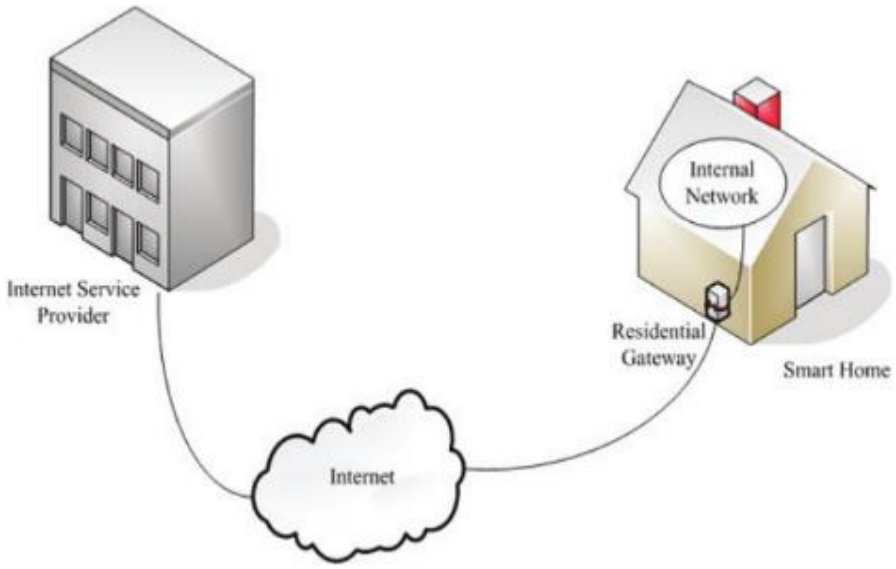

Рисунок 1.1 – Концепція «розумного будинку»

Внутрішня мережа є основою «розумного будинку» і може складатися з дротових і бездротових мереж. Внутрішня мережа «розумного будинку» включає поєднання різних комунікаційних медіа та протоколів для підтримки ряду систем «розумного будинку», які спрощують життя мешканців та покращують якість їх життя. Зовнішня мережа «розумного будинку» включає Інтернет та постачальника послуг, який відповідає за надання послуг через Інтернет користувачам. Житловий шлюз (RG) є завжди підключеним пристроєм, розташованим у «розумному будинку» і грає дуже важливу роль подолання внутрішньої мережі «розумного будинку» та зовнішнього світу [5].

У сучасному світі ми можемо стежити за своїм будинком з будь–якого місця. Маємо можливість регулювати температуру будь–якого приміщення за допомогою смартфона або слухати улблене радіо в будь–якому приміщенні будинку. Вогнями, розетками та електронікою можна керувати дистанційно через Інтернет. Завдяки зручності керування системою, її інтеграцією, можливості приладів працювати один з одним, тим самим розширювати функції кожного з них окремо, ми можемо назвати будинок – «Розумним». Він здатен підтримувати клімат, тим самим створює затишок лише однією кнопкою.

«Розумний дім» робить життя користувача спокійним та безтурботним. Він постійно контролює всі інженерні системи і слідкує щоб не було витоку газу або витоку води. Також якщо буде спроба прникнення в будинок постороннього, то система буде створювати неприємні умови перебування і постарається випровадити його, і обов'язково оповістить користувача та надішле сигнал на пульт тривоги, використовуючи мобільний з'язок чи почту [5]. Користувач може віддалено "спілкуватися" з «розумним будинком» та керувати ним, і торимувати у відповідь дані про стан систем в дому, при цьому бути далеко від нього.Тому питання няньки для дітей само відпадає, так як не обов'язково стежити за тим щоб вони не засиджувалися біля телевізору, за вашої відсутності вдома. Ми будете мати змогу самі спостерігати за цим та контролювати віддалено.

1.3 Система інтелектуальної автоматизації

«Розумний дім» – являється інтелектуальною системою автоматики, яка керує всіма інженерними системами. Кожна людина хоче відчувати комфорт та безпеку, будучи в квартирі чи в офісі. Комфорт та безпека являються основними цілями «розумного будинку», а також ектетика вигляду приладів [6].

Завдяки тому, що інтелектуальна система керує усіма приладами в дому, користувач може налаштовувати комфортні умови для себе, це може бути температура, світло, рівень вологості та забезпечення безпеки. «Розумний будинок» керує такими об'єктами автоматизації як:

– світло;

– електроприлади;

– клімат;

– вентиляція;

–охоронна система;

– камери;

– сигналізація;

–доступ до будинку;

–інженерні прилади через сенсорні панелі;

–керування сервером.

Система розумного будинку відповідає за централізований контроль та його безпеку, також за інтелектуальне керування офісних, житлових, або громадських приміщень [6]. З після інсталяції подібної системи дома або на роботі користувач може в рамках загального середовища налаштовувати параметри індивідуально (температура, світло , звук і т.д.) та виконуючи управління отримувати інформаію про стан всіх приладів в будинку відалено або будучи всередині нього. На рисунку 1.2 показано загальну схему управління системою.

Рисунок 1.2 – Схема управління системою

Процесор використовує такі інтерфейси як RS232, IR, ethernet, RS485 та аналогові та цифрові входи/виходи та ін.

Центральний проесор також маж багатозадачну операсійну систему, засоби програмування та деколи веб- сервер. Датчики користувач розташовує упо всьому будинку у певних місях, які з'єднуються в єдину мережу через деякі проміжні

пристрої. Загальне керування системою будинку виконують інтерфейси управління [7].

Побудований загальний алгоритм таким чином:

– інформаія від датчиків чи інтерфейсів по власній мережі відправляється на центральний процесор керування;

– ПЗ процесору займається обробкою отриманої дних після чого генерує команди і подає їх керуючим пристроям.

Команди на пристрої надходять з власної та домоміжної мережі.На етапі розробки ПЗ закладається склад та форма інформації і генерування команд враховуючи вимоги до проекту [7].

1.4 Підсистеми «розумного будинку»

Внутрішня мережа «розумного дому» може інтегрувати різноманітні системи, які забезпечують зручне та безпечне середовище для користувачів, а також допомагають їм виконувати всі задані їм команди та домашні завдання. Систему «розумного дому» можна класифікувати за чотирма категоріями (рисунок 1.3). Побутова техніка, світло та контроль клімату, система домашніх розваг та домашнього зв’язку, та головне система домашньої безпеки [8].

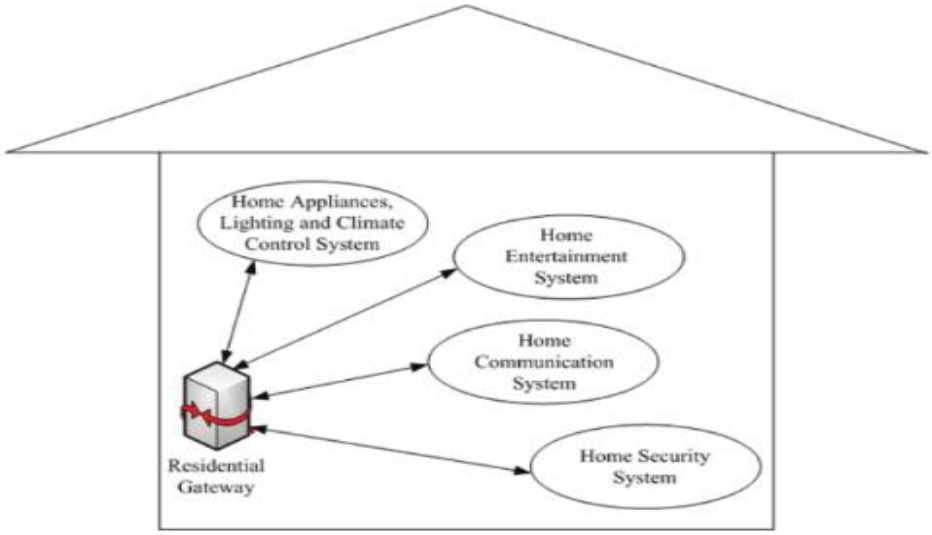

Рисунок 1.3 – Системи «розумного будинку»

1.4.1 Побутова техніка, система освітлення та управління кліматом

Система побутової техніки, освітлення та управління кліматом складається з трьох підсистем. Підсистема управління побутовою технікою контролює і керує розетками в «розумному будинку». Таким чином, на основі цієї підсистеми середовище існування здатне контролювати споживання енергії, а також окремо відключати розетки. Підсистема управління побутовими приладами може включати в себе розумні прилади, які спілкуються один з одним і з зовнішнім світом Інтернету, роблячи щоденне життя середовища проживання більш комфортним і приємним [8].

Підсистема управління світлом має в своєму складі перемикачі і датчики. Ця підсистема відповідає за інтенсивність світла, а також діяльність користувачів у внутрішньому середовищі дому, та адаптує режим освітлюваності інтелектуальних кімнат.

І на кінець, підсистема контролю клімату включає функції опалення, вентиляції та кондиціонування. Ця підсистема відстежує і контролює температуру і вологість в середовищі «розумного дому», що дозволяє користувачу бути впевненим у безпеці та здорових умов проживання. Крім того, підсистема світла та упрата контроль клімату зменшує затрати на опалення, охолодження та освітлення завдяки інтелектуальному управлінню енергією, що допомагає користувачам житла заощадити гроші [8].

1.4.2 Підсистема домашніх розваг

Система домашньої розваги забезпечує зв'язок та зв'язок аудіо– та відеообладнання над широкосмуговими мережами, що обслуговують розподіл високоякісного аудіосигналу та високоякісного цифрового відео. Система розваг може складатися з домашнього кінотеатру, проекційних систем, плазмових або РК–екранів, багатоканальної системи об'ємного звучання, супутникових і цифрових телевізійних каналів, систем відеоспостереження, ігрових консолей, центрального медіа–сервера,система управління, а також багатоканальна аудіо відеосистема для повного аудіо та візуального розповсюдження. Цифровий звук поширюється з MP3–

файлів, інтернет–радіо та домашнього медіа–сервера по всій системі в кожній кімнаті «розумного будинку». Крім того, цифровий відеовміст розповсюджується з широкосмугового з'єднання, DVD–дисків, ПК та домашнього медіа–сервера на будь–який відеоекран у розумному середовищі [9].

1.4.3 Підсистема домашнього зв’язку

Система домашньої комунікації надає телефонні послуги, такі як звичайні голосові послуги та відеоконференції, а також включає систему взаємодії інтелектуального внутрішнього середовища для виклику з кімнати в кімнату. Крім того, ця система керує пристроями, такими як ПК, телефони, персональні помічники (PDA), принтери і сканери, та дозволяє їм спілкуватися один з одним, обмінюватися інформацією та широкосмуговим з'єднанням у межах «розумного будинку». Таким чином, користувачі можуть спілкуватися, надсилати електронні листи та обмінюватися даними (наприклад, цифровими фотографіями, відео) з іншими людьми в будь–якому місці світу [10].

1.4.4 Підсистема безпеки «розумного будинку»

Підсистема домашньої безпеки охоплює такі механізми ідентифікації, як біометричне розпізнавання, розпізнавання голосу і розпізнавання облич, маркери RFID і смарт–карти, що забезпечують контроль доступу. Більш того, вона включає в себе механізми повідомлення, такі як охоронні сигналізації, які дозволяють негайну реакцію. Крім того, механізми спостереження, такі як відеоспостереження, можуть бути частиною системи безпеки для моніторингу в «розумному будинку». Більше того, існують рішення, такі як датчики вібраційного удару, датчики розриву скла, для виявлення порушника на місці проживання. Також існують системи, які використовують світло, яке автоматично вмикається і вимикається, створюючи враження, що хтось є вдома. Крім того, система домашньої безпеки містить електромеханічні дверні замки, електричні вікна та дверні жалюзі. Моніторинг здоров'я та благополуччя для інвалідів та людей похилого віку, а також дітей може бути частиною цієї системи [10].

1.5 Мережевий шлюз

У «розумному будинку» мережевий шлюз або машрутизатор – це пристрій, що об'єднує усі різні мережеві технології, які існують у внутрішній мережі будинку, а також забезпечує доступ від внутрішньої мережі до Інтернету і навпаки. Мережевий шлюз служить єдиною точкою конвергенції і розподілу внутрішніх мереж і ініційованих LAN і ініційованих глобальною мережею послуг. Мережевий шлюз дозволяє перемикання, маршрутизацію та взаємодію між пристроями систем по внутрішній мережі. Цей мережевий пристрій також підтримує високий рівень розподілу передових мультимедійних послуг через широкосмугове підключення до Інтернету. Крім того, підтримує дистанційне керування системами «розумного будинку» і побутовою технікою [11].

Завдяки різноманітності технологій мережі доступу, мережевий шлюз може взаємодіяти з більшістю мереж дротового або бездротового широкосмугового доступу (наприклад, ADSL, широкосмугова мережа мобільних телефонів, супутниковий зв'язок і т.д.). Різні типи інтерфейсів сторін WAN можуть бути надані шлюзом для резидентного розміщення, але одночасно підтримується тільки один інтерфейс. Крім того, мережевий шлюз може підтримувати інтерфейси через дротові / бездротові локальні мережі по відношенню до внутрішньої мережі, оскільки існує багато дротових (HomePlug, HomePNA, ethernet, IEEE1394 та USB) і бездротових мереж (IEEE 802.11, Bluetooth, Zigbee і HiperLAN) технології в «розумному будинку». Також мережевий шлюз забезпечує керування QoS для підтримки служб різних типів одночасно. Мережевий шлюз містить правила класифікації, масового обслуговування та відображення пріоритетних полів [11].

Також шлюз може забезпечувати функціональність, пов'язану з безпекою в середовищі «розумного будинку». Вона забезпечить захист користувача від вторгнень. Тим самим, мережевий шлюз може охоплювати функції що відповідають за безпеку, починаючи з брандмауерів закінчуючи на механізмах виявлення вторгнень [11].

1.6 Розумна домашня мережа

Внутрішня мережа «розумний будинок» заснована на різних носіях інформації та протоколах. Це поєднання дротових та бездротових мереж, оскільки різні засоби передачі, такі як лінії телефонну та електропередач, радіозв'язок та дротові кабелі, використовуються для передачі сигналу в середовищі «розумний будинок». Дротові та бездротові мережі можуть передавати загрози у внутрішню мережую. Домашню мережу можна організувати по трьом категоріям: існуючі дротові, провідні та бездротові мережі.

Існуючі провідні мережі використовують повторно в домашній електропроводці, яка складається з електричної проводки, телефонної проводки та коаксіального кабелю для передачі даних [12].

Нові провідні мережі потребують спеціального кабельного зв’язку для поширення високошвидкісних даних та відео по всьому житлу. Нарешті, бездротові мережі використовують повітря як середовище передачі і пропонують рішення з вимогами "без проводів".

Провідні мережі забезпечують більшу безпеку порівняно з бездротовими мережами, оскільки їх не можна так легко прослухати. Противнику легко перехопити сигнал або порушити нормальну роботу бездротової мережі через те, що бездротові технології не можуть контролювати дальність передачі. Крім того, динамічність та мобільність, що забезпечуються бездротовими мережами, дають більше шансів супротивни–кам використовувати вразливі місця мережі непомітно [12].

1.6.1 Існуючі дротові мережі

Існуючі технології дротових мереж безпосередньо застосовуються до нових і старих будинків, оскільки не потрібно проводити електропроводку дому. Основними обмеженнями технології є структура мережі та перешкоджають початковій роботі мережі. Основа існуючої електропроводки дому можуть

розроблятися мережа електропередач та ланія телефону, а також коаксіальна мережа щоб задовільнити потреби користувача [13].

1.6.2 Мережі електропередач

Мережі використовують існуючу електричну проводку, яка вже використовується для забезпечення живленням побутовою технікою та освітленням. Основна мета мереж Powerline (Лінія електропередач) – підключити пристрої один до одного та підключити їх до Інтернету безпосередньо у розетки змінного струму в «розумному будинку». Однак, виходячи з сучасних технологій Powerline [13], нам потрібно додати адаптер до кожного пристрою, перш ніж він підключений до розетки. В даний час мережі Powerline підтримують низькошвидкісні з'єднання через малу пропускну здатність дроту. Таким чином, в мережі «розумного будинку» Powerline можна використовувати мережу побутової техніки, освітлення та кліматичного контролю, а також систему домашньої безпеки для додатків із низькими вимогами швидкості передачі даних. Крім того, нові методи та технології модуляції підвищили швидкість передачі даних мереж Powerline, що дозволило їм підтримувати мультимедійні програми, такі як аудіо– та відеопотік у «розумному будинку» [14]. Однак є можливість що переданий сигнал через мережу електропередач витікає із середовища «розумного будинку» через протікаючу електромагнітну хвилю від лінії електропередач. Таким чином, блокуючі фільтри, які блокують високочастотний компонент сигналу, повинні бути встановлені в мережі зв'язку електропередач.

HomePlug (штекер) – Powerline для зв'язку як головний стандарт. Це простий у використанні стандарт класу ethernet, його було створено на основі HomePlug Powerline Alliance.

Існує чотири версії стандарту HomePlug:

– перша версія, HomePlug 1.0, підтримує з'єднання зі швидкістю передачі даних на 14 Мбіт / с;

– друга версія – HomePlug 1.0 Turbo, працює на швидкості 85 Мбіт / с;

– третя версія, HomePlug AV, призначена для додатків HDTV та VoIP, працює на швидкості 189 Мбіт / с.

Нарешті, остання версія, HomePlug Command and Control, працює з низькою швидкістю передачі даних і підходить для застосувань системи побутової техніки, освітлення та клімат–контролю. Крім того, протокол HomePlug AV формує віртуальні приватні локальні мережі, використовуючи криптографічну ізоляцію. Коли віртуальна приватна мережа сформована, ключ користувача в мережі [14] розподіляється на всі станції цієї мережі. Розподіл NMK по всіх станціях може відбуватися трьома способами.

По–перше, Network Membership Key (NMK) кожну станцію він приймає безпосередньо. По–друге, він може бути розповсюджений за допомогою ключа доступу до пристрою Device Access Key (DAK). По–третє, він може бути переданий за допомогою протоколу обміну ключами Unicast. Володіння NMK визначає кожну станцію в мережі. Крім того, в цій мережі використовується ще один ключ, який називається Network Encryption Key (NEK). Цей ключ періодично змінюється з міркувань безпеки. Контролер мережі розподіляє НЕК, який зашифрований за допомогою NMK, по всіх станціях, та застосовує 128–бітнине AES шифрування, щоб забезпечити неможливість підслуховувати потоки інформації. Кожна станція має у своєму використанні NEK для шифрування корисних навантажень інформаії, що надсилаються в мережу.

1.6.3 Мережева телефонна лінія

Мережева лінія телефону забезпечує простий і недорогий спосіб для обміну даними, пристроями периферії а високошвидкісним доступом до Інтернету в межах «розумного будинку» за допомогою зареєстрованих телефонних роз'ємів та існуючих в домашніх телефонних кабелях, не впливаючи на телефонну послугу завдяки підключенню пристроїв. Мережева телефонна лінія вимагає встановлення мережевого адаптера, який підтримує протоколи лінії телефону, до кожного пристрою, який власник хоче підключити до мережі лінії телефону. Потім

користувач має змогу підключити мережевий адаптер пристрою до розетки за допомогою стандартного телефонного кабелю [15].

На відміну від мереж Powerline та коаксіальних мереж, які потребують фізичної ізоляції або шифрування даних для запобігання підслуховування, мережі Phoneline не використовують жодного методу забезпечення безпеки, оскільки вони не є спільними. HomePNA є головним галузевим стандартом для мережевих телефонних зв’язків і забезпечує додатковий канал зв'язку по існуючій телефонній лінії. HomePNA – це стандарт, заснований на Ethernet, і розроблений Альянсом домашньої телефонної лінії. Останнім часом існує багато постачальників, які відповідають цьому стандарту [12]. Існує три версії HomePNA, HomePNA 1.0, що гарантує швидкість передачі інформації з швидкістю 1 Мбіт / с, HomePNA 2.0 - 10 Мбіт / с, і HomePNA 3.0 - 100 Мбіт / с. Тому мережа телефонних ліній може обробляти додатки системи домашнього спілкування та системи розваг, які включають додатки з високою швидкістю передачі інформації.

1.6.4 Коаксіальні мережі

Коаксіальна мережа використовує коаксіальний кабель, який зазвичай використовується для розподілу радіо– і телевізійного сигналу в резиденції. Коаксіальні мережі характеризуються великими можливостями пропускної здатності і можуть підтримувати додатки системи домашнього спілкування та системи домашніх розваг. Основним стандартом цієї технології є HomeCNA, розроблений Альянсом Home Cable Network Alliance. Однак коаксіальна мережа представляє меншість внутрішніх мереж для існуючих будівель через мале використання коаксіального кабелю. У коаксіальних мережах необхідна фізична ізоляція, а також шифрування, щоб уникнути підслуховування мережевого трафіку [13].

1.6.5 Нові провідні мережі

Нові провідні мережі або структуровані електропроводки забезпечують високу продуктивність підключення та високу надійність. Таким чином, цей тип

внутрішніх мереж може підтримувати додатки системи домашнього спілкування, системи домашніх розваг та системи домашньої безпеки. Основним недоліком нових провідних мереж є те, що їх неможливо легко встановити чи розширити в існуючому будинку чи квартирі через їх вимоги до електропроводки. Запуск нових кабелів передачі даних всередині стін цегляного або кам'яного будинку – не доступне рішення. Однак, хороша ідея провести електропроводку по всьому будинку, поки він будується. Найпоширенішими стандартами зв'язку нових провідних мереж є EEE1394, ethernet і USB . Ethernet або IEEE 802.3 – це найпоширеніший стандарт дротової локальної мережі для ПК та робочих станцій. Ethernet – це зріла технологія, яка характеризується простотою в установці та конфігурації [14]. Цей стандарт може підтримувати безліч таких служб, як TCP / IP на основі даних, голосові та відеопрограми в «розумному будинку», і його підтримує багато постачальників.

У 1985 році було визначено першу версію, ethernet (10Base), яка передає дані з швидкістю 10 Мбіт / с. Через десять років з'явилася друга версія, Fast ethernet (100Base), яка мала швидкість100 Мбіт / с. Третя версія, Gigabit ethernet - 1 Гбіт / с. Нарешті, остання версія, 10Gigabit ethernet - 10 Гбіт / с. Ethernet має ряд вразливостей, які впливають на безпеку мережі. Основна слабкість полягає в тому, що всі станції в локальній мережі мають один і той же фізичний канал. Таким чином, зловмисник може легко підслуховувати переданий трафік, оскільки те, що станція надсилає по мережі, може отримувати одночасно всі інші станції мережі. Крім того, стандарт Ethernet не забезпечує жодного механізму для перевірки ідентичності відправника повідомлення або перевірки цілісності повідомлення. Тому супротивник може породити шахрайські дані та вставляти їх у мережевий трафік, або він/вона може отримувати повідомлення, які обмінюються між двома законними сторонами, що спілкуються, та повторно передавати їх згодом як уповноважена особа. Ці дві слабкості можуть слід вирішити поділ Ethernet LAN у «розумному будинку» на підмережі за допомогою мостів [15].

1.6.6 Бездротові мережі

Такі мережі являються дуже привабливим рішенням для мереж «розумного дому», вони забезпечать просту установку, велику гнучкість та швидке отримання даних. Також, вони не включають витрати на електропроводку, а також проблеми існуючих мереж електропроводки. Більше того, бездротові мережі можна легко розширити в домашніх умовах відповідно до потреб користувачів. Такі мережі використовуються для задоволення вимог щодо мобільності, переїзду, а також для областей, де важко проводяться локальні мережі. Отже, існує безліч прикладних областей для такої мережі. Однак іноді вони мають вимоги до прямого зору та обмежене покриття. Вони можуть використовуватися у всіх розумних будинках, від побутової техніки, до систем світла і контролю клімату, зв'язок, розваги та безпека. Є багато стандартів житлових мереж, але найбільш домінуючими є IEEE802.11, Bluetooth, Zigbee та HiperLAN [16].

1.6.7 Bluetooth

Bluetooth (IEEE 802.15.1) – це відкрита стандартна специфікація, яка дозволяє скоротити бездротові з'єднання для широкого кола портативних та / або стаціонарних пристроїв. Старіший Bluetooth 1.0 мав максимальну швидкість передачі інформації у 1 Мбіт / с, тоді як найновіший Bluetooth 2.0 може передавати інформацію з швидкістю до 3 Мбіт / с. Пристрой Bluetooth підтримує зв'язок через спеціальну мережу короткого діапазону, яку називаються піконетами. Піконети встановлюються динамічно, коли пристрой Bluetooth входить і залишає радіо близькість [17].

Крім того, технологія Bluetooth одночасно підтримує передачу даних і голосу. Bluetooth реалізує декілька механізмів аутентифікації та шифрування даних для забезпечення безпеки.[17] Схема аутентифікації Bluetooth використо–вує метод реагування на виклик. Схема шифрування Bluetooth шифрує корисні навантаження переданих пакетів за допомогою шифру потоку E. Крім того, будь–яка пара пристроїв із підтримкою Bluetooth, які бажають спілкуватися один з одним, повинна генерувати сеансовий ключ, який називається ключем зв'язку, використовуючи комбінацію ключа ініціалізації, MAC–адреса пристрою та номер, що ідентифікує

користувача (PIN–код). Однак Bluetooth має ряд недоліків, які можуть бути використані супротивниками для отримання ключів та номерів PIN–кодів, залежно від того, як виконується ініціалізація сеансу стандарту зв'язку [18].

1.6.8 Zigbee

Zigbee (IEEE 802.15.4) – це бездротовий стандарт передачі даних, що дозволяє передавати з пристрою на пристрій з низькою вартістю, а також з низькою швидкістю передачі даних та низьким енергоспоживанням [19]. Він замінює дротові рішення з низькими вимогами швидкості передачі даних.

Zigbee може працювати на частоті 2,4 ГГц з базовою швидкістю передачі даних в 250 Кбіт / с. Zigbee підходить для домашніх програм, таких як додатки для побутової техніки, системи освітлення та клімат–контролю, а також для системи домашньої безпеки. Існує централізована організація довіри, якій довіряють усі вузли мережі та відповідає за розповсюдження ключів та контроль надходженням вузлів, що вимагають доступу до мережі. Кожна мережа не може мати більше одного централізованого цільового об'єкта і кожен пристрій може бути пов'язаний лише з одним централізованим довірчим об'єктом [19]. Однак ця сутність може розглядатися як єдина точка відмови і може бути вразливою до безпеки мережі, яку можуть використовувати зловмисники. Крім того, стандарт Zigbee пропонує три типи ключів: ключ посилання, мережевий ключ та головний ключ. Клавіша зв’язку ділиться між будь–якими двома пристроями та використовується для забезпечення їх зв'язку. Клавіша Net–Work – це загальний ключ для всіх пристроїв і ділиться між усіма пристроями в мережі [20].

Мережевий ключ використовують щоб захистити широкомовний зв'язок в мережі. Головний ключ попередньо встановлений або походить від централізованого довірчого об'єкту, його використовують для генерації ключів посилання. Крім того, стандарт Zigbee забезпечує свіжість даних, цілісність даних, автентифікацію та шифрування. Свіжість даних досягається за допомогою лічильників, які скидаються щоразу, коли генерується новий ключ. Цілісність даних

забезпечується кодами аутентифікації повідомлень. Надається аутентифікація на рівні мережі та аутентифікація на рівні пристроїв використовуючи загальний мережевий ключ та відповідні клавіші посилання. Нарешті, Zigbee пропонує шифрування яке має 128–біт завдяки зоагальному мережевому ключеві для шифрування мережі та клавіш посилання для шифрування гаджету [21].

1.6.9 HiperLAN

HiperLAN – стандарт бездротової локальної мережі, опублікований Європейським інститутом телекомунікаційних стандартів (ETSI).Є дві версії: HiperLAN 1 та HiperLAN 2.

HiperLAN 1 був опублікований у 1996 році, 23,5 Мбіт / с - це максимум швидкості передачі інформації

HiperLAN 2 був опублікований в 2000 році і має 54 Мбіт / с швидкості передачі інформації. Основними послугами, які можуть підтримувати дві версії, є передача даних, аудіо та відео. Гіперлайн використовує схеми взаємного аутентичного керування телефонів, шифровки інформаїта обміну ключами шифрування [22]. Стандарт HiperLAN пропонує п'ять механізмів аутентифікації, засновані на підході до відповіді на виклик, що забезпечує взаємну аутентифікацію між мобільними пристроями та точкою доступу. Крім того, HiperLAN використовує алгоритми DES та 3DES для шифрування даних. Нарешті, заснований обмін ключами шифрування на протокол Діффі–Гелмана. Незважаючи на те, що в HiperLAN є кілька відносно сильних механізмів захисту, існує багато вразливих місць [23].

1.7 Вимоги безпеки в середовищі «розумного будинку»

Представивши концепцію «розумного будинку» та описавши мережеві технології, що застосовуються для впровадження її систем, вимоги безпеки для середовища «розумного будинку» визначено. Основні завдання безпеки, яких повинно виконувати середовище «розумного будинку», – це конфіденційність,

цілісність, автентифікація, авторизація, неприйняття статусу та доступність. Конфіденційність стосується запобігання несанкціонованого доступу до певної інформації. При нападі на конфіденційність противник може використовувати послуги, що надають інформацію про статус «розумного будинку» з метою забезпечення непрямого спостереження за діяльністю мешканців у середовищі «розумного дому». Конфіденційність може бути досягнута за допомогою симетричних шифрів криптографа–hic [24].

Цілісність – це служба безпеки, яка забезпечує запобігання несанкціонованому зміненню інформації. Цілісність гарантує, що дані не були змінені, знищені або втрачені під час будь–якого процесу, наприклад передачі, зберігання чи пошуку. Іншими словами, цілісність забезпечує узгодженість та правильність даних. Цілісність може бути порушена зловмисником, який підслуховує трафік до внутрішньої мережі «розумного будинку» та підробляє дані. Цілісність може бути надана за допомогою коду аутентифікації повідомлення [25].

Автентифікація – служба безпеки, пов’язана з верифікацією суб'єкта господарювання на основі пароля або спільного секретного ключа між сторонами, що спілкуються. Автентифікація дозволяє одному суб’єкту перевірити особу іншого суб'єкта. Існує два типи аутентифікації: аутентифікація сутності та автентифікація повідомлень. Аутентифікація суб'єкта господарювання підтверджує дійсність заявленої особи кожного суб'єкта [25].

Іншими словами, автентифікація суб'єкта господарювання підтверджує особу сторін, що спілкуються. З іншого боку, автентифікація повідомлення підтверджує, що повідомлення походить від заявленої сутності. У середовищі «розумного будинку» потрібно багато механізмів аутентифікації для користування пристроєм, користувачем та внутрішньою мережею, пристроєм пристроєм, мережею між пристроєм та аутентифікацією постачальника послуг. Противник може претендувати на інший законний користувач чи організацію з метою отримання важливої інформація щодо домашніх користувачів або доступу до служб навколишнього середовища «розумного будинку» [26].

Авторизація – це процес, який визначає права доступу користувача на пристрій чи мережевий ресурс і те, що пристрою дозволено робити в середовищі «розумного будинку». Авторизація також може забезпечити різні рівні доступу для гарантії що суб'єкти можуть здійснювати доступ та виконувати операції лише на мережевих ресурсах, на які вони уповноважені.

Пристрої що належать внутрішній мережі «розумного дому» можна класифікувати на два типи : домашні пристрої та іноземні пристрої. Що стосується домашніх пристроїв, механізм авторизації заснований на правах доступу домашнього користувача на пристрої. Що стосується іноземних пристроїв, власник кожного пристрою делегує певні права доступу іноземним користувачам, які повинні платити, коли вони бажають ними користуватися [26].

Однак противник може використовувати підроблені авторизації для здійснення заборонених дій у середовищі «розумного будинку». Невідхилення відповідає службі безпеки, що забезпечує захист від відмови в причетності до дії [27]. Наприклад, неприйняття даних забороняє як відправнику, так і одержувачу передачу повідомлень або отримувати доступ до послуг. Ця послуга схожа на підпис автором або одержувачем документа в реальному житті. Крім того, ця послуга не може перешкодити користувачу відмовити у виконанні певної дії. Однак він може надати доказ того, що може бути збережено та використане пізніше третьою стороною, для вирішення спорів, які виникають у випадках, коли дії відхиляють одним із суб'єктів, які брали участь у акції. Неприйняття може бути надано за допомогою цифрових підписів на основі шифрування відкритого ключа систем. Наявність гарантує, що мережеві послуги та ресурси є доступними та захищеними від подій, що впливають на мережу, таких як шкідливі атаки. Тим більше, що ВМ «розумного дому» піддається прямій відмові в службових атаках, оскільки вона піддається впливу інтернету безпосередньо. Більше того, рішення щодо відновлення після аварій включаються в цю послугу, оскільки внутрішня мережа піддається різноманітним атакам, які призводять до втрати або зменшення доступності [27].

Безпека є важливою та критичною проблемою в середовищі «розумного будинку». Багато домашніх користувачів стурбовані несанкціонованим доступом до

свого будинку та конфіденційністю своїх даних. Однак, це не тривіальне завдання забезпечити безпеку в середовищі «розумного будинку» через його неоднорідний характер, той факт, що він завжди підключений до Інтернету, а також відкриті задні двері безпеки, отримані від користувачів.

Внутрішня мережа «розумного будинку» – надзвичайно неоднорідна мережа, оскільки вона складається з широкого спектру різних пристроїв, додатків та технологій зв'язку, як ми вже описали. У «розумному будинку» є багато пристроїв, таких як вимикачі світла, білі прилади, датчики, камери, телевізори, телефони, ПК та КПК, що мають дуже різні можливості та вимоги, і спілкуються один з одним за допомогою дротової та бездротової мереж. Є такі пристрої, як ПК, які легко обробляють складні обчислення та підтримують функції безпеки [28]. Однак є такі пристрої, як слухавка бездротового телефону, які не мають відповідної обчислювальної потужності через обмежені ресурси (тобто запам’ятовування пам’яті, заряд батареї та обчислювальна здатність). Зазвичай ці пристрої не забезпечують захисту, або вони можуть підтримувати лише прості механізми захисту. Тож, через використання цих пристроїв, зловмисники можуть поставити під загрозу житлові мережі. Крім того, не всі пристрої вимагають однакового рівня безпеки. Він може змінюватися від низького до високого рівня. Різна безпека механізми повинні бути реалізовані залежно від потреб кожного пристрою. Крім того, додатки, що підтримуються в системах «розумного будинку», також різноманітні [29].

Існують програми, які підтримують різні типи даних, такі як аудіо, відеосигнали та інформація датчика низької швидкості, з різними можливостями. Таким чином, кожен додаток має схеми захисту, які повинні бути оптимальними для нього. Програми, які підтримують послуги з високою швидкістю передачі даних (наприклад, мультимедійні програми), потребують механізмів захисту, які не збільшують затримки або тремтіння. Підтримка послуг з низькою швидкістю передачі даних (наприклад, через сенсорну мережу) може бути обмежена для використання складних схем безпеки через споживання електроенергії [30].

Крім того, представивши технологію мереж «розумного будинку», зрозуміло, що внутрішня мережа «розумного будинку» – це абсолютно неоднорідна мережа, яка інтегрує низку різних комунікаційних технологій. свої особливості та недоліки безпеки.

Наприклад, бездротові технології можуть бути легко використані через характер їх трансляції. Зловмисник може перехопити сигнал або порушити нормальну роботу бездротового зв'язку.

З іншої сторони, дротові технології суттєво можуть забезпечити більш безпечний рівень. У середовищі «розумний будинок» також існує безліч бездротових пристроїв, що підтримують широкий спектр послуг, які приєднуються та залишають внутрішню мережу повністю довільно, утворюючи надзвичайно мінливу спеціальну підмережу. Ця спеціальна підмережа надзвичайно динамічна і час від часу змінюється. Таким чином, топологія внутрішньої мережі є динамічною, а це означає, що необхідні механізми захисту повинні динамічно переналаштовуватися щоразу, коли топологія змінюється без втручання домашнього користувача [31]. В іншому випадку внутрішня мережа страждає від кількох вразливих місць безпеки. Однак розгортання механізмів безпеки у спеціальній мережі є складним питанням через притаманну їй динамічну природу. Таким чином, рішення щодо безпеки щодо спеціальних мереж повинні базуватися на динамічних механізмах безпеки з достатньою кількістю інтелекту для запобігання порушенням безпеки.

Крім того, розширення внутрішньої мережі «розумного будинку» на зовнішній світ через Інтернет створює багато проблем із безпекою мережі, оскільки вона піддається різним кібератакам, таким як DoS–атаки, шкідливе програмне забезпечення, підслуховування тощо. На відміну від набору номера підключення до Інтернету [32].

Домашні високошвидкісні з'єднання забезпечують постійне підключення до Інтернету, що передбачає статичну IP–адресу. Той факт, що IP–адреса не змінюється, змушує легко зламати внутрішню мережу, оскільки зловмисники мають багато часу, щоб вгадати IP–адресу та зламати підключені пристрої. Більше того,

внутрішня мережа піддається всім застарілим атакам безпеки відкритої мережі, оскільки вона доступна через Інтернет [33].

По–перше, зловмисники можуть спричинити загрозу в середовищі «розумного будинку», оскільки вони можуть перехоплювати та змінювати віддалені повідомлення мереж (тобто мережа Powerline , мережа телефонної лінії, бездротові мережі), які складають внутрішню мережу «розумного будинку». Крім того, зловмисники можуть поставити під загрозу внутрішню мережу та використовувати її для запуску атак проти інших мереж, що охоплюють їх доріжки. Супротивники також можуть використовувати обчислювальну потужність та ресурси компрометованої внутрішньої мережі для атак відмови в сервісі проти інших вузлів Інтернету. Також супротивники можуть отримати доступ через Інтернет для конфіденційної інформації користувачів, що підслуховують їхній інтернет–трафік. Наприклад, перехоплювати повідомлення про трансакції, що надходять в електронний банк, супротивники можуть дізнатися номер кредитної картки, можуть отримати пароль механізму блокування будинку для того, щоб його пограбувати [34]. Тому, завдяки неоднорідності пристроїв, додатків та комунікаційних технологій у середовищі «розумного будинку», динамічній природі внутрішньої мережі, а також швидкий постійний зв’язок з зовнішнім світом, не існує єдиного рішення безпеки, яке здатне надати усі необхідні користувачу служби безпеки, щоб зменшити ризик атак безпеки. Отже, проблеми зі страхуванням безпеки можна вирішити за допомогою різноманітних механізмів, протоколів та служб безпеки, які слід інтегрувати і керують ними у внутрішній мережі «розумного будинку». Більшість користувачів, як правило, не є професіоналами в галузі мереж, а також у галузі безпеки мережі. Однак вони зазвичай будують внутрішню мережу без участі фахівців із безпеки. Таким чином, у внутрішній мережі завжди можуть бути слабкі місця безпеки. [35].

Виявлення вторгнення використовується як друга лінія захисту для захисту внутрішньої мережі «розумного будинку», оскільки як тільки виявлено вторгнення, може відбутися відповідь, щоб мінімізувати збитки. У випадку, якщо зловмиснику вдасться здійснити напад на внутрішню мережу «розумного будинку», системи

виявлення вторгнень (IDS) можуть виявити цю атаку і зупинити діяльність зловмисника. У «розумному будинку» внутрішня мережа може використовуватись як мережевий IDS, так і хост IDS [35].

Мережеві IDS використовують дротові мережі, де моніторинг трафіку відбувається за комутаторами, маршрутизаторами та шлюзами. Однак IDS як хости використовуються у спеціальних мережах, де немає таких точок концентрації трафіку. Ідентифікатори, що базуються на хості, переймаються тим, що відбувається на кожному окремому вузлі спеціальної мережі [36].

Техніка виявлення зловживань вимагає аудиторських даних для аналізу та порівняння цих даних з уже відомими моделями атак, що зберігаються у великих базах даних. У випадках, коли будь–яке порівняння між аудиторськими даними та відомими моделями атак призводить до відповідності, встановлюється сигнал про вторгнення. Основна перевага методики виявлення зловживань полягає в тому, що вона може точно і ефективно виявити випадки відомих атак. Однак ця методика не в змозі виявити щойно винайдені напади. З іншого боку, методика виявлення аномалій заснована на статистичній поведінці. Детектори аномалії шукають поведінку, яка відхиляється від нормальної активності в мережі. Перш за все, ця методика вимагає збору аудиторських даних для аналізу. Потім дані аудиту перетворюються у формат статистично порівнянні з профілем користувача, що генерується динамічно та оновлюється на основі використання користувача. У випадку, коли будь–яке порівняння між аудиторськими даними та профілем користувача призводить до відхилення, яке переходить встановлений поріг, активується сигнал про вторгнення.

Основна перевага методики виявлення аномалії полягає в тому, що вона може виявляти невідомі або нові вторгнення, не вимагаючи попередніх знань про вторгнення. Основним недоліком цієї методики є те, що вона може не в змозі описати, що таке напад [36].

1.8 Технології безпеки для «розумних будинків»

Найбільш важливими технологіями безпеки для забезпечення безпеки внутрішньої мережі «розумного будинку» є механізми аутентифікації та авторизації. Обидва механізми необхідні для того, щоб обмежити доступ будь–якої шкідливої особи до внутрішньої мережі «розумного будинку». Крім того, використання брандмауерів є ще одним механізмом запобігання вторгнень, який важливий для підвищення безпеки в середовищі «розумного будинку». Однак самих механізмів запобігання вторгнень недостатньо для внутрішньої мережі «розумного будинку» через її складність та неоднорідність. Тому необхідно також використовувати системи виявлення вторгнень (IDS) [36].

Процес аутентифікації включає автентифікацію сутності та автентифікацію повідомлень. Автентифікація особи забезпечує автентичність сутності, а автентифікація повідомлення підтверджує, що отримане повідомлення походить від правого відправника. Існують механізми аутентифікації сутності, а також аутентифікації повідомлень. Механізми аутентифікації сутності підтримують два процеси; процес ідентифікації та процес верифікації. У процесі ідентифікації суб'єкт господарювання вимагає доступу до мережі, яка вимагає певної ідентичності на основі ідентифікатора [37].

Процес верифікації базується на трьох підходах : доказ знанням, доказ володінням та доказ власністю. Підхід доказування знаннями враховує те, що знає користувач. Цей підхід зазвичай перевіряє секретний пароль або ідентифікатор користувача, який вимагає доступу. Механізми аутентифікації, засновані на такому підході, називають механізмами аутентифікації на основі ID–пароля. Підхід доказування володіння залежить від того, чим володіє користувач. Цей підхід заснований на власності на смарт–карту, яка повинна бути підключено під час процесу входу.

Підхід щодо доказування власності ґрунтується на тому, що є користувачем. У цьому підході верифікатор вимірює певні біометричні властивості (наприклад, відбиток пальців, райдужка,сітківка) користувача. Механізми аутентифікації, засновані на такому підході, називають механізмами аутентифікації на основі біометричних даних [37].

На відміну від внутрішньодоменних механізмів аутентифікації, що відбуваються в середовищі «розумного будинку», механізми аутентифікації між доменами застосовуються поза середовищем. Механізми аутентифікації внутрішньодоменних включають механізми аутентифікації, засновані на доказі знаннями, підтвердженням володіння та доказ власними підходами.

Однак механізми аутентифікації для міждоменів включають механізми аутентифікації, засновані на доказі знаннями та підтвердження методами володіння. Механізми аутентифікації, що використовують біометричну інформацію, не використовуються для міждоменної аутентифікації. Це трапляється через те, що, коли біометрична інформація розкривається зловмисникам, користувач не може обмінятися відкритою біометричною інформацією на нову, оскільки модифікація людського тіла дуже складна. Таким чином, це призводить до серйозного порушення конфіденційності у випадках виявлення біометричної інформації. Отже, не логічно використовувати механізми аутентифікації на основі біометричних даних у додатках, які вимагають передачі біометричної інформації через Інтернет [37].

У середовищі «розумного будинку» механізм аутентифікації кидає виклик доманьому користувачеві надавати свою унікальну інформацію. Якщо механізм аутентифікації може переконатися, що інформація представлена правильно,то користувач аутентифікується. Крім того, для отримання доступу до будь–якого мережевого ресурсу чи послуги для домашнього користувача потрібно лише один раз пройти автентифікацію. Якщо аутентифікація не вдається, це призводить до відхилення або припинення доступу та створення звіту до центру управління безпекою. Крім того, є випадки, коли домашній користувач бажає отримати доступ до віддаленого сервера додатків, який виконує власну аутентифікацію. У цих випадках користувач ідентифікується за допомогою житлового шлюзу, і він робить необхідну автентифікацію з віддаленим сервером замість користувача. Це трапляється тому, що житловий шлюз має функцію відображення автентифікації, яка досягає відображення між механізмами аутентифікації для внутрішньодоменного і механізмами аутентифікації для міждоменних [38].

1.9 Висновки до розділу

Протягом останніх десятиліть концепція «розумного будинку» почала стрімко розвиватися, але вона стикається з винятковими проблемами. Проте нещодавні події в інформаційно–комунікаційних технологіях призвели до розвитку інтелектуального будинку на хорошому рівні зрілості. «Розумний дім» – це середовище для життя, яке включає в себе відповідну технологію, яка називається технологією «розумного будинку», для досягнення цілей комфортного проживання, безпеки життя та ефективності.

2 ОГЛЯД АПАРАТНИХ ТА ПРОГРАМНИХ РІШЕНЬ ДЛЯ СИСТЕМИ БЕЗПЕКИ «РОЗУМНОГО БУДИНКУ»

2.1 Апаратні рішення

В повсякденному світі інтелектуальна автоматика дає змогу управляти автоматизованими системами «розумної домівки», користувачу дається можливість створювати для себе комфортні умови через телефон чи ноутбук – це може бути як температура в кімнаті, так і рівень вологості або світло, і саме основне забезпечувати безпечне проживання. Така мережа включає такі об'єкти автоматизації як контроль клімату та проникнення, відповідає за збереження енергоресурсів та керування світлом [39].

2.1.1 Управління освітленням

Система «розумноного дому» дозволяє керувати освітленням за натисканням однієї кнопки. Завдяки наявності пульту стає можливим налаштовування ламп, люстр, світильників так як завгодно користувачу.

Датчик руху забезпечить вмикання та вимикання освітлення автоматично. Система «розумного будинку» позбавить вас від необхідності встановлювати купу непотрібних вимикачів. Їх можна буде замінити зручними сенсорами. Сенсорні вимикачі дозволять регулювати яскравість, а також включити або вимкнути світло. Вночі світло буде вмикатися на меншу яскравість [40].

Також система дає змогу управляти освітленням дистанційно з ПК або з телефону. На рисунку 2.1 показано схему для керування світлом «розумного будинку».

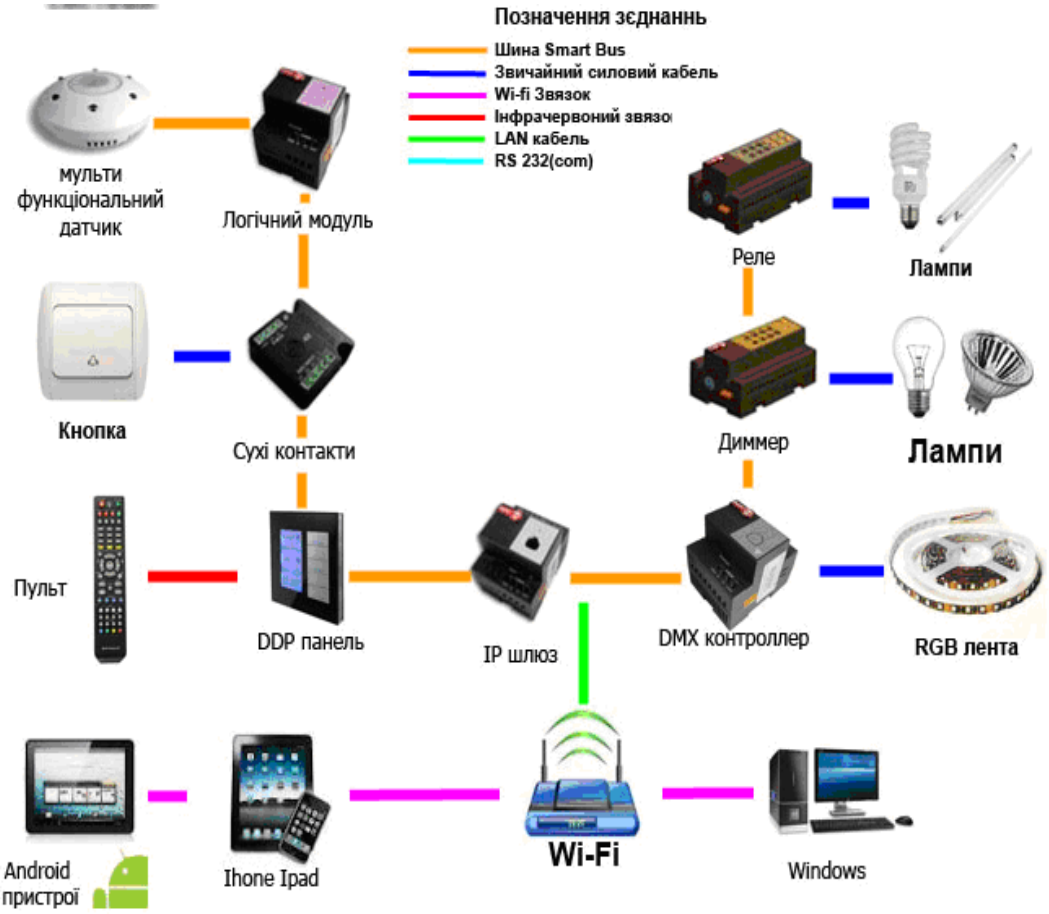

Рисунок 2.1 – Схема керування світлом «розумного будинку»

Система «розумного дому» допомагає економити електроенергію і термін користування лампами. Також вона є зручна у використанні так як більше немає необхідності шукати вимикачі світла. Система сама здатна вирішувати яке освітлення потрібно у приміщенні, наприклад легке підсвічування перед сном щоб не дратувати очі, або яскраве при пахмурній погоді [41].

Систему освітлення можна налаштувати так, що вона сама здатна буде визначити в якій частині буде знаходитися людина щоб освітлювати саме її. Таке управління освітленням може бути не тільки завдатком комфорту, а й безпеки також. «Розумний будинок» самостійно може вмикати світло тим самим імітуючи присутність людей.

2.1.2 Контроль клімату

Система контролю клімату працює з допомогою алгоритмів, закладених у неї заздалегідь. Вона підтримує параметри повітряного середовища і різних кліматичних зон при цьому затрачує мінімум енергії [42].

Охолоджується або нагрівається розміщення завдяки цій системі. При цьому кондиціонер та опалення працюють одночасно.

Система контролю клімату коригує температуру, вологість, контролює приток свіжого повітря, і одночасно виконуючи таку кількість функцій, забезпечує економію ресурсів та вирішує проблему збереження енергії. Така система є дуже зручною та корисною, так як дозволяє зниження температури в нічний час в пустих приміщеннях, тим самим створює зручні умови для сну. Також можна апаратуру і обладнання можна ставити в режим так званого «сну» під час відсутності користувачів або взагалі повністю виключити систему. Перед поверненням додому користувач може заздалегідь встановити в приміщеннях потрібний йому режим клімату через відділений доступ або інтернет [43].

На рисунку 2.2 зображено схему керування кліматом «розумного будинку».

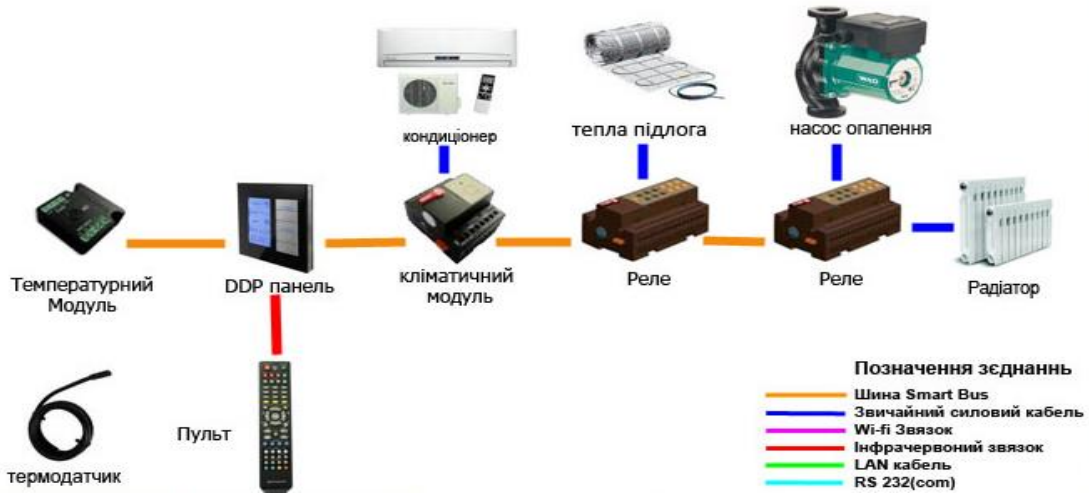

Рисунок 2.2 – Схема керування кліматом «розумного будинку»

На рисунку можна побачити DDP панель, яка може мати під своїм контролем ще 8 температурних зон. Для цього просто необхідно додати температурний модуль в систему, а до нього підключити ще чотири датчика що відповідають за температуру. Також, якщо в системі опалення декілька насосів, що подають гарячу

воду в різні приміщення або поверхи, то завдяки їм можна окремо контролювати клімат в різних кімнатах. Модуль що відповідає за клімат ідеально підходить для контролю кондиціонерів. Він містить виходи що керують режимом нагріву та режимом охолодження, та відповідає за швидкість вентилятора і т.д. [43]. Завдяки своїм функціям система контролю клімату створює здоровий і комфортний мікроклімат для користувачів.

Тепер деякі системи розумного дому не мають функції бездротоваго з'єднання через всесвітню павутину. Але телефони які мають постійний доступ інтернету є на сьогодення звичним для нас явищем, бо є майже у кожного.

Є два можливі варіанти застосування хмарних обчислень в мережі розумного дому. Перший варіант – при наявності доступу до інтернету то керування системами може відбуватися звідки завгодно, для цього не є обов'язковим розташування контролеру чи серверу в самому будинку. Другий варіант – контролер може знаходитися в приміщенні, але при цьому хмара буде забезпечувати тільки віддалене керування – все ПЗ буде встановлено на «хмарі»[44].

2.1.3 Економія енергії

Система економії енергії світла в багатоповерховому будинку (автостоянка, підвал, під'їзд тощо) дозволяє заощадити кількість електроенергії в декілька раз. Ці системи застосовують пристрій управління світлом з роздільними силовими компонентами, завдяки чому використовують існуючі лінії електропередач [45]. За рахунок природного світла що на максимум можна використовувати протягом дня , при правильну плануванні будинку теж можна значно заощадити електроенергію. Великий ефект дає навіть сама економна лампа або світлодіодна лампа, потужність якої регулюється датчиком присутності. Тобто якщо користувач забуде вимкнути світло, то система зробить це за нього, так як помітить що в приміщенні нікого немає [45]. На рисунку 2.3 можна розглянути просту схему керування освітленням.

Рис. 2.3 – Проста схема освітлення «розумного будинку»

В основу функції збереження енергії поставлено контролер для температури та електроконвектори, вони пожежобезпечні та не дають повітрю бути сухим. У щиті для захисту системи від перенавантажень та замикання монтують автоматичні вимикачі. В системі використовують тільки якісне та надійне обладнання. Такою системою дуже легко керувати, керування можна здійснювати за допомогою контролеру та датчиками і розетками [46].

2.1.4 Контроль проникнення

Охорона «розумного дому» відіграє дуже важливу роль. При вході розміщено кодову панель, з якої можна буде відключити сигналізацію. Якщо користувач або зловмисник введе не правильний код то система «розумного будинку» включить сигналізацію та надішле повідомлення власникам будинку про проникнення [47].

Для впевненості того що в дім ніхто не проникне користувач може використовувати різні датчики. Наприклад для вікон та дверей можна використовують датчики , що одразу повідомляють про відкриття та закриття – геркони (рис.2.4).

Рисунок 2.4 – Гекони

Виявити проникнення через вікна можна буде завдяки датчикам руху, які розташовують по всьому будинку. Також в будинку можна монтувати датчики, що повідомляють про розбите скло на вікнах або дверях (рисунок 2.5). В кімнатах монтують датчики що ловлять рух/присутність [48].

Рисунок 2.5 – Датчик руху та датчик розбиття скла

Якщо за захист будинку відповідає охоронна компанія, то в разі небезпеки сигнал буде відправлено на пульт охорони. В противному випадку будинок сам надішле повідомлення користувачу, буде вмикати світло в усьому будинку, заблокує двері та вікна, увімкне сирену, або може будь яка реакція, яку запрограмує користувач [48]. До прикладу в «розумному будинку» Inels є два елементи, які відповідають за доступ до помешкання – клавіатура безпеки та панель що зчитує картки (рисунок 2.6).

Рисунок 2.6 – Панель для читання карток та клавіатура безпеки

Клавіатура служить не тільки для вмикання або вимикання охоронної системи, вона також захищає паролем будь які команди. Панель, має ті ж самі функції, також дозволяє організацію різних рівнів доступу.

2.1.5 Захист в надзвичайних ситуаціях

Якщо до до мережі «розумного будинку» підключено захист від протікання води чи потопів, газу чи навіть пожежу, то на телефон користувача буде вислано сигнал про те що є неполадки [49]. На рисунку 2.7 показано максимальну схему для захисту «розумного будинку» в надзвичайних ситуаціях.

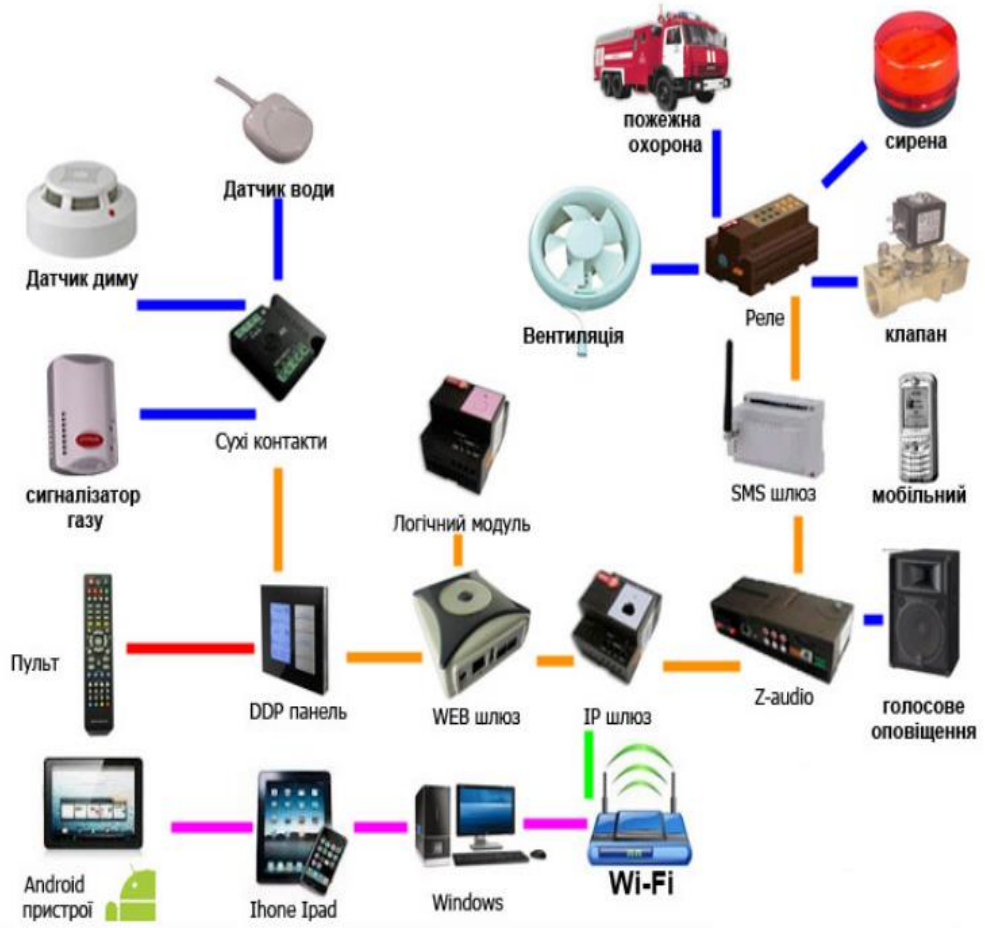

Рисунок 2.7 – Схема захисту в надзвичайних ситуаціях в «розумному будинку»

На схемі показано модуль, який може при різних ситуаціях відсиати оповіщення, а також вести керування «розумним будинком» за SMS, які надсилає користувач [50]. Також якщо додати IP шлюз та маршрутизатор то буде змога вести спостереження за системою з ПК, але якщо є відповідне програмне забезпечення, а веб– шлюз в свою чергу– дає робить можливим робити це віддалено, тобто через інтернет. За аналіз з датчика відповідає логічний модуль, також приймає деякі комплексні рішення: до прикладу, якщо спрацює датчик диму або газу, то вже не дасть змоги вентилятору працювати. В аудіо програмують голосові оповіщення різного типу на будь який випадок [51].

2.2 Програмні рішення

Загроза інформації може бути різна, це може бути як випадкова так і навмисна загроза. Інформаційна безпека – це сукупність правил або процесів, що захищають інформацію. Загроза – це все, що може негативно вплинути на дані користувача та інформацію якою він володіє. Загрози можуть бути внутрішніми чи зовнішніми, фізичними чи ні [52].

Види загроз інформації наведено на рисунку 2.8.

Рисунок 2.8 – Види загроз

Зазвичай часто користувач, адміністратор чи інші особи, що обслуговують чи використовують систему можуть ненавмисно створити загрозу [53].

2.2.1 RSA

RSA являється алгоритмом, який підходить як для кодування такі для розшифрування повідомленя. Це асиметричний криптографічний алгоритм. Асиметриність означає, що є дві різні клавіші. Також підходить для цифрового підпису [54]. Принип роботи показано на рисунку 2.9.

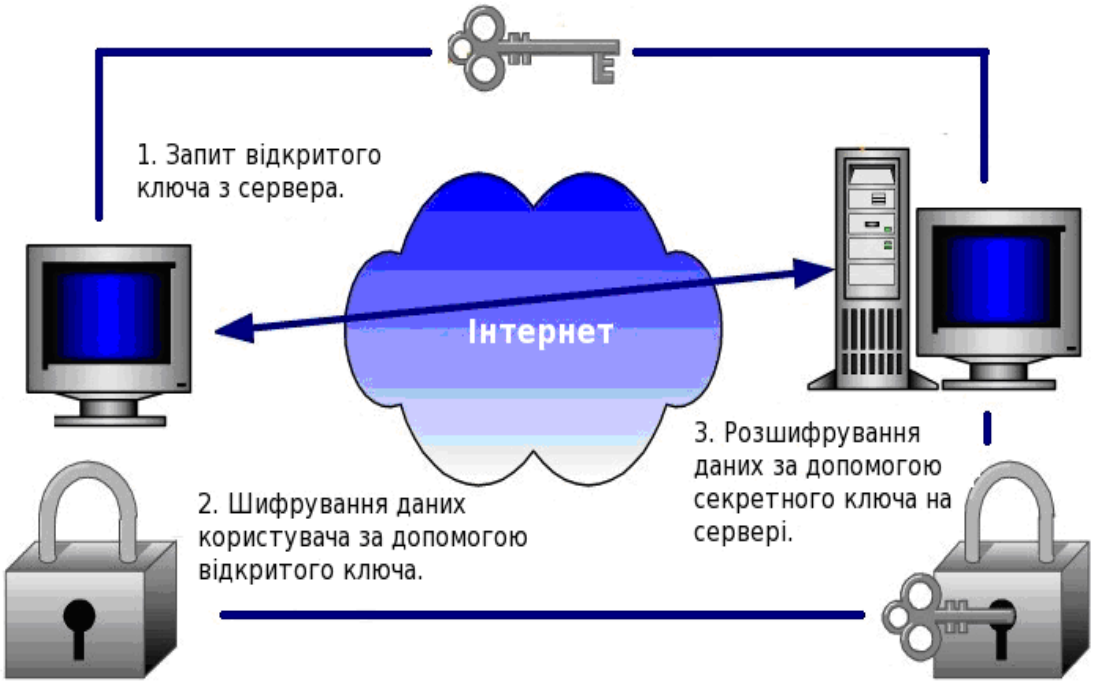

Рисунок 2.9 – Принцип роботи RSA

Якщо користувач володіє приватним ключем то він з легкістю зможе розшифрувати закодоване повідомлення. Цей алгоритм включає в себе такі етапи, як генерацію та розповсюдження ключів. Безпеку алгоритма гарантує використання двох ключів [54].

2.2.2 Google Cloud Platform

Google Cloud Platform – інтегрований хмарний сервер надається компанією Google, що побудований на такій же інфраструктурі, Google Search і YouTube [55].

GCP дає такі можливості, як:

– google Cloud Monitoring – забезпечує хмарні додаткии оповіщеннями та панеллю моніторингу;

– google Cloud Logging – дає змогу перегдяду, фільтрації та експорту інформації через збережені журнали;

– google Cloud audit logs – зберігає дані про анміністрацію та доспут до даних з Cloud Platform, які в подльшому використовують для аудиту.

Якщо більшість пристроїв реагують на деякі зовнішні події, то платформа використовує шипи для обробки інформації. Далі йде буферизація шипів для ізоляції їх від додаткі для моніторингу даних.

Cloud Pub / Sub підключається до сервісів хмарної платформи, для підключення прийому інформації, шлюзів та систем зберігання цієї інформації. При включенні різних компонентів застосування можна підписатися на деякі ресурсні потоки, при цьому не обов'язково будувати індивідуальні абонентські канали на кожному пристрої [55].

З зовнішнього світу інформація приходить різних форм і розмірів, тому хмара дає можливість обирати як саме користувач буде зберігати цю інформацію. Це можна робити через зображення, відео потоки, також можливе структуроване збереження показників девайсів або транзакцій.

Firebase (рисунок 2.10) підходить для підтримки локального стану пристроїв, вона надає такі функції, як аналітика, бази даних, обмін повідомленнями та звіти про аварійне, користувач може швидко орієнтуватися яко з пристроями щось не так. Firebase побудований на інфраструктурі Google і автоматично масштабується навіть для найбільших додатків. Продукти Firebase відмінно працюють індивідуально, але обмінюються даними і знаннями, тому вони працюють ще краще разом. Декі пристрої можуть бути підключені до 30 апаратних приладів. Також гаджети можуть існувати на рівні додатків. Часто стає необхідним для іншого ПО зміна останніх налаштувань гаджетів. Їх треба синхронізувати з сервером, і тоді коли вони будуть у стані сну то дані до них будуть доступні. Також Firebase ключі дають нам дані про поточний стан гаджету. Клієнтські бібліотеки Firebase полегшують видачу інформації різним користувачам [56].

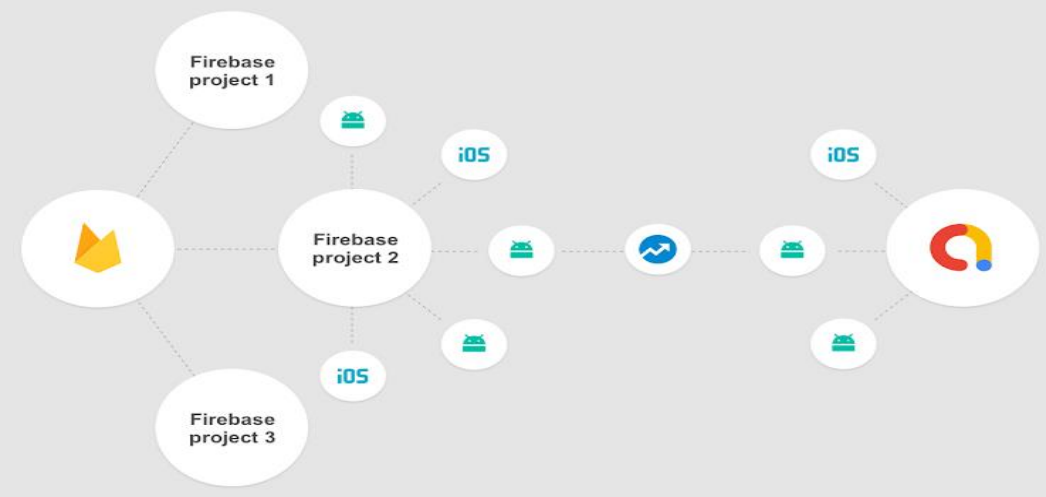

Рисунок 2.10 – Схема роботи Firebase

Платформа представляє собою повністю керований сервіс для робочих навантажень Oracle з провідними партнерами. Платформа відкрита для підключення, моніторингу та захисту мікросервісів.

Модернізація на місці з використанням відкритої, безпечної і ефективної хмари. Надає користувачам простий і швидкий доступ до хмарних інструментів і звільняє IT–відділ від адміністративних завдань за допомогою Chrome Enterprise [57].

2.2.3 Samsung Smart Home

Спеціалізується на наданні ПЗ на базі Android, що легко встановлюється на Samsung девайси та отримує дані з хмари без написання спеціального ПЗ [58].

Smart Home Cloud API дає можливість керувати SSH гаджетами. Додаток SHService Control надає розширені послуги клієнтам та з'єднує з різними приладами. SHService Control працює за принцципом хмара–хмара між клієнською хмарою і SHCloud. SHData Model відповідає за структуру даних в форматі JSON та подає сигнали SSH приладам, таким як холодильник, кондиціонер, пральна машина, очищувач повітря, пилосос, сушарка та піч [58].

Покрокова інтеграція користувачів (партнерів) SHC:

– аутентифікація. Для з'єднання з девайсами Samsung, система стежить за авторизацією в акаунті Samsung. Тобто, користувач має можливість спілкуватися з SHC, якщо він має маркер, який, отримав після аутентифікації. Samsung

аутентифікація є унікальною системою, вона являється єдиним акаунтом на всі прилади від Samsung;

– відкриття. Спостерігач має можливість отримувати список всіх "розумних" домашніх гаджетів, які зареєстровані для конкретного користувача, отримуючи таку інформацію про них як тип, модель пристрою, версія та навіть назву;

– зондування. Спостерігач може відправляти запит на інформацію про стан будь якого гаджету;

– підписка. Користувач має змогу реєструвати оповіщення про будь які зміни в Smart Home гаджеті, далі отримувати інформацію в режимі реального часу;

– сповіщення. Якщо SHC помічає зміну в стані гаджету, то система відправить дані і повідомить стан користувачу;

– контроль. З допомогою хмари Smart Home ористувач може керувати будь яким пристроєм;

– скасування підписки. Користувач може відмовитися від надходження сповіщень про зміну девайсу, але після цього він не отримає будь–яких оповіщень від самого пристрою.

Цей пакет послуг являється платним від початку. Також надається доступ довсіх послуг відразу таавтоматично відбувається розширення, але залежить від нових версій та оновлення платформи. При тому платформа при тому підтримує зв‘язок лише з пристроями, які випускає компанія Samsung. Це є мінусом, бо знижується можливість тестування бюджетної реалізації даної платформи [58].

2.3 GL SmartHome Cloud Solution

В наш час завдяки стрімкому інтегруванню технологій вже мало кого можна здивувати підсистемою «розумний будинок». Але не все так просто, як здається: не дивлячися на популярність смарт будинків до тепер не було сервісу який би давав дозвіл управляти девайсами різних фірм. Тож розобники GlobalLogic створилаи своє ПЗ Gateway SDK, яке дає можливість управляти різними гаджетами розумного дому [59].

2.3.1 Реалізація

GL SmartHome Cloud Solution — це готовий продукт, що дає можливість автоматизувати роботу великої кількості функцій (управління опаленням, освітенням, перевіряти рівень забруднення в повітрі і т. д.) «розумного дому» або для цілого «розумного міста» [59].

На даний момент платформа має демо версію що функціонує (демостенд): це маленький дім, що обладнаний новими сучасними устаткуваннями що використовують провідні IoT–технології (Java, Docker, РБД)(рисунок 2.11).

Smart–home– це програма, яка створювалася для того щоб прилади від різних виробників мали могли працювати одне з одним в спільному середовищі. Програма має додаток на базі Android, чим саме дає змогу користувачу управляти та/або спостерігати за усіма пристроями «розумного дому» віддалено, через телефон чи ПК. Ця програма розроблена для компанії США, вона вже отримала усі необхідні сертифікації, але не виходу на український ринок зараз в планах немає [59].

Рисунок 2.11 – Smart Home Cloud Solution

Суть платформи полягає в тому, щоб об'єднати прилади через модуль IFTTT (IfThisThenThat) які раніше не могли працювати в одному середовищі, тобто прилади від різних фірм і виробників.

На сьогоднішній день хмарний сервіс може підтримувати п'ятдесят п'ять пристроїв, і їхня кількість буде тільки збільшуватися. Наприклад, в списку є об'єднані є лампи від Philips, термостат від Honeywell, камера від фірми Nest. Віддалений доступ користувачу до розумного дому забезпечують такі бездротові інтерфейси, як Zigbee, Z–Wave та Wi–Fi [60].

2.3.2 Архітектура

Платформа побудована за догмомогою сервісів Амазон, серед яких:

– EC2 (Обчислювальна хмара) — відповідає за інфраструктуру серверів;

– ECS (Служба контейнерів) — для централізованого з’єднання контейнерів і безпосередньо керування ними користується докером;

– RDS (Реляційна база даних) — база даних на окремому сервері,де зберігаються дані про користувачів та сценарії;

– IoT — використовує MQTT брокер;

– SQS (Сервіс Amazon Simple Queue) — відповідає за формування черги для додатків Java;

– SES (Простий сервіс електронної пошти Amazon) — мейл–сервіс від Амазон;

– SNS (Проста служба сповіщень Amazon) — сервіс що відповідає за сповіщенння.

Сервіси, що використовувалися було поділено на три кластери:

– кластер з додатками для wtb і API, що дає доступ до елементів розумного дому через зовнішню мережу;

– logic–кластер, який в свою чергу має такі підкластери як:

– сервер часу;

– служба оповіщення;

– шлях до хмари;

– правило двигуна;

– кластери адаптерів, які з’єднують пристрої через додаток з cloud–ом виробників приладів.

Сервіси Амазон були вибрані для реалізування цього проекту через свою гнучкість, адаптивність та стабільність. Розробники додали також і Amazon Alexa Voice Service (AVS) (рисунок 2.12), яка була запрограмована для взаємодії з хмарою і керування розумним домом через ту саму хмару. Використовуючи набори для інтеграції багатофункціональних функцій цифрового помічника з підтримкою AI – створили нові ринкові можливості для ряду пристроїв IoT, включаючи інтелектуальні пристрої, пристрої віртуального помічника і навіть іграшки [60].

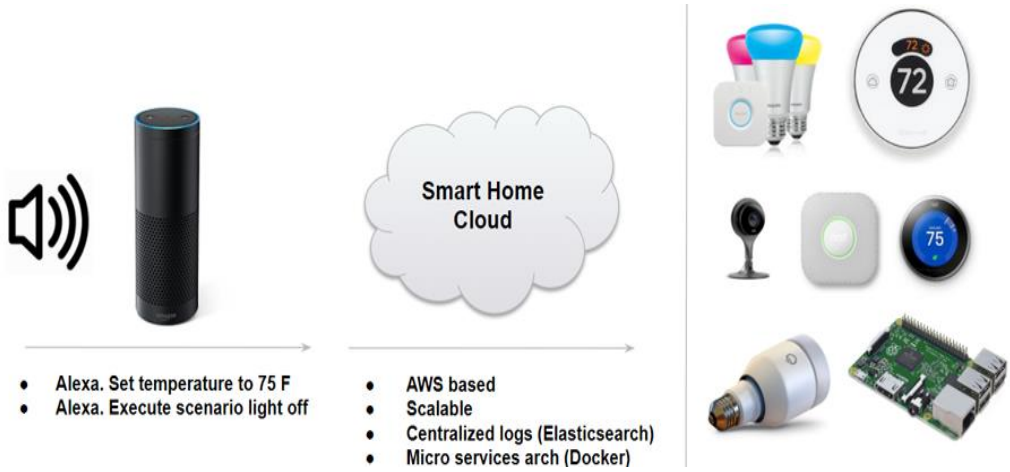

Рисунок 2.13 – Amazon Alexa Integration

Комплекс включає в себе Gateway SDK на базі Raspberry 2/3 програма для телефону на базі Android.

Шлюз SDK на базы Raspberry PI 2/3 може здійснювати конект між девайсами, що "спілкуються" при цьому використовувати такі інтерфейси Z–Wave, Zig–Bee, Wi–Fi, та можуть здійснювати двохсторонній контакт із хмарою, через протокол MQTT. Передбачає змогу виконання IFTTT сценарію, коли нема можливості зв'язатися з хмарою, надсилання оповіщення про зміни в приладі на телефон [60].

Мобільний продукт у вигляді додатку в свою чергу демонструє функції хмари і вчить, як вірно їх використовувати.

2.4 Висновки до розділу

Так як основними завданнями "розумного будинку" є комфорт та безпека, в розділі було представлено апаратні та програмні рішення для середовища "розумного будинку". Безпека є дуже важливою, так як це впливає на приватне життя користувачів, тому були обговорені різноманітні важливі проблеми щодо безпечного проживання в такому будинку. Були представлені існуючі механізми безпеки, що її забезпечують. У багатьох випадках більшість домашніх користувачів недостатньо обізнані з безпекою, щоб усвідомити наслідки середовища. Однак важливість безпеки буде піднята в майбутньому через зростаючу складність та неоднорідність внутрішніх мереж та все більш широке використання віддалених робочих звичок для домашніх користувачів. Крім того, слід встановити операційні системи та прикладне програмне забезпечення та налаштувати його правильно, щоб уникнути проникнення або атак на домашню мережу.

3 СПЕЦІАЛЬНА ЧАСТИНА

3.1 Класифікація загроз безпеки інформації

Під загрозою безпеки інформації розуміють подію або дію, яка може викликати зміну функціонування системи, пов'язане з порушенням захищеності оброблюваної в ній інформації.

Вразливість інформації – це можливість виникнення такого стану, при якому створюються умови для реалізації загроз безпеки інформації.

Атакою на інформаційну систему називають дії, що робляться порушником, яке полягає в пошуку і використанні тієї або іншої уразливості. Інакше кажучи, атака на КС є реалізацією загрози безпеки інформації в ній.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи [61]:

– перехоплення інформації – цілісність інформації зберігається, але її конфіденційність порушена;

– модифікація інформації – вихідне повідомлення змінюється або повністю підміняється іншим і відсилається адресату;

– підміна авторства інформації. Дана проблема може мати серйозні наслідки.

Наприклад, хтось може послати лист від чужого імені (цей вид обману прийнято називати Спуфінга) або веб – сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

Специфіка комп'ютерних мереж, з точки зору їх уразливості, пов'язана в основному з наявністю інтенсивного інформаційної взаємодії між територіально рознесеними і різнорідними (різнотипними) елементами. Вразливими є буквально всі основні структурно–функціональні елементи КС: робочі станції, сервери (Host–машини), міжмережеві мости (шлюзи, центри комутації), канали зв'язку і т.д. Відомо велика кількість різнопланових загроз безпеці інформації різного походження. У літературі зустрічається безліч різноманітних класифікацій, де в якості критеріїв

розподілу використовуються види породжуваних небезпек, ступінь злого умислу, джерела появи загроз і т.д. Одна з найпростіших класифікацій наведена на рис. 3.1.

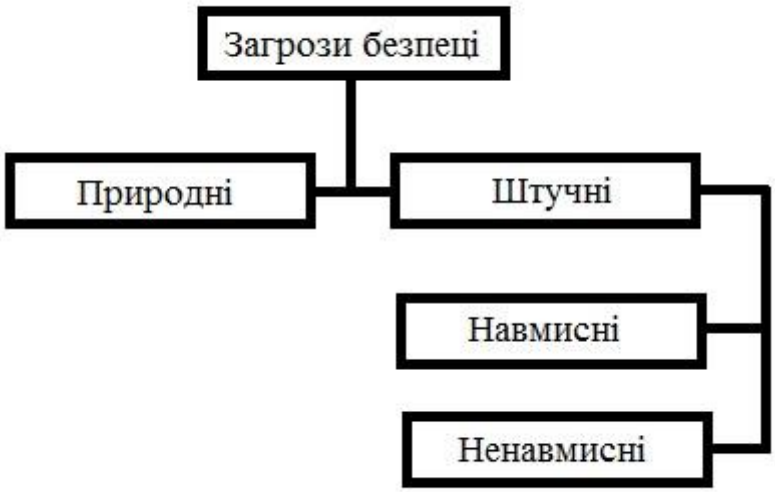

Рисунок 3.1 – Класифікація загроз

Природні загрози – це загрози, викликані впливами на інформаційну систему і її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози – це загрози інформаційну систему, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

– ненавмисні (ненавмисні, випадкові) загрози, викликані помилками в проектуванні інформаційну систему і її елементів, помилками в програмному забезпеченні, помилками в діях персоналу і т.п .;

– ненавмисні (навмисні) загрози, пов’язані з корисливими діями людей (зловмисників).

Джерела загроз по відношенню до інформаційної системи можуть бути зовнішніми або внутрішніми (компоненти самої інформаційної системи – її апаратура, програми, персонал) [61].

Аналіз негативних наслідків реалізації загроз припускає обов'язкову ідентифікацію можливих джерел загроз, вразливостей, що сприяють їх прояву і методів реалізації. І тоді ланцюжок виростає в схему, представлену на рис. 3.2.

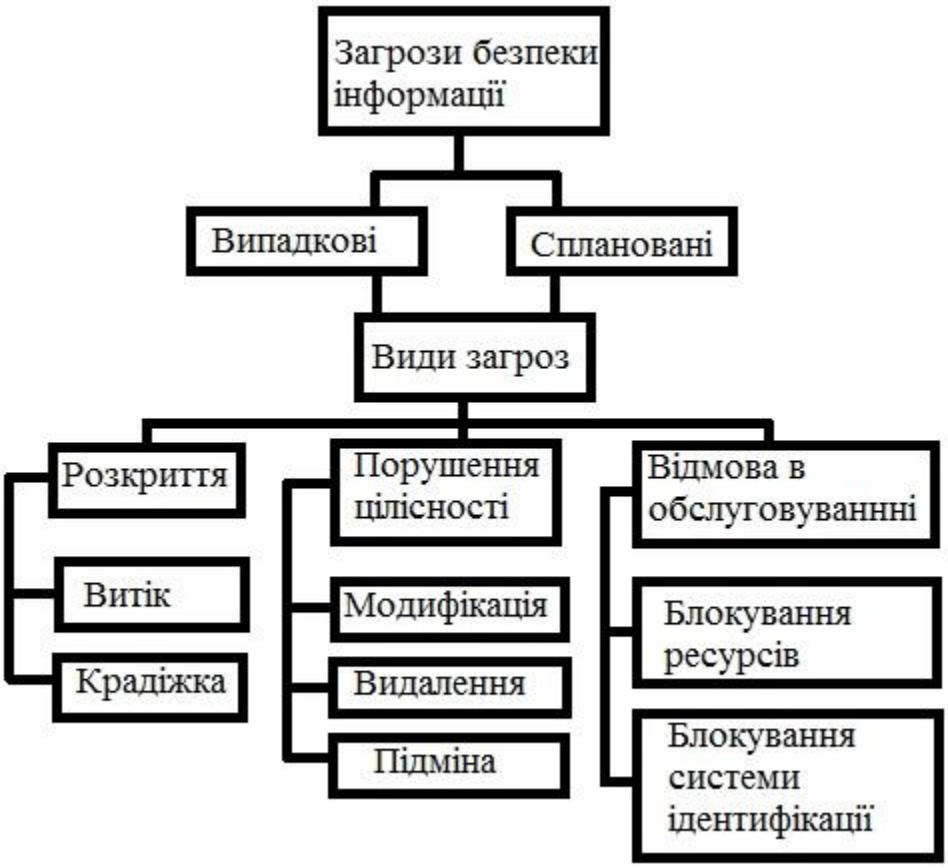

Рисунок 3.2 – Види загроз безпеки інформації в комп’ютерних мережах

Загрози класифікуються за можливості нанесення шкоди суб'єкту відносин при порушенні цілей безпеки [61]. Збиток може бути заподіяна будьяким суб'єктом (злочин, вина або недбалість), а також стати наслідком, не залежних від суб'єкта проявів. Загроз не так вже й багато. При забезпеченні конфіденційності інформації це може бути розкрадання (копіювання) інформації і засобів її обробки, а також її втрата (ненавмисна втрата, витік).

При забезпеченні цілісності інформації список загроз такий: модифікація (спотворення) інформації; заперечення автентичності інформації; нав'язування неправдивої інформації. При забезпеченні доступності інформації можливе її блокування, або знищення самої інформації і засобів її обробки. Класифікація можливостей реалізації загроз (атак), являє собою сукупність можливих варіантів дій джерела загроз певними методами реалізації з використанням вразливостей, які призводять до реалізації цілей атаки.

Мета атаки може не збігатися з метою реалізації загроз і може бути спрямована на отримання проміжного результату, необхідного для досягнення надалі реалізації загрози. У разі такого неспівпадіння атака розглядається як етап підготовки до вчинення дій, спрямованих на реалізацію загрози, тобто як «підготовка до вчинення» протиправної дії. Результатом атаки є наслідки, які є реалізацією загрози і / або сприяють такої реалізації. Вихідними даними для проведення оцінки та аналізу загроз безпеки при роботі в мережі служать результати анкетування суб'єктів відносин, спрямовані на з'ясування спрямованості їх діяльності, передбачуваних пріоритетів цілей безпеки, завдань, що вирішуються в мережі і умов розташування та експлуатації мережі.

3.2 Найбільш поширені загрози

Найчастішими і найнебезпечнішими (з точки зору розміру шкоди) є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують комп'ютерну мережу [61].

Іноді такі помилки і є власне погрозами (неправильно введені дані або помилка в програмі, яка викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники (такі зазвичай помилки адміністрування). За деякими даними, до 65% втрат – наслідок ненавмисних помилок. Пожежі та повені не приносять стільки бід, скільки безграмотність і недбалість у роботі.

Очевидно, найрадикальніший спосіб боротьби з ненавмисними помилками – максимальна автоматизація і строгий контроль. Інші загрози доступності можна класифікувати за компонентами інформаційної системи, на які націлені загрози:

– відмова користувачів;

– внутрішня відмова мережі;

– відмова підтримуючої інфраструктури.

Зазвичай стосовно користувачів розглядаються наступні загрози:

– небажання працювати з інформаційною системою;

– неможливість працювати з системою через відсутність відповідної підготовки (нестача загальної комп'ютерної грамотності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією тощо);

– неможливість працювати з системою в силу відсутності технічної підтримки (неповнота документації, недолік довідкової інформації тощо).

Основними джерелами внутрішніх відмов є:

– відступ (випадкове або навмисне) від встановлених правил експлуатації;

– вихід системи з штатного режиму експлуатації в силу випадкових або навмисних дій користувачів або обслуговуючого персоналу (перевищення розрахункового числа запитів, надмірний обсяг оброблюваної інформації тощо);

– помилки при (пере) конфігурації системи;

– відмови програмного і апаратного забезпечення;

– руйнування даних;

– руйнування або пошкодження апаратури.

По відношенню до підтримуючої інфраструктурі рекомендується розглядати наступні загрози:

– порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо– та / або теплопостачання, кондиціонування;

– руйнування або пошкодження приміщень;

– неможливість або небажання обслуговуючого персоналу та / або користувачів виконувати свої обов'язки (цивільні безлади, аварії на транспорті, терористичний акт або його загроза, страйк і т.п.).

Досить небезпечні так звані "скривджені" співробітники – нинішні і колишні. Як правило, вони прагнуть завдати шкоди організації – "кривднику", наприклад: зіпсувати обладнання; вбудувати логічну бомбу, яка з часом зруйнує програми та / або дані; видалити дані.

Скривджені співробітники, навіть колишні, знайомі з порядками в організації і здатні завдати чималої шкоди. Необхідно стежити за тим, щоб при звільненні співробітника його права доступу (логічного і фізичного) до інформаційних ресурсів анулювалися.

3.3 Програмні атаки

Як засіб виведення мережі зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (зазвичай – смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті).

По розташуванню джерела загрози таке споживання підрозділяється на локальне та віддалене. При прорахунках в конфігурації системи локальна програма здатна практично монополізувати процесор і / або фізичну пам'ять, звівши швидкість виконання інших програм до нуля. Найпростіший приклад віддаленого споживання ресурсів – атака, що отримала найменування "SYN–повінь"[62].

Вона являє собою спробу переповнити таблицю "напіввідкритих" TCP–з'єднань сервера (встановлення з'єднань починається, але не закінчується). Така атака щонайменше ускладнює встановлення нових сполук з боку легальних користувачів, тобто сервер виглядає як недоступний. По відношенню до атаки "Papa Smurf" уразливі мережі, що сприймають ping–пакети з широкомовними адресами. Відповіді на такі пакети "з'їдають" смугу пропускання. Віддалене споживання ресурсів останнім часом проявляється в особливо небезпечній формі – як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю спрямовуються цілком легальні запити на з'єднання та / або обслуговування. Часом початку "моди" на подібні атаки можна вважати лютий 2000, коли жертвами виявилися кілька найбільших систем електронної комерції (точніше – власники та користувачі систем). Якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною здатністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність вкрай важко.

Для виведення систем зі штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних і апаратних помилок. Наприклад, відома помилка в процесорі Pentium I давала можливість локальному користувачеві шляхом виконання певної команди "підвісити" комп'ютер, так що

допомагає тільки апаратний RESET. Програма "Teardrop" віддалено "підвішує" комп'ютери, експлуатуючи помилку в збірці фрагментованих IP–пакетів [62].

3.4 Класифікація заходів забезпечення безпеки комп’ютерних систем

За способами здійснення всіх заходів забезпечення безпеки комп'ютерних мереж поділяються на: правові (законодавчі), морально–етичні, організаційні (адміністративні), фізичні, технічні (програмні).

До правових заходів захисту відносяться діючі в країні закони, укази та нормативні акти, що регламентують правила поводження з інформацією, що закріплюють права та обов'язки учасників інформаційних відносин у процесі її обробки та використання, а також встановлюють відповідальність за порушення цих правил, перешкоджаючи тим самим неправомірному використанню інформації і є стримуючим фактором для потенційних порушників.

До морально–етичних заходів протидії належать норми поведінки, які традиційно склалися або складаються в міру поширення комп'ютерних мереж у країні або суспільстві. Ці норми здебільшого не є обов'язковими, як законодавчо затверджені нормативні акти, проте, їх недотримання веде звичайно до падіння авторитету, престижу людини, групи осіб або організації.

Морально–етичні норми бувають як неписані (наприклад, загальновизнані норми чесності, патріотизму і т.п.), так і писані, тобто оформлені в деякий звід (статут) правил чи приписів.

Організаційні (адміністративні) заходи захисту – це заходи організаційного характеру, що регламентують процеси функціонування системи обробки даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою утруднити чи виключити можливість реалізації загроз безпеці. Вони включають [63]:

– заходи, здійснювані при проектуванні, будівництві та обладнанні мереж та інших об'єктів систем обробки даних;

– заходи щодо розробки правил доступу користувачів до ресурсів мереж (розробка політики безпеки); заходи, здійснювані при підборі й підготовці персоналу;

– організацію охорони і надійного пропускного режиму;

– організацію обліку, зберігання, використання та знищення документів і носіїв з інформацією; розподіл реквізитів розмежування доступу (паролів, ключів шифрування тощо);

– організацію явного і прихованого контролю за роботою користувачів;

– заходи, здійснювані при проектуванні, розробці, ремонті і модифікаціях обладнання та програмного забезпечення і т.п.

Фізичні заходи захисту засновані на застосуванні різного роду механічних, електро– або електронно–механічних пристроїв і споруд, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів мереж і захищається, а також технічних засобів візуального спостереження, зв'язку та охоронної сигналізації.

Технічні (апаратні) заходи захисту засновані на використанні різних електронних пристроїв, що входять до складу КС і виконують (самостійно або в комплексі з іншими засобами) функції захисту. Програмні методи захисту призначаються для безпосереднього захисту інформації за трьома напрямками: а) апаратури; б) програмного забезпечення; в) даних і керуючих команд.

Для захисту інформації при її передачі зазвичай використовують різні методи шифрування даних перед їх введенням в канал зв'язку або на фізичний носій з наступною розшифровкою. Як показує практика, методи шифрування дозволяють досить надійно приховати зміст повідомлення. Всі програми захисту, що здійснюють управління доступом до машинної інформації, функціонують за принципом відповіді на питання: хто може виконувати, які операції і над якими даними.

Доступ може бути визначений як:

– загальний (безумовно що надається кожному користувачеві);

– відмова (безумовний відмову, наприклад дозвіл на видалення порції інформації);

– залежний від події (керований подією);

– залежний від змісту даних;

– залежний від стану (динамічного стану комп'ютерної системи);

– частотно–залежний (наприклад, доступ дозволений користувачеві тільки один чи певну кількість разів);

– по імені або іншим ознакою користувача;

– залежний від повноважень;

– за дозволом (наприклад, по паролю);

– за процедурою.

Також до ефективних заходів протидії спробам несанкціонованого доступу відносяться засоби реєстрації. Для цих цілей найбільш перспективними є нові операційні системи спеціального призначення, що широко застосовуються в зарубіжних країнах і отримали назву моніторингу (автоматичного спостереження за можливу комп'ютерної загрозою).

Моніторинг здійснюється самою операційною системою (ОС), причому в її обов'язки входить контроль за процесами введення–виведення, обробки та знищення машинної інформації. ОС фіксує час несанкціонованого доступу та програмних засобів, до яких був здійснений доступ. Крім цього, вона виробляє негайне оповіщення служби комп'ютерної безпеки про посягання на безпеку комп'ютерної системи з одночасною видачею на друк необхідних даних (лістингу).

Останнім часом в США і низці європейських країн для захисту комп'ютерних систем діють також спеціальні підпрограми, що викликають самознищення основної програми при спробі несанкціонованого перегляду вмісту файлу з секретною інформацією за аналогією дії «логічної бомби».

Завдання забезпечення безпеки:

– захист інформації в каналах зв'язку і базах даних криптографічними методами;

– підтвердження автентичності об'єктів даних і користувачів (аутентифікація сторін, що встановлюють зв'язок);

– виявлення порушень цілісності об'єктів даних;

– забезпечення захисту технічних засобів і приміщень, в яких ведеться обробка конфіденційної інформації, від витоку по побічних каналах і від можливо впроваджених у них електронних пристроїв знімання інформації;

– забезпечення захисту програмних продуктів і засобів обчислювальної техніки від впровадження в них програмних вірусів і закладок;

– захист від несанкціонованих дій по каналу зв'язку від осіб, не допущених до засобам шифрування, але мають мети компрометації секретної інформації та дезорганізації роботи абонентських пунктів;

– організаційно–технічні заходи, спрямовані на забезпечення схоронності конфіденційних даних [63].

3.5 Висновки до розділу

В даному розділі було розглянуто класифікації загроз інформації системи та програмних атак. Було наведено приклади заходів забезпечення безпеки комп’ютерних систем. Дійшли до висновку що загрозою безпеки інформації розуміють подію або дію, яка може викликати зміну функціонування системи, пов'язане з порушенням захищеності оброблюваної в ній інформації.

Для захисту інформації при її передачі зазвичай використовують різні методи шифрування даних перед їх введенням в канал зв'язку або на фізичний носій з наступною розшифровкою. Як показує практика, методи шифрування дозволяють досить надійно приховати зміст повідомлення. Всі програми захисту, що здійснюють управління доступом до машинної інформації, функціонують за принципом відповіді на питання: хто може виконувати, які операції і над якими даними.

4 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Головною метою розділу є дослідження та впровадження функціональних складових інтелектуального керування та підсистема захисту «розумного будинку».

Щоб виконати оцінку економічної ефективності необхідно розрахувати трудомісткість реалізації дослідження, витрати на оплату праці найманим працівникам, витрати апаратного і програмного забезпечення, амортизаційні відрахування, витрати енергоресурсів та інші витрати які є основними пунктами виконання обчислень, а також показники економічної ефективності даного дослідження.

4.1 Розрахунок норм часу на виконання науково-дослідної роботи

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального використання часу.

Дослідження щодо функціональних складових інтелектуального керування та підсистеми захисту «розумного будинку» можна поділити на декілька етапів, що значно полегшить виконання даного дослідження.

До основних етапів можна віднести:

– опис задачі;

– збір інформації по системі “розумного будинку”;

– проведення порівняльного аналізу рішень щодо системи “розумного будинку”;

– структуризація даного дослідження;

– оформлення аналітичної роботи.

Норми часу на виконання науково-дослідницької роботи розраховувються на основі середнього часу виконання стадії в годинах, що наведені в таблиці 4.1 разом із інформацією про виконавців і сумарною кількості затраченого часу.

Таблиця 4.1 – Операції технологічного процесу та їх час виконання

Таблиця 4.1 – Операції технологічного процесу та їх час виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	Підготовча стадія	Проектний менеджер	18
		Інженер-програміст	
2	Технічна пропозиція	Проектний менеджер	30
		Інженер-програміст	
3	Створення технічного завдання	Проектний менеджер	30
4	Проектування системи	Інженер-програміст	20
5	Практична реалізація	Інженер-програміст	70
6	Тестування системи	Тестувальник	18
7	Верифікація системи	Тестувальник	30
		Інженер-програміст	
		Проектний менеджер	
8	Створення документації	Інженер-програміст	18
9	Заключна стадія	Проектний менеджер	10
Разом			244

В підсумку на реалізацію дослідження функціональних складових інтелектуального керування та підсистеми захисту «розумного будинку”» необхідно 244 людино-година, залучення трьох спеціалістів та виконання дев’яти різноманітних стадій реалізації проекту.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Визначення витрат на оплату праці та відрахувань на соціальні заходи прямо залежить від кількості витраченого працівниками часу на роботу, ставки в годину чи місяць, кількість відрахувань на соціальні заходи встановлених в законному порядку на час розрахунку.

В результаті розрахунку потрібно визначити основну та додаткову заробітну плату, витрати на соціальні заходи та на основі цих даних визначити сумарні витрати на оплату праці.

Основна заробітна плата нараховується за виконану роботу за тарифними ставками.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

У штаті найманих працівників для розробки системи захисту залучено проектного менеджера, інженера-програміста і тестувальника.

Тарифні ставки учасників процесу розробки інформаційної системи управління доступом з використанням інформаційних технологій розпізнавання образів:

– Проектний менеджер – 100 грн./год.

– Інженер-програміст – 85 грн./год.

– Тестувальник – 75 грн./год.

Основна заробітна плата розраховується за формулою 4.1:

$$З_{осн.} = Т_с \cdot К_г, \quad (4.1)$$

де $Т_с$ – тарифна ставка, грн.; $К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в виконує три спеціаліста, то основна заробітна плата буде розраховуватись за даною формулою 4.1;

$$З_{осн.} = 100 \cdot 74 + 85 \cdot 142 + 75 \cdot 28 = 21570 \text{ грн.}$$

Додаткова заробітна плата становить 10–15% від суми основної заробітної плати й визначається за формулою 4.2.

Коефіцієнт додаткових виплат працівникам становить 0,1.

$$З_{дод.} = З_{осн.} \cdot К_{допл.} \quad (4.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам

$$З_{дод} = 21570 \cdot 0,1 = 2157 \text{ грн}$$

Звідси загальні витрати на оплату праці (фонд заробітної плати) визначаються за формулою 4.3:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (4.3)$$

$$В_{о.п.} = 21570 + 2157 = 23627 \text{ грн.}$$

З цієї суми утримуються обов'язкові відрахування на заробітну плату:

– єдиний соціальний внесок (ЄСВ), що становить 22%;

– військовий збір (ВЗ), що становить 1,5%;

Сума відрахувань становить 23,5% від фонду оплати праці та визначається за формулою 4.4:

$$B_{с.з.} = Ф_{оп} \cdot 0,235 \quad (4.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$B_{с.з.} = 23627 \cdot 0,235 = 5575,85$$

Усі витрати обчислюються детально наведені в таблиці 4.2

Таблиця 4.2 – Розрахунки витрат на оплату праці

з/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на плату праці, грн. (6=3+4+5)
		Тарифна ставка, грн.	Кількість відпрацьованих год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1.	Проектний менеджер	100	74	7400	740	-	-
2.	Інженер-програміст	85	142	12070	1207	-	-
3.	Тестувальник	75	28	2100	210	-	-
Разом		260	244	21570	2157	5575,85	29302,85

З таблиці розрахунку витрат на оплату праці видно, що всього витрати на плату праці становить 29302,85.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати є невід'ємною частиною розробки системи захисту «розумного будинку» та визначаються як добуток кількості витрачених матеріалів та їх ціни за формулою 4.5:

$$M_{вi} = q_i \cdot p_i \,, \tag{4.5}$$

де: q_i – кількість витраченого матеріалу і–го виду; p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.7:

$$З_{м.в.} = \sum M_{вi} \,. \tag{4.6}$$

Результати проведених розрахунків наведено у таблиці 4.3.

Таблиця 4.3 – Результати розрахунків матеріальних витрат.

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Фактично витрачено матеріалів	Ціна одиниці, грн.	Загальна сума витрат, грн.
1	Лампочка	шт.	1	14	28
2	Геркони	листів	2	450	900
3	Датчики руху	шт.	3	153	459
Всього					1387

Згідно проведених розрахунків, матеріальні витрати становлять 1387 грн.

4.4 Розрахунок витрат на електроенергію

Однією із статей витрат є витрати на електроенергію під час проходження усіх етапів реалізації кінцевого продукту.

Затрати на електроенергію одиниці обладнання визначаються за формулою 4.7:

$$З_в = W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт; T – кількість годин на реалізацію розробки; S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютерів для реалізації кінцевого продукту – 400 Вт, кількість годин роботи обладнання згідно таблиці 4.1 – 231 годин.

Визначимо витрати на електроенергію згідно формули 4.10:

$$З_в = 0{,}4 \cdot 231 \cdot 2{,}42 = 223{,}6 \text{ грн.}$$

Згідно формули затрати на електроенергію становлять 223,6грн.

4.5 Розрахунок суми амортизаційних відрахувань

Для будь якої діяльності характерною є властивість зношування на зниження якості властивостей інструментарію та фондів за допомогою яких ведеться діяльність.

Для вирішення проблеми із відновленням даних фондів використовується амортизація, що являє собою процес трансформації вартості основних фондів на вартість продукції, яка щойно була створена, задля повного відновлення основних фондів.

Для визначення амортизаційних відрахувань використовується формула 4.8:

$$А = \frac{Б_В \cdot Н_А}{100\%} \qquad (4.8)$$

де, $C_Б$ – балансова вартість обладнання, грн;

N_A – норма амортизаційних відрахувань в рік, %;

– річний робочий фонд часу, год;

– фактичний час роботи обладнання по написанню програми, год.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60% (квартальна – 15%).

Річний робочий фонд становитиме 2352 годин, так як робочий день становить 8 годин, а кількість робочих днів в місяці становить 24,5 годин.

Для дослідження та впровадження функціональних складових інтелектуального керування та підсистема захисту «розумного будинку» засобом розробки є комп'ютер. Його сума становить 17500 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 17500 \cdot 5\% / 100\% = 875 \text{ грн.}$$

Згідно проведених обчислень амортизаційні відрахування становлять 875 грн.

4.6 Обчислення накладних витрат

Накладні витрати пов’язані з обслуговуванням , утриманням апарату управління спілкою та створення необхідних умов праці проведення дослідження та впровадження функціональних складових інтелектуального керування та підсистема захисту «розумного будинку».

В залежності від організаційно-правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20–60% від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2…0{,}6 , \qquad (4.9)$$

де $H_в$ – накладні витрати.

Отже, накладні витрати становлять згідно формули 4.9:

$$H_в = 23627 \cdot 0{,}2 = 4725{,}4 \text{ грн.}$$

Накладні витрати згідно розрахунку формули, становить 4725,4 грн.

4.7 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків наведено у таблиці 4.4.

Таблиця 4.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	23627	70,8
Відрахування на соціальні заходи	5575,85	14,6
Матеріальні витрати	1387	0,3
Витрати на електроенергію	223,6	0,4
Амортизаційні відрахування	875	1,5
Накладні витрати	4725,4	12,4
Собівартість	36413,85	100

Собівартість ($С_в$) програмного продукту розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.з.} + З_{м.в.} + З_в + А + Н_в \ . \quad (4.10)$$

Отже, собівартість програмного продукту дорівнює:

Св = 23627 + 5575,85 + 1387 + 223,6 + 875 + 4725,4 = 36413,85 грн.

Загальний кошторис витрат та визначення собівартості дослідження та впровадження функціональних складових інтелектуального керування та підсистема захисту «розумного будинку» становить 36413,85 грн.

4.8 Розрахунок вартості на проведення дослідження

Витрати наукової роботи щодо систем захисту «розумного будинку» визначається за формулою:

$$Ц = \frac{С_В \cdot (1 + Р_{РЕН.} + К \cdot В_{Н.І.})}{К} \cdot (1 + ПВД) \ , \quad (4.11)$$

де $Р_{рен.}$ – рівень рентабельності, 30%;

К – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем);

$В_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

ПДВ – ставка податку на додану вартість, (20%).

Оскільки розробка є теоретичною, і використовуватиметься тільки для «Розумного міста», то для розрахунку ціни не потрібно вказувати коефіцієнти К та Ві.н , оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = С_В \cdot (1 + Р_{РЕН}) \cdot (1 + ПВД) \quad (4.12)$$

Звідси ціна на роботу складе:

$$Ц = 36413{,}85 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 56805{,}606 \text{ грн.}$$

Загальний розрахунок ціни програмного продукту становить 56805,606 грн.

4.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

В даному пункті було проведено визначення економічної ефективності і терміну окупності капітальних вкладень для проведення дослідження щодо систем захисту «розумного будинку». Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$Е_р = \frac{П}{С_В}, \quad (4.13)$$

де *П* – прибуток; $С_В$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - С_в \ . \qquad (4.14)$$

Розраховуємо плановий прибуток:

$$П_{пл} = 56805{,}606 - 36413{,}85 = 20391{,}756 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П}{С_В} \ . \qquad (4.15)$$

Тоді,

$$E_р = 36413{,}85 \ / \ 56805{,}606 = 0{,}64.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_р$):

$$Т_р = \frac{1}{E_р} \ , \qquad (4.17)$$

Термін окупності дорівнює:

$$T_р = 1 \ / \ 0{,}64 = 1{,}56 \text{ р.}$$

Згідно формул плановий прибуток від розробки становить 56805,606 грн., економічна ефективність дорівнює 0,64, а термін окупності становить 1,56 роки що вважається доцільним та економічно вигідним.

4.10 Висновок до розділу

В розділі обґрунтування економічної ефективності дипломної роботи освітнього рівня «магістр» було розраховано основні техніко-економічні показники по дослідженню системи захисту «розумного будинку» (див. таблиця 4.5).

Орієнтоване значення економічної ефективності становить 0,64 що є достатньо високим значенням.

Період окупності повинен варіюватися від 1 до 3 років, тоді реалізація дослідження буде вважатися доцільною та економічно вигідною. Термін окупності дослідження 1,56 років.

Таблиця 4.5 – Техніко-економічні показники науково-дослідної роботи

№ п/п	Показник	Значення
1.	Собівартість, грн.	36413,85
2.	Плановий прибуток, грн.	20391,756
3.	Ціна, грн.	56805,606
4.	Економічна ефективність	0,64
5.	Термін окупності, рік	1,56

Отже, дослідження та впровадження функціональних складових інтелектуального керування та підсистема захисту «розумного будинку» може бути реалізовано та розвинено, оскільки воно є економічно вигідним для всіх технічних та економічних показників.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Комісія з питань охорони праці: склад, основні завдання та права

Комісія з питань охорони праці підприємства може створюватися у відповідності з Законом України "Про охорону праці" (ст. 26) на підприємствах, в організаціях, господарствах з кількістю працюючих 50 і більше чоловік, незалежно від форм власності та видів господарської діяльності. Комісія є постійно діючим консультативно-дорадчим органом [64].

На підприємстві з метою забезпечення пропорційної участі працівників у вирішенні будь-яких питань безпеки, гігієни праці та виробничого середовища за рішенням трудового колективу може створюватися комісія з питань охорони праці. Комісія складається з представників роботодавця та професійної спілки, а також уповноваженої найманими працівниками особи, спеціалістів з безпеки, гігієни праці та інших служб підприємства відповідно до типового положення, що затверджується центральним органом виконавчої влади, що забезпечує формування державної політики у сфері охорони праці [64]. (Стаття 16, частина друга із змінами, внесеними згідно із Законом №5459-VI від 16.10.2012.).

Працівники, зайняті на роботах з підвищеною небезпекою або там, де є потреба у професійному доборі, повинні щороку проходити навчання і перевірку знань з питань охорони праці (ст. 18 Закону № 2694). Перевірку знань працівників з питань охорони праці здійснює відповідна комісія підприємства, склад якої затверджується керівником підприємства.

Комісія у своїй діяльності керується законодавством про працю, міжгалузевими і галузевими нормативними актами з охорони праці, а також Положенням про комісію з питань охорони праці підприємства.

Основними завданнями комісії є захист законних прав та інтересів працівників у сфері охорони праці, узгодження, шляхом двосторонніх консультацій, позицій сторін у вирішенні практичних питань у сфері охорони праці з метою

забезпечення поєднання інтересів держави, роботодавця та трудового колективу, кожного працівника, запобігання конфліктам [65].

Члени комісії виконують свої обов'язки, як правило, на громадських засадах. При залученні до окремих перевірок, проведенні навчання вони можуть звільнятися від основної роботи на передбачений колективним договором термін із збереженням за ними середнього заробітку. Рішення комісії оформляються протоколами і мають рекомендаційний характер, впроваджуються в життя наказами роботодавця. При незгоді роботодавця з рекомендаціями Комісії він дає аргументовану відповідь. Комісія не менше одного разу на рік звітує про свою роботу на загальних зборах (конференції) трудового колективу.

Основними завданнями комісії є:

– підготовка, на основі аналізу стану безпеки та умов праці на виробництві, рекомендацій власнику та працівникам щодо профілактики виробничого травматизму та професійних захворювань, практичної реалізації принципів державної політики н області охорони праці на підприємстві; узгодження, шляхом двосторонніх консультацій, позицій сторін у вирішенні практичних питань у сфері охорони праці з метою забезпечення поєднання інтересів держави, власника та трудового колективу, кожного працівника, запобігання конфліктам;

– вироблення пропозицій щодо включення до колективного договору окремих питань з охорони праці та використання коштів фонду охорони праці підприємства.

Комісія має право:

– звертатися до власника або уповноваженого ним органу, органу самоврядування трудового колективу, профспілкового комітету зпропозиціями щодо регулювання відносин у сфері охорони праці;

– створювати робочі групи з числа членів комісії для вироблення узгоджених рішень з конкретних питань охорони праці з залученням до їх складу на договірній основі за погодженням сторін відповідних фахівців, експертів, інспекторів державного нагляду за охороною праці;

– одержувати від окремих працівників, служб підприємства, профспілкового комітету (комітетів) інформацію, необхідну для виконання функцій і завдань, передбачених типовим положенням;

– встановлювати ступінь вини потерпілого та винуватця (в т.ч. і власника) нещасного випадку в порядку, що визначається трудовим колективом за поданням власника та профспілкового комітету, при вирішенні питання про розмір одноразової допомоги, коли нещасний випадок стався внаслідок невиконання потерпілого вимог нормативних актів про охорону праці і факт наявності його вини встановлено комісією по розслідуванню нещасних випадків;

– здійснювати контроль за дотриманням вимог законодавства з питань охорони праці безпосередньо на робочих місцях, забезпечення працюючих засобами колективного та індивідуального захисту, змиваючими та знешкоджуючими засобами, лікувально–профілактичним харчуванням, молоком або рівноцінними харчовими продуктами, газованою підсоленою водою та станом використання санітарно-побутових приміщень;

– знайомитись з будь-якими матеріалами з питань охорони праці, аналізувати стан умов і безпеки праці на підприємстві, виконання відповідних програм і колективних договорів;

– вільного доступу на всі дільниці виробництва і обговорення з працюючими питань охорони праці.

Комісія може делегувати своїх представників для участі:

– у розв'язуванні разом з представниками державного нагляду за охороною праці конфліктів, пов'язаних з відмовою працівника виконувати доручену роботу з мотивів небезпечної для його здоров'я чи життя виробничої ситуації на підприємстві, де відсутня профспілкова організація;

– в обговоренні питань охорони праці власником або уповноваженим ним органом, профспілковим комітетом чи органом самоврядування трудового колективу (за погодженням з цими органами).

Члени комісії виконують свої обов'язки, як правило, на громадських засадах. При залученні до окремих перевірок, проведенні навчання вони можуть звільнятися

від основної роботи на передбачений колективним договором термін із збереженням за ними середнього заробітку [65].

Комісія здійснює свою діяльність на основі планів, що розробляють на квартал, півріччя чи рік і затверджуються нею. Рішення комісії оформляються протоколами і мають рекомендаційний характер, впроваджуються в життя наказами власника. При незгоді власника з рекомендаціями Комісії він дає аргументовану відповідь. Комісія не менше одного разу на рік звітує про свою роботу на загальних зборах (конференції) трудового колективу.

5.2 Режим праці та відпочинку працівників, які використовують у своїй роботі ПК

При організації праці, що пов'язана з використанням персональних комп'ютерів, для збереження здоров'я працюючих, запобігання професійним захворювання і підтримки працездатності слід передбачити регламентовані перерви для відпочинку. Режими праці і відпочинку мають передбачати додаткові нетривалі перерви в періоди, що передують появі об'єктивних і суб'єктивних ознак стомлення і зниження працездатності. За основну роботу з персональним комп'ютером слід вважати таку, що займає не менше 50% часу впродовж робочої зміни.

Відповідно до п. 5.3 ДСанПіН 3.3.2.007-98 протягом дня мають передбачатися:

– перерви для відпочинку і вживання їжі (обідні перерви);

– перерви для відпочинку і особистих потреб (згідно з трудовими нормами);

– додаткові перерви, що вводяться для окремих професій з урахуванням особливостей трудової діяльності.

Тривалість обідньої перерви визначається чинним законодавством про працю і правилами внутрішнього трудового розпорядку [66].

Пунктом 5.8 ДСанПіН 3.3.2.007-98 встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні залежно від характеру праці:

– для розробників програм слід призначати регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи за персональним комп'ютером;

– для операторів персональних комп'ютерів слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години;

– для операторів комп'ютерного набору слід призначати регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи за персональним комп'ютером.

У всіх випадках, коли виробничі обставини не дозволяють застосувати регламентовані перерви, тривалість безперервної роботи з персональним комп'ютером не повинна перевищувати 4 години. При 12-годинній робочій зміні регламентовані перерви повинні встановлюватися в перші 8 годин роботи аналогічно перервам при 8-годинній робочій зміні, а протягом останніх 4-х годин роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хвилин (п. 5.9 та п. 5.10 ДСанПіН 3.3.2.007-98) [66].

З метою зменшення негативного впливу монотонності є доцільним застосовувати чергування операцій обробки тексту і числових даних (зміна змісту роботи), чергування вводу даних та редагування текстів. Для зниження нервово-емоційного напруження, стомлення зорового аналізатора, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втомі доцільні деякі перерви використовувати для виконання комплексу вправ, приклади яких також наведено в ДСанПіН 3.3.2.007-98 [67].

В окремих випадках – при хронічних скаргах працюючих на зорове стомлення, незважаючи на дотримання санітарно – гігієнічних вимог до режимів праці і відпочинку, а також застосування засобів локального захисту очей – допускається індивідуальний підхід до обмеження часу робіт з персональним комп'ютером, зміни характеру праці, чергування з іншими видами діяльності, не пов'язаними з персональним комп'ютером [67].

5.3 Комп’ютерне забезпечення процесу оцінки радіаційної та хімічної обстановки

Екологічне співтовариство розробило сімейство інструментів комплексної екологічної оцінки. Програмне забезпечення і послуги (ESS), комерційна група IIASA, включаючи AirWare (для повітряних проблеми якості), WaterWare (для якості води), CityWare (якість повітря і води в контексті великих міст) і EIAxpert (для надання допомоги із загальним впливом на навколишнє середовище). Функціональність в цілому схожа на RAISON, хоча з великим акцентом на моделювання і меншим акцентом на керування даними. Знову ж таки, інструменти ESS розроблені як модульні
набори інструментів (доступні спеціальні системи для вирішення конкретних завдань). Компоненти включають стандартні імітаційні моделі, включаючи моделі ISC і PBM Агентства з охорони навколишнього середовища США, управління даними, в тому числі ГІС, аналіз даних (наприклад, аналіз часових рядів даних спостережень), візуалізація, а також оптимізація [68].

Іноді немає готових моделей, придатних для конкретного застосування, але тягар розробки нової програми на Фортране або C / C ++ є надмірним. Розробка моделі оточення може відносно легко реалізувати власні моделі комп'ютерів і не турбуватися про включення процедур для вирішення рівнянь, візуалізації і т. д. Як правило, за допомогою цих інструментів користувач просто повинен вказати свою модель, використовуючи або математичні рівняння, або спеціальні графічні символи або значки, які безпосередньо представляють поведінку системи. На даний момент є розроблені моделі комп’ютерного забезпечення процесу для оцінки радіаційної та хімічної обстановки.

GEMS – це система на основі моделей, яка підтримує оцінки схильності і ризику, надаючи доступ до одиночних і мультимедійних моделям експозиції, фізико-хімічні властивості методи оцінки, статистичний аналіз, графічні та картографічні програми з відповідними даними на навколишнє середовище, джерела, рецептори і популяції. У розробці з 1981 року, GEMS надає аналітикам

інтерактивний, легко досліджуваний інтерфейс для різних моделей, програм і даних, які необхідні для оцінки хімічного впливу і ризику [68].

HSPF – це комплексний пакет для моделювання кількості і якості стоків з багатоцільових водозборів і процесів радіації, що відбуваються в потоках або повністю змішаних озерах. Це дозволяє інтегроване моделювання землі і грунту, процесів забруднення при гідравлічній і осадово-хімічній взаємодії. Результатом моделювання є тимчасові дані витрати стоку, концентрація поживних речовин і пестицидів, а також дані кількості і якості води в будь-якій точці водозбору. Алгоритми якості води включають динаміку BOD / DO, вуглець, азот і фосфор. Процеси трансформації, які включені в модель це: гідроліз, фотоліз, окислення, випаровування, сорбція і биодеградація. Вторинні або «дочірні» хімічні речовини також моделюються;

Вимоги до даних для моделі можуть бути досить обширними в залежності від конкретного застосування.

Модель MMSOILS – це методологія оцінки впливу на людину і ризику для здоров'я, пов'язаних з викидами забруднень з небезпечних відходів. Мультимедійна модель, що стосується перенесення хімічної речовини в ґрунтові води, поверхневі води, атмосферу і накопичення в їжі. Шляхи впливу на людину, які розглянуті в методології включають: потрапляння в грунт, вдихання летких речовин в повітря і тверді частинки, шкірний контакт, прийом питної води і т.д. Ризик, пов'язаний із загальною дозою опромінення, розраховується на основі хімічної токсичності [69].

5.4 Ергономічні вимоги до робочого місця користувача ПК

Робоче місце — це зона простору, що оснащена необхідним устаткуванням, де відбувається трудова діяльність одного працівника чи групи працівників [69].

Раціональне планування робочого місця має забезпечувати: найкраще розміщення знарядь і предметів праці, не допускати загального дискомфорту, зменшувати втомлюваність працівника, підвищувати його продуктивність праці. Площа робочого місця має бути такою, щоб працівник не робив зайвих рухів і не

відчував незручності під час виконання роботи. Важливо мати також можливість змінити робочу позу, тобто положення корпуса, рук, ніг. Проте доцільно виключати або мінімізувати всі фізіологічно неприродні і незручні положення тіла. Проведені дослідження показують, що при раціональній організації робочих місць продуктивність праці зростає на 15–25%.

Організація робочого місця користувача ПК має відповідати ергономічним вимогам ГОСТ 12.2.032. ССБТ. “Рабочее место при выполнении работ сидя. Общие эргономические требования”, ДНАОП 0.00-1.31-99, ДСан ПіН 3.3.2.007-98, характеру та особливостям трудової діяльності.

Площа одного робочого місця користувача ПК повинна складати не менше 6 м2, а об’єм – не менше 20 м3. Конструкція робочого місця користувача ПК повинна відповідати сучасним вимогам ергономіки, характеру виконуваної роботи і забезпечити оптимальне розміщення на робочій поверхні документів та обладнання ПК (монітора, системного блоку, клавіатури, мишки та інших периферійних пристроїв. Монітор на робочому місці встановлюється так, щоб верхній край екрана знаходився на рівні очей.

Розташування монітора ПК має забезпечувати:

– безпечність роботи в цілому;

– зручність та ефективність зорової роботи з екраном в вертикальній площині під кутом 300 від лінії зору, площина екрана при цьому має бути перпендикулярною нормальній лінії зору користувача.

Клавіатура розміщується на поверхні столу або висувній полиці на відстані 100-300мм від краю, ближчого до користувача. Кут нахилу клавіатури має бути в межах 5-150. Поверхня клавіатури повинна бути матовою з коефіцієнтом відбиття 0,4. клавіші клавіатури мають бути зручними в роботі і м’якими при натисканні (хід всіх клавіш має бути одинаковим з мінімальним опором натискання 0,25Н та максимальним – не більше 1,5Н) [70].

При розміщенні робочих місць з ПК слід дотримуватися вимог, зазначених в ДНАОП 0.00-1.31-99:

– робочі місця розміщуються на відстані не менше 1м від стін з світловими прорізями;

– відстань між бічними поверхнями моніторів ПК має бути не менше 1,2м;

– відстань між тильною поверхнею монітора одного ПК та екраном монітора іншого ПК має бути не меншою 2,5м.

Вимоги двох останніх пунктів враховуються також при розміщенні робочих місць з ПК в суміжних приміщеннях з урахуванням конструктивних особливостей стін та перегородок.

Загальні принципи організації робочого місця:

– на робочому місці не повинно бути нічого зайвого. Усі необхідні для роботи предмети мають бути поряд із працівником, але не заважати йому;

– ті предмети, якими користуються частіше, розташовуються ближче, ніж ті предмети, якими користуються рідше;

– предмети, які беруть лівою рукою, повинні бути зліва, а ті предмети, які беруть правою рукою – справа;

– якщо використовують обидві руки, то місце розташування пристосувань вибирається з урахуванням зручності захоплювання його двома руками;

– робоче місце не повинно бути захаращене;

– організація робочого місця повинна забезпечувати необхідну оглядовість.

Статичні напруження працівника в процесі праці пов'язані з підтриманням у нерухомому стані предметів і знарядь праці, а також підтриманням робочої пози.

Робоча поза – це основне положення працівника у просторі: зручна робоча поза має забезпечувати стійкість положення корпуса, ніг, рук, голови працівника під час роботи, мінімальні затрати енергії та максимальну результативність праці. Неправильна сидяча поза може викликати застій крові в ногах, а якщо виконується великий обсяг роботи для пальців рук – запалення суглобів.

Організація робочого місця користувача комп'ютера повинна забезпечувати відповідність усіх елементів робочого місця та їх взаємного розташування ергономічним вимогам (рисунок 5.1).

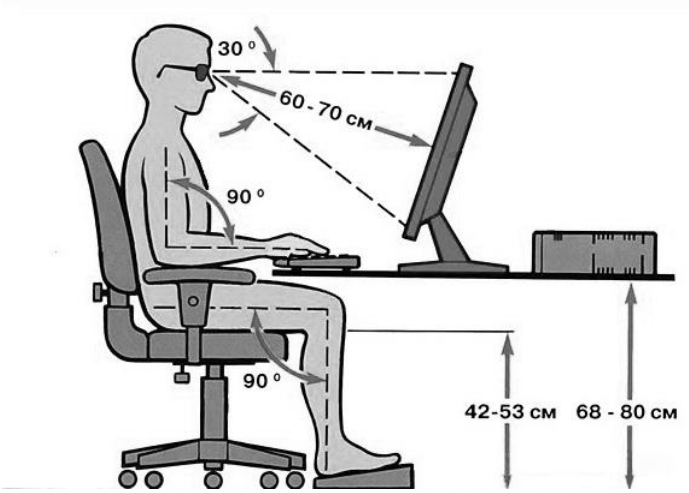

Рисунок 5.1 –Робоче місце і робоча поза користувача ПК

Найпоширенішими у процесі праці є пози сидячи і стоячи. Проектуючи робоче місце, потрібно враховувати, що при виконанні роботи з фізичним навантаженням бажана поза стоячи, а при малих зусиллях – сидячи.

Робоча поза стоячи втомлює людину більше, ніж сидяча. Вона вимагає на 10% більше енергії, спричиняє підвищення артеріального і венозного тиску крові, розширення вен на ногах, пошкодження ступень, викривлення хребта [72].

5.5 Висновки до розділу

В даному розділі було розглянуто актуальні питання з охорони праці та безпеки в надзвичайних ситуаціях.

Отже, основними завданнями комісії є захист законних прав та інтересів працівників у сфері охорони праці, узгодження, шляхом двосторонніх консультацій, позицій сторін у вирішенні практичних питань у сфері охорони праці з метою забезпечення поєднання інтересів держави, роботодавця та трудового колективу, кожного працівника, запобігання конфліктам.

Іноді немає готових моделей, придатних для конкретного застосування, але тягар розробки нової програми на Фортране або C / C ++ є надмірним. Розробка моделі оточення може відносно легко реалізувати власні моделі комп'ютерів і не турбуватися про включення процедур для вирішення рівнянь, візуалізації і т. д. Як

правило, за допомогою цих інструментів користувач просто повинен вказати свою модель, використовуючи або математичні рівняння, або спеціальні графічні символи або значки, які безпосередньо представляють поведінку системи.

Раціональне планування робочого місця має забезпечувати: найкраще розміщення знарядь і предметів праці, не допускати загального дискомфорту, зменшувати втомлюваність працівника, підвищувати його продуктивність праці. Площа робочого місця має бути такою, щоб працівник не робив зайвих рухів і не відчував незручності під час виконання роботи.

6 ЕКОЛОГІЯ

6.1 Статистична оцінка екологічного стану навколишнього природного середовища та закономірностей його розподілу

Властивістю статистичної сукупності є коливання, мінливість значень будь–якої ознаки, тобто варіація. Вона зумовлена дією безлічі взаємопов'язаних причин, серед яких є основні і другорядні. Основні причини формують центр розподілу, другорядні – варіацію ознак, сукупна їх дія – форми розподілу.

Більшість статистичних сукупностей у природі і суспільстві підпорядковується закону нормального розподілу. Крива нормального розподілу відіграє роль стандарту, з якою порівнюються всі емпіричні розподіли. Нормальний розподіл описує залежність між змінною ознакою і густиною розподілу безперервної випадкової величини [73].

При вивченні закономірностей розподілу застосовують середню арифметичну, варіації – середню квадратичну, інтенсивності розвитку – середню геометричну.

Слід зауважити, що різні види середніх, обчислені на основі однієї і тієї ж вихідної інформації, мають різну величину.

Це співвідношення називається правилом мажорантності.

В екологічній статистиці це правило не може бути застосоване, оскільки обчислення різних середніх для однієї і тієї ж сукупності недоцільне. Вибір виду середньої має Грунтуватись на всебічному теоретичному аналізі суті явищ та наявній інформації. Середня лише тоді може бути справжньою узагальнюючою характеристикою, коли при заміні нею всіх варіантів загальний обсяг варіюючої ознаки залишиться незмінним [73].

Отже, залежно від того, що являє собою загальний обсяг варіюючої ознаки, в кожному конкретному випадку обирають вид середньої.

Закономірність розподілу – це закономірність зміни частот відповідно до зміни ознаки.

Дослідження закономірності розподілу складається з трьох послідовних етапів:

– встановлення загального характеру розподілу,

– вирівнювання емпіричного розподілу за теоретичною кривою розподілу,

– встановлення відповідності теоретичного розподілу емпіричному.

Міжнародне співтовариство на даному етапі розглядає показники стану навколишнього середовища як комплексний інструментарій для виміру та репрезентації еколого-економічних тенденцій у країні. Виходячи з цих позицій, можна виділити чотири основні типи показників:

– показники сучасного екологічного стану, які визначають чинні екологічні параметри;

– показники впливу або тиску, які відображають антропогенний вплив на навколишнє середовище;

– показники, що регулюють вплив на навколишнє середовище, і за допомогою яких визначається, як різні агенти реагують на специфічний вплив;

– показники якісного стану або ступеня забруднення (в регіонах і населених пунктах).

Останній тип показників пов'язаний з впровадженням конкретних заходів при виробленні екологічної політики.

Чинна в Україні система статистичної звітності в галузі охорони навколишнього середовища не орієнтована на оцінку реакції екосистем на техногенний вплив і критичні параметри впливу для конкретних екосистем та груп населення, а відображає натуральні об'єми забруднювальних речовин і вартісні показники дотримання підприємством чи місцевим органом влади природоохоронного законодавства та планових параметрів проведення природоохоронних заходів [74].

З точки зору економічних показників система статистичної звітності в Україні в галузі охорони навколишнього середовища оперує, в основному, саме опосередкованими показниками стану навколишнього середовища, тоді як, виходячи з міжнародних вимог, необхідно впроваджувати інтегральні показники

прямої дії, що відображали б еколого–економічні процеси на національному рівні [75].

Охорона навколишнього природного середовища пов'язана з розробленням і здійсненням комплексу екологічно спрямованих заходів, що запобігають або знижують негативний вплив антропогенної діяльності на природу.

Природоохоронні заходи розглядаються у вузькому і широкому розумінні.

У вузькому розумінні природоохоронні заходи – це ті види господарської діяльності, які безпосередньо спрямовані на вирішення певних природоохоронних завдань: будівництво очисних споруд і пристроїв; перероблення, утилізацію відходів; рекультивацію земель; заходи щодо боротьби з ерозією грунтів та ін.

Такий розподіл обумовлений тим, що природоохоронні заходи вважаються не універсальною, а вузько цільовою сферою діяльності, спрямованою на досягнення вузьких цілей при обмеженості фінансових і матеріальних ресурсів.

У широкому розумінні до середовище захисних заходів можна віднести всі види господарської діяльності, що як прямо, так і побічно сприяють зниженню або ліквідації негативного впливу дій людини на довкілля. До них належать ті, які так чи інакше підвищують загальну ефективність функціонування економічних систем [76].

У кінцевому підсумку це обумовлює зменшення ресурсомісткості (матеріаломісткості, енергоємності чи водоємності) виробництва одиниці продукції (виконання певної роботи, надання послуг). Інакше кажучи, зменшується питома потреба в зазначених ресурсах. Безпосередніми наслідками цього є відносне зменшення екологічного тиску на стадіях виробництва: зникає (або зменшується) потреба в ресурсі - зникають (або зменшуються) і негативні наслідки його виробництва [77].

Основними показниками природоохоронної діяльності в Україні слід вважати, з одного боку, обсяги та напрямки фінансування екологічних заходів, з іншого - різні види екологічних платежів і зборів, які не тільки виступають як одне із джерел природоохоронних видатків, але і є дієвим інструментом мотивації природо спрямованої діяльності.

6.2 Роль матеріало– та ресурсозбереження у вирішенні екологічних проблем

Відтворення і ефективне використання природноресурсного потенціалу є одним з основним завдань, які стоять перед усіма господарюючими суб'єктами. Адже з використанням інноваційних ресурсозберігаючих технологій досягається збільшення виробництва продукції при незначному негативному впливові на довкілля, а, відповідно, і зростає конкурентоспроможність підприємств на ринку[78].

За видами ресурсів, що зберігаються, ресурсозбереження може бути класифіковане на матеріало-, водо-, енерго-, трудо-, фондозбереження, збереження фінансових, інформаційних та інших видів ресурсів. Даний напрямок класифікації має важливе значення, оскільки збереження окремого виду ресурсу характеризується певною специфікою, вивчення якої надає можливість сформувати комплекс відповідних ресурсозберігаючих заходів, що забезпечують найвищу віддачу вкладених коштів, та застосувати адекватні економічні пільги. Завдяки коп'ютерним технологіям стає можливим передбачувати оптимальне використання обмежених ресурсів та екологічних матеріалоресурсів, включаючи видобуток і переробку сировини, створення екологічно прийнятної продукції, мінімізацію, переробку і знищення відходів [79].

Уміле застосування еколого – економічних інструментів в поєднанні з коп'ютерними програмами дозволяє ефективно вирішувати проблеми ресурсозбереження в рамках механізмів саморегулювання ринкової економічної системи. Комплекс взаємопов'язаних дій як на державному, так і на місцевому рівнях забезпечує реалізацію стратегії ресурсозбереження, використовуючи прогресивні технології, методи управління ресурсозбереження діяльністю, підвищуючи її ефективність в національній економіці [80].

Ключового значення для розвитку вітчизняного ринку ресурсозбереження набуває в сучасних умовах розробка програмних технологій для допомоги

ресурсосервісним компаніям. Враховуючи, що основною проблемою реалізації ресурсозберігаючих заходів в Україні є дефіцит фінансових коштів, формування розгалуженої мережі підприємств, які надають широкий спектр послуг зі зниження плати за споживання ресурсів з інвестиційним забезпеченням, тим самим знижуючи антропогенне навантаження на довкілля, що є на часі досить актуальним [80].

6.3 Висновки до розділу

В данному розділі представлено актуальні теми з екології. Та представлено сучасні методи оцінки стану компонентів навколишнього природного середовища, антропогенного навантаження на стан довкілля. Екологічна оцінка – це виявлення стану середовища життєдіяльності або ступеня впливу на неї сукупності факторів.

Уміле застосування еколого – економічних інструментів в поєднанні з коп'ютерними програмами дозволяє ефективно вирішувати проблеми ресурсозбереження в рамках механізмів саморегулювання ринкової економічної системи.

ВИСНОВКИ

Під час виконання дипломної роботи магістра було досягнуто поставленої мети дослідження, а саме було проведено дослідження по системах та підсистемах захисту «розумного будинку».

В ході виконання дослідження отримано такі результати:

– проведено аналіз літературних джерел та розглянуто проблемні питання;

– розглянуто основні програми інтелектуальної автоматизації;

– були представлені існуючі механізми безпеки, що забезпечують функції безпеки в середовищі «розумного будинку»;

– наведено приклади пристроїв для комфортабельності дому;

– проведено аналіз програмних рішень для «розумного будинку»;

– розглянуто питання забезпечення безпеки користувачів в середовищі дому.

У багатьох випадках більшість домашніх користувачів недостатньо обізнані з безпекою, щоб усвідомити наслідки середовища. Однак важливість безпеки буде піднята в майбутньому через зростаючу складність та неоднорідність внутрішніх мереж та все більш широке використання віддалених робочих звичок для домашніх користувачів. Таким чином, існують вимоги, для зменшення ризиків атак на безпеку в середовищі «розумного будинку». Перш за все, основними вимогами забезпечення безпеки в середовищі є правильне проектування та побудова мереж, а також правильна конфігурація мережевих приладів професіоналами з питань безпеки мережі.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безпека «розумного будинку» [Електронний ресурс] – Режим доступу до ресурсу: URL: https://www.pcmag.com/thebest-smart-home-security-systems – Дата доступу до ресурсу до ресурсу до ресурсу: 07.09.2019.

2. "Умный дом": жить в ногу со временем. [Електронний ресурс] – Режим доступу до ресурсу: URL: http://www.ihome.ru/site.xp/049055044.html – Дата доступу до ресурсу до ресурсу до ресурсу: 08.09.2019.

3. История умного дома. [Електронний ресурс] – Режим доступу до ресурсу: URL: http://scsiexplorer.com.ua/index.php/istoriaotkritiy/2112istorijaumnogodo ma.html – Дата доступу до ресурсу до ресурсу до ресурсу:10.09.2019.

4. Экологически умный дом для экономии электроэнергии [Електронний ресурс] Режим доступу до ресурсу:URL: https://zwavekiev.com.ekologi cheskiyumnyydom_dlyaekonomiielektroene rgii.html – Дата доступу до ресурсу до ресурсу до ресурсу: 15.09.2019.

5. Integrated Wireless Technologies for Smart Homes Applications, Mahmoud A. Al-Qutayri and Jeedella S. Jeedella, 2010.

6. "Умный дом" своими руками. строим интеллектуальную цифровую систему в своей квартире, Тесля Е.В., 2008.

7. Smart Homes For Dummies, by Danny Briere (Author), Pat Hurley (Author), 2007.

8. Что такое умный дом. [Електронний ресурс] – Режим доступу до ресурсу: URL:http://smarton.com.ua/smart_home/

9. Smart Home Systems P. Lalanda, J. Bourcier, J. Bardin and S. Chollet, 2010.

10. Сколько стоит умный дом и что он умеет. [Електронний ресурс] – Режим доступу до ресурсу: URL: http://kievbudservis.com.ua/skolko-stoit-umnyj-dom-i-chto-onumeet/#prettyPhoto – Дата доступу до ресурсу до ресурсу до ресурсу: 28.03.2019.

11. Hu Fei. Wireless sensor networks: principles and practice / Fei Hu, Xiaojun Cao. – Boca Raton: CRC press, 2010. – Т.27, №50.

12. Zhang. F. Effective Algorithms And Protocols For Wireless Networking: a dissertation for the degree of doctor of philosophy / Fenghui Zhang – Texas: Texas A&M University, 2008. – 20 p.

13. Hersent O. The Internet of Things: Key Applications and Protocols / O. Hersent, D. Boswarthick, O. Elloumi. – 2-nd Ed. – Massachusetts : Willey, 2012. — 370 p.

14. Raspberry Pi [Електронний ресурс] // – Режим доступу до ресурсу: URL: https://www.raspberrypi.org/raspbian/ – Дата доступу до ресурсу: 03.10.2019.

15. Arduino Info [Електронний ресурс] // – Режим доступу до ресурсу: URL: https://arduinoinfo.wikispaces.com/ArduinoPower – Дата доступу до ресурсу до ресурсу до ресурсу: 06.10.2019.

16. Ricquebourg et al.,2006; Pohl & Sikora, 2005; Jiang, Liu, & Yang, 2004; Friedewald, Da Costa, Punie, Alahuhta, & Heinonen, 2005.

17. Jeong, Chung, & Choo, 2006; Herzog et al., 2001; Thomas & Sandhu, 2004; Wang, Yang, & Yurcik, 2005; Schwiderski-Grosche, Tomlinson,Goo, & Irvine, 2004; He, 2002.

18. Ricquebourg et al., 2006; Pohl & Sikora, 2005; Valtchev et al., 2002; 2003; HGI, 2006; Delphinanto, 2003.

19. Санітарні норми мікроклімату виробничих приміщень: ДСН 3.3.6.042-99.

20. Природнє і штучне освітлення: ДБН В.2.–2006.

21. Санітарні норми виробничого шуму, ультразвуку та інфразвуку: ДСН 3.3.6.– 2000.

22. Государственные санитарные правила и нормы работы с визуальными дисплейными терминалами электронно-вычислительных машин: ДСанПіН 3.3.2.007-98.

23. Ricquebourg et al., 2006; Pohl & Sikora, 2005; Valtchev et al., 2002; Adams, 2002; Zahariadis, 2003; HGI, 2006.

24. Kim, Lee, Han, & Kim, 2007; Zahariadis,2003; HGI, 2006.

25.Smart hause [Електронний ресурс] – Режим доступу до ресурсу: URL: https://nachasi.com/2018/06/25/smart-house-faq/ – Дата доступу до ресурсу до ресурсу до ресурсу: 20.10.2019.

26. Дистанційне керування домом [Електронний ресурс] – Режим доступу до ресурсу: URL: http://hifidom.com.ua/statti/smarthome/distcontrol – Дата доступу до ресурсу до ресурсу до ресурсу: 21.11.2019.

27. Paruchuri, Durresi, & Ramesh, 2008.

28. Jiang et al., 2004; Teger etal., 2002; Valtchev et al., 2002; Zahariadis, 2003;HGI, 2006; Delphinanto, 2003.

29. Nishi, Morioka, & Sakurai,2005.

30. Tegeret al., 2002; Valtchev et al., 2002; Zahariadis,2003; HGI, 2006)

31. Ricquebourg et al., 2006; Adams, 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003.

32. Krishnamurthy et al., 2002; Hager & Midkiff, 2003.

33. Herzog et al., 2001; Bergstrom et al., 2001; Komninos et al., 2007c; Krishnamurthy et al., 2002.

34. Jeong et al., 2006; Herzog et al., 2001; Kim et al., 2007; Schwiderski-Grosche et al., 2004; Kangas, 2002; He, 2002; Bergstrom et al., 2001; Komninos et al., 2007c.

35. He, 2002; Komninos et al., 2007c; Krishnamurthy et al., 2002.

36. Kim et al., 2007; Kangas, 2002; Komninos & Mantas, 2008, 2009.

37. Kim et al., 2007; Kangas, 2002; Stallings, 2005.

38. Баранов В М. и др. Защита информации в системах и средствах информатизации и связи. Учебное пособие. – СПб.: 1996. – 111 с.

39. Правила безпечної експлуатації електроустановок споживачів, затверджених наказом Комітету по нагляду за охороною праці Міністерства праці та соціальної політики України від 09 січня 1998 року № 4, зареєстрованих у Міністерстві юстиції України 10 лютого 1998.

40. Керування світлом [Електронний ресурс] – Режим доступу до ресурсу: URL: https://www.smarthouse.ua/ua/upravlenie_osvecsheniem.html – Дата доступу до ресурсу до ресурсу до ресурсу: 23.11.2019.

41. «Санитарные правила работы с источниками неиспользуемого рентгеновского излучения». № 1960-79. - М.: «Атомиздат», 1981. -32 с.

42. Climate control [Електронний ресурс] Режим доступу до ресурсу: URL: https://porsche.ua/models/panamera/panamera-4-sport-turismo/comfort-audio/climate-control/ – Дата доступу до ресурсу до ресурсу до ресурсу: 25.11.2019.

43. Кліматичні системи «розумного будинку» [Електронний ресурс] – Режим доступу до ресурсу: URL: https://sutem.com.ua/725smartbus.php – Дата доступу до ресурсу до ресурсу до ресурсу: 27.11.2019.

44. Санітарні норми мікроклімату виробничих приміщень: ДСН 3.3.6.042-99.

45. Система енергозбереження [Електронний ресурс] – Режим доступу до ресурсу: URL: https://sutem.com.ua/3189smartbus.php – Дата доступу до ресурсу до ресурсу до ресурсу: 28.11.2019.

46. Збереження енергії [Електронний ресурс] Режим доступу до ресурсу: URL: http://www.nerc.gov.ua/?id=19531 – Дата доступу до ресурсу до ресурсу до ресурсу: 29.11.2019.

47. Системи охорони «розумного будинку» [Електронний ресурс] – Режим доступу до ресурсу: URL: https://sutem.com.ua/025%20inels.php – Дата доступу до ресурсу до ресурсу до ресурсу: 30.11.2019.

48. Захист «розумного будинку» [Електронний ресурс] Режим доступу до ресурсу: URL: https://eset.ua/ua/news/view/665/zashchita-umnogo-doma-kak-zashchitit-umnyy-dom-ot-kiberprestupnikov – Дата доступу до ресурсу до ресурсу до ресурсу: 01.12.2019.

49. Захист в надзвичайних ситуаціях [Електронний ресурс] – Режим доступу до ресурсу: URL: http://thefuture.news/lessons/ua/smarthome – Дата доступу до ресурсу до ресурсу до ресурсу: 02.12.2019.

50. Захист від протікання [Електронний ресурс] Режим доступу до ресурсу: URL: https://electrica-shop.com.ua/ua/c1210-zahist_vid_zatoplennya – Дата доступу до ресурсу до ресурсу до ресурсу: 03.12.2019.

51. Захист від витоку газу [Електронний ресурс] Режим доступу до ресурсу: URL: https://lvivska-ploscha.com.ua/news/vprovadzhennia-tekhnolohii-riel-smart-home-v-zhk-l-vivs-ka-ploshcha –Дата доступу до ресурсу до ресурсу до ресурсу: 04.12.2019.

52. Загроза інформації [Електронний ресурс] – Режим дотупу до ресурсу: https://uk.wikipedia.org/wiki/ – Дата доступу до ресурсу до ресурсу до ресурсу: 05.12.2019.

53. Безпека даних користувача [Електронний ресурс] – Режим дотупу до ресурсу: chromeextension://html/block_page.html?url=http%3A//suddya.com.ua/news/rozumnii-budinok-ci-v-bezpeci-personalni-danivlasnika&cache=true – Дата доступу до ресурсу до ресурсу до ресурсу: 06.12.2019.

54. RSA [Електронний ресурс] – Режим доступу до ресурсу: URL: https://uk.wikipedia.org/wiki/RSA – Дата доступу до ресурсу до ресурсу до ресурсу: 07.12.2019.

55. Google Cloud Platform IOT Solutions [Електронний ресурс] – Режим доступу до ресурсу: URL: https://developers.google.com/iot – Дата доступу до ресурсу до ресурсу до ресурсу: 08.12.2019.

56. Google cloud IoT [Електронний ресурс] – Режим доступу до ресурсу: URL: https://cloud.google.com/solutions/iot/ – Дата доступу до ресурсу до ресурсу до ресурсу: 09.12.2019.

57. Офіційний сайт компанії Samsung [Електронний ресурс] – Режим доступу до ресурсу: URL: http://developer.samsung.com/smart-home – Дата доступу до ресурсу до ресурсу до ресурсу: 10.12.2019.

58. Samsung smart home [Електронний ресурс] – Режим доступу до ресурсу: URL: https://ipress.ua/news/samsung_smart_home_41167.html – Дата доступу до ресурсу до ресурсу до ресурсу: 11.12.2019.

59. Офіційний сайт компанії Амазон [Електронний ресурс] – Режим доступу до ресурсу: URL: https://aws.amazon.com/?hql_ny_livestream_blu – Дата доступу до ресурсу до ресурсу до ресурсу: 11.12.2019.

60. SmartHome Cloud Solution [Електронний ресурс] – Режим доступу до ресурсу: URL: https://www.globallogic.com/ua/news/doulabsgloballogic-smarthome-solution/ – Дата доступу до ресурсу до ресурсу до ресурсу: 12.12.2019.

61. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2005. - 608 с.: ил.

61. Ярочкин В.И. Информационная безопасность. - М.: Изд-во "Академический проект", 2004. - 640 с.

62. Бармен С. Разработка правил информационной безопасности. - М.: 10.Mark Gasson, Martin Meints, Kevin Warwick (2005), D3.2: A study on PKI and biometrics, FIDIS deliverable (3)2, July 2005.

63. Типи атаки [Електронний ресурс]. – Режим доступу до ресурсу: URL: https://sites.google.com/site/zahistlokalnoiemerezi/tipi-atak – Дата доступу до ресурсу до ресурсу до ресурсу: 13.12.2019.

64. Охорона праці та промислова безпека [Електронний ресурс]. – Режим доступу до ресурсу: URL: https://buklib.net/books/27305/ – Дата доступу до ресурсу до ресурсу до ресурсу: 14.12.2019.

65. Ткачук К.Н., Зацарний В.В., Сабарно Р.В. та інші.: Посібник Охорона праці та промислова безпека. – Київ: Лібра, 2010. –559 с.

66.Режим праці та відпочинку з комп'ютером [Електронний ресурс]. – Режим доступу до ресурсу: URL: https://www.kadrovik.ua/novyny/rezhim-praci-ta-vidpochinkuobidnya-ta-reglamentovani-pererви-pracya-z-kompyuterom – Дата доступу до ресурсу до ресурсу до ресурсу: 15.12.2019.

67. Державні санітарні правила і норми роботи з візуальними диспоейними терміналами ЕОМ [Електронний ресурс] – Режим доступу до ресурсу: URL: https://protocol.ua/ua/proohoronu_pratsi_stattya_16/ – Дата доступу до ресурсу до ресурсу до ресурсу: 16.12.2019.

68. USNRC. 1979. Расчет выбросов радиоактивных материалов в газообразных и жидких сточных водах из реакторов с кипящей водой (код BWR-GALE), NUREG-0016/

69. Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навч. посібник. – 2011. – 215 с.

70. H Dowlatabadi, “Integrated Assessment Models Of Climate Change: An Incomplete Overview”. Energy Policy, 1995

71. Яремко З. М. Безпека життєдіяльності: Навч. посіб. — К., 2005.

72. Програма підготовки студентів вищих навчальних закладів з дисципліни "Безпека життєдіяльності". — К., 2003.

73. Тарасова В.В. Екологічна статистика . 2008 – 392 с.

74.Закон України “Про охорону навколишнього природного середовища” : від 25 червня 1991 року / Верховна Рада України. – Офіц. вид. – К.: Парлам. вид – во, 1991. – 59с. – (Бібліотека офіційних видань).

75. Большаков А. М. Оценка и управление рисками влияния окружающей среды на здоровье населения / Большаков А. М., Крутько В. Н., Пуцилло Е. В. – М.: Эдиториал УРСС, 1999. – 255 с.

76. Ієрархічний підхід до оцінювання екологічного ризику погіршення стану екосистем поверхневих вод України / О. Г. Васенко, О. В. Рибалова, О. В. Поддашкін [та ін.] // Проблеми охорони навколишнього природного середовища та техногенної безпеки : зб. наук. праць УкрНДІЕП. – Харків, 2010. – Вип. XXXII. – С. 75–90.

77. Балацкий О. Ф. Экономика и качество окружающей природной среды. / О. Ф. Балацкий, Л. Г. Мельник, А. Ф. Яковлев. – Л.: Гидрометеоиздат, 1984. – 190 с.

78. Розміщення продуктивних сил України : навч.-метод. посібник [для самост. вивч. дисц.] / [Дорогунцов С. І., Пітюренко Ю. І., Олійник Я. Б. та ін.]. – К. : КНЕУ, 2000. – 364 с.

79. Большаков А. М. Оценка и управление рисками влияния окружающей среды на здоровье населения / Большаков А. М., Крутько В. Н., Пуцилло Е. В. – М.: Эдиториал УРСС, 1999. – 255 с.

80. Ресурсозбереження. Основні положення : ДСТУ 3051-95 (ГОСТ 30166 .

ДОДАТКИ

Додаток А

ІІ Міжнародна студентська науково - технічна конференція
"ПРИРОДНИЧІ ТА ГУМАНІТАРНІ НАУКИ. АКТУАЛЬНІ ПИТАННЯ"

Міністерство освіти і науки України,
Тернопільський національний технічний університет
імені Івана Пулюя
Маріборський університет (Словенія)
Технічний університет в Кошице (Словаччина)
Каунаський технологічний університет (Литва)
Львівський національний університет імені
Івана Франка,
Гірничо-металургійна академія ім. Станіслава Сташиця
(Польща)
Луцький національний технічний університет,
Чернівецький національний університет
імені Юрія Федьковича,
Вроцлавський економічний університет (Польща)
Донбаська державна машинобудівна академія

Студентське наукове товариство

ІІ МІЖНАРОДНА

студентська науково - технічна конференція

"ПРИРОДНИЧІ ТА ГУМАНІТАРНІ НАУКИ.

АКТУАЛЬНІ ПИТАННЯ"

25-26 квітня 2019 р.

(збірник тез конференції)

Тернопіль 2019

Продовження додатку А

II Міжнародна студентська науково - технічна конференція
"ПРИРОДНИЧІ ТА ГУМАНІТАРНІ НАУКИ. АКТУАЛЬНІ ПИТАННЯ"

УДК 004.031

Цубера В.І., Янковська Д.А. - ст.гр. СТм-51, Квач С.М. - ст.гр. САм-51
Тернопільський національний технічний університет імені Івана Пулюя

ПРОГРАМНІ АСПЕКТИ «РОЗУМНОГО БУДИНКУ». АНАЛІЗ ІСНУЮЧИХ ПРОГРАМ ЗАХИСТУ

Tsubera V.I., Yankovska D., Kvach S.M.
Ternopil Ivan Puluj National Technical University

SOFTWARE ASPECTS OF SMART HAUSE. ANALYSIS OF EXISTING PROGRAMS OF PROTECTION

Ключові слова: Розумний будинок, безпека.
Keywords: Smart House, security.

В роботі буде коротко розглянуто концепцію розумного будинку, а також його будову та інформаційно-комунікаційні технології. Безпека розумного будинку є надзвичайно важливою задачею.

В роботі будуть висвітленні важливі питання безпеки в середовищі розумного будинку. Зокрема, будуть описані цілі безпеки розумного дому, а також основні фактори, що підвищують рівень складності для забезпечення безпеки в середовищі розумного будинку (див.рис. 1).

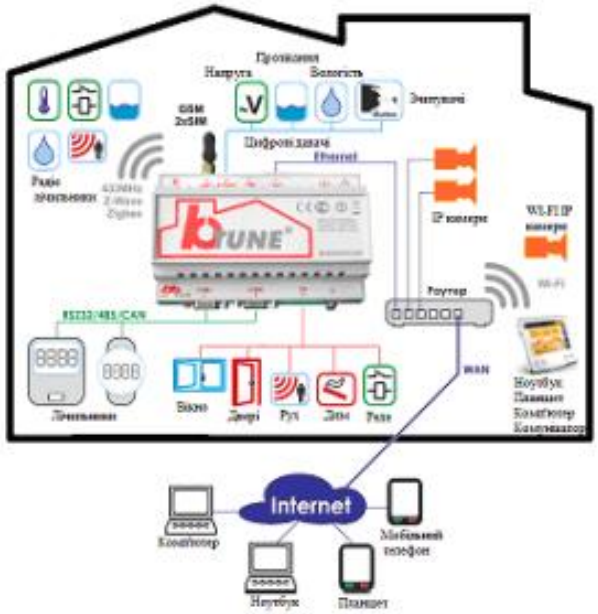

Рисунок 1- Розумний будинок

Внутрішня мережа розумного будинку підлягає численним загрозам, що походять від зовнішніх малих об'єктів. Існують два загальних типи загроз: пасивні та активні атаки.

Продовження додатку А

У пасивних атаках зловмисник має намір отримати несанкціонований доступ до інформації, що передається, не змінюючи її. Виявлення пасивних атак у зв'язку не є простим, оскільки зловмисник не змінює повідомлень, які обмінюються між відправником та одержувачем. Пасивні атаки можуть бути або згортання, або аналіз трафіку [1].

Протягом останніх років концепція Розумний будинок почала стрімко розвиватися,але вона стикається з винятковими проблемами. Однією з цих проблем являється атака програмного забезпечення системи захисту Розумного будинку.

На жаль, більшість систем захисту будівель не мають систему захисту проти кібер-атак. Більшість рішень для захисту, пов'язані з установкою стандартних програм, які виконують функцію брандмауера. Головною частиною будь-якого комплексу програмного забезпечення є сервер. Туди приходять запити від різних клієнтів. Він обробляє всі команди, аналізує параметри системи життєзабезпечення і приймає рішення про здійснення дії. Потім сформована команда передається на драйвери для доступу до мережі. Після чого здійснюється безпосереднє маніпулювання об'єктами.

Інтерфейс користувача може реалізуватися різними способами. Кожен із способів залежить від протоколу.Це може бути мобільний додаток призначений для обміну команд через TCP/IP з'єднання, може розглядатися протокол HTTP, ZigBee, Wi-Fi, Bluetooth, Z-Wave,EnOcean,X 10 і тому подібні [2].

Найбільш важливими технологіями безпеки для створення внутрішньої мережі розумного будинку є механізми аутентифікації та авторизації. Обидва механізми необхідні для обмеження доступу до внутрішньої мережі будь-яким шкідливим об'єктом. Внутрішні загрози виникають у межах довіреної внутрішньої мережі Розумним будинком. Внутрішні загрози можуть бути отримані з невідповідної побудови мережі та конфігурації, неповного плану безпеки та програмних пасток.

Невідповідна побудова внутрішньої мережі Розумного будинку та налаштування пристроїв які підтримують мережу, створюють багато порушень безпеки в середовищі розумного будинку[3]. Дуже важливим є професійне проектування та впровадження внутрішньої мережі та налаштування мережевих пристроїв.

Будь-якому домашньому користувачеві дозволено використовувати будь-який пристрій і отримувати доступ до будь-якої служби. Крім того, будь-хто може змінити внутрішню мережу розумного будинку, оскільки він може змінити конфігурацію мережевого обладнання, додати або видалити мережні пристрої з внутрішньої мережі, а також встановити або видалити програмне забезпечення мережевих пристроїв. Також будь-який домашній користувач може навмисно або ненавмисно змінювати функції безпеки середовища Розумного дому. Таким чином, багато порушень безпеки для порушників можуть бути підняті, коли домашній користувач не відповідає правилам безпеки.

Література

1.Adams, C. E. (2002). Home area network tech-nologies. BT Technology Journal, 20(2), 53–72.

2. Baronti, P., Pillai, P., Chook, V. W. C., Chessa,S., Gotta, A., & Hu, Y. F.(2007). Wireless sen-sor networks: A survey on the state of the art and the 802.15.4 and ZigBee Standards. Computer.

3. Björklund, H. F. (2007, March). Wiring Devices and Technologies in Home Environment. Paper presented at the TKK T-110.5190 Seminar on Internetworking.

4. https://umniedoma.ru/besprovodnoj-umnyj-dom-ot-zigbee-texnologii-i-ustrojstva/

Додаток Б

Міністерство освіти і науки України,
Тернопільський національний технічний університет
імені Івана Пулюя
Маріборський університет (Словенія)
Технічний університет в Кошице (Словаччина)
Каунаський технологічний університет (Литва)
Львівський національний університет імені
Івана Франка,
Гірничо-металургійна академія ім. Станіслава Сташиця
(Польща)
Луцький національний технічний університет,
Чернівецький національний університет
імені Юрія Федьковича,
Вроцлавський економічний університет (Польща)
Донбаська державна машинобудівна академія

Студентське наукове товариство

II МІЖНАРОДНА

студентська науково - технічна конференція

"ПРИРОДНИЧІ ТА ГУМАНІТАРНІ НАУКИ.

АКТУАЛЬНІ ПИТАННЯ"

25-26 квітня 2019 р.

(збірник тез конференції)

Тернопіль 2019

Продовження додатку Б

II Міжнародна студентська науково - технічна конференція
"ПРИРОДНИЧІ ТА ГУМАНІТАРНІ НАУКИ. АКТУАЛЬНІ ПИТАННЯ"

УДК 004.032
Янковська Д., Цубера В.І., ст.гр. СТм-51, Квач С.М., ст.гр. САм-51
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ ІНСНУЮЧИХ РОЗУМНИХ ПАРКОВОК ДЛЯ РОЗУМНОГО МІСТА

Yankovska D., Tsubera V.I., Kvach S.M.
Ternopil Ivan Puluj National Technical University

ANALYSIS OF EXISTING SMART PARKING FOR SMART CITY

Ключові слова: Смарт–парковка, розумне місто, автомобіль.
Keywords: Smart Parking, Smart City, car.

Інноваційна система Smart Parking є рішенням, яке допоможе вирішити проблему дефіциту парковочних місць у великих містах. Постійне збільшення кількості транспортних засобів, високі ціни на землю, невеликі ділянки та вартість будівництва підземного гаражу, що перевищує бюджети інвесторів, роблять систему Smart Parking відмінною альтернативою традиційним парковкам.

Smart Parking надзвичайно проста у використанні та добре розроблена парковка для щоденних зручностей.

Система Smart Parking зазвичай отримує інформацію про наявні місця для паркування в певній географічній зоні, а процес – у режимі реального часу, щоб розмістити транспортні засоби у вільних місцях [4]. Вона передбачає використання недорогих давачів, збору даних у реальному часі та автоматизованих платіжних систем з підтримкою функцій мобільного телефону, які дозволяють водіям заздалегідь зарезервувати місце для паркування або дуже точно передбачити, де вони, швидше за все, знайдуть місце.

Розгляне існуючу парковку «P+» Smart Parking пропонує переконливе рішення задачі обмеженого місця для паркування [1]. Smart Parking – невибаглива, мобільна, гнучка, масштабована система, яка дозволяє власникам і операторам парковки швидко збільшувати свою потужність. Smart Parking стала широко розгорнутим механізованим рішенням для паркування в країнах Європейського Союзу та Азії Використання сучасних інформаційно–комунікаційних технологій дозволяє збільшити попит парковки, отримати нових клієнтів і розширити зони паркування.

Встановлення системи Smart Parking є швидкою та зручною.

Система Smart Parking ідеально підходить для сучасних ділових районів, історичних старих міст, житлових комплексів і торгових та має наступні переваги:

- Легкий у використанні – щоб припаркувати або забрати автомобіль, потрібно лише ввести чотиризначний PIN-код за вашим вибором;
- Швидке час реалізації системи Smart Parking у Вашому місті;
- Тривалий термін служби;
- Низький рівень шуму і вібрації – Smart Parking може бути розташований недалеко від житлових і офісних будівель. Відсутність втручання в мир і комфорт мешканців або працівників;
- Низьке енергоспоживання - потужність двигуна становить від 7,5 до 15 кВт, залежно від моделі пристрою;
- Простий процес технічної перевірки - структура та механізм автоматизованої системи паркування настільки проста, що технічні перевірки можуть бути виконані швидко і ефективно.

Smart Parking обладнаний оптичними датчиками на вході, сигнальними лампами, аварійними вимикачами і захисним обладнанням від падіння з висоти [2].

Продовження додатку Б

Смарт–парковка була розроблена таким чином, щоб зберегти вас і ваш автомобіль в безпеці (див. рис.1).

Рисунок 1 – Загальний вигляд Smart Parking

При використанні системи Smart Parking вам не потрібно турбуватися про злодіїв або про те, що хтось зруйнує ваш автомобіль, треті особи не мають доступу до користування вашим автомобілем.

Простий спосіб паркування в автоматизованій системі паркування знижує до мінімуму можливість випадкових ударів автомобіля та подряпин [3].

Smart Parking є екологічно чистим. Немає необхідності шукати місця для паркування, що призводить до зниження викидів шкідливих газів.

Завдяки застосуванню розумних рішень для паркування, працівники правоохоронних органів можуть бути негайно попереджені про всі порушення [4]. Вони можуть бути проінформовані про важливість кожного з них в пріоритеті. Це дозволить їм швидко очистити серйозні перебої, щоб уникнути проблем, перш ніж перейти до менш тривожних порушень паркування.

Література:

4. http://smartparking-systems.com/katalog/SmartParking-EN-WIROMET-SA.pdf
5. https://www.researchandmarkets.com/research/fdshsn/smart_parking?w=4
6. https://www.happiestminds.com/whitepapers/smart-parking.pdf
7. http://www.enggbook.com/interesting-engineering/p-smart-parking-system/

Авторська довідка

(реферату дипломної роботи магістра)

Назва дипломної роботи магістра: *Функціональні складові інтелектуально керування та підсистема «розумного будинку»*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Functional components of intelektual control and security of «smart house*
переклад англійською

Освітній ступінь : магістр

Шифр та назва спеціальності: 126 Інформаційні системи та технології
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія №29
напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя
напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 24 грудня 2019 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок дипломної роботи: Кількість сторінок реферату:

УДК: 004.89

Автор дипломної роботи
Прізвище, ім'я, по батькові (укр.): Цубера Віталія Іванівна
розкривати ініціали

Прізвище, ім'я (англ.): Tsubera Vitaliia
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра комп'ютерних наук, м.Тернопіль, Україна

Керівник
Прізвище, ім'я, по батькові (укр.): Мацюк Олександр Васильович
повністю

Прізвище, ім'я (англ.): Matsiuk Oleksandr
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра комп'ютерних наук, м.Тернопіль, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри комп'ютерних наук

Рецензент
Прізвище, ім'я, по батькові (укр.): Цуприк Галина Богданівна
повністю

Прізвище, ім'я (англ.): Tsupryk Halyna
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра програмної інженерії, м. Тернопіль, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри програмної інженерії

Ключові слова

українською: будинок, система, дослідження, аналіз, інтелект.
до 10 слів

англійською: hause, system, research, analysis, intelect.
до 10 слів

Анотація

українською:

У дипломній роботі проведено дослідження по функціональних складових інтелектуального керування та підсистем захисту “розумного будинку”».

англійською:

The diploma work conducted research on the Intelligent Control Functional Components and Smart Home Subsystems.

Бібліографічний опис:

1. Цубера В.І., Програмні аспекти «Розумного будинку». Аналіз існуючих програм захисту / Цубера В.І, Янковська Д.А., Квач С.М., // Збірник тез конференції II Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання» , 25-26 квітня 2019 року. — Т. : ТНТУ, 2019. — С. 53-54.

2. Цубера В.І., Аналіз існуючих розумних парковок для розумного міста / Цубера В.І., Янковська Д.А, Квач С.М., // Збірник тез конференції II Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання», 25-26 квітня 2019 року. — Т. : ТНТУ, 2019. — С. 59-60.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМПЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ
І ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА КОМПЮТЕРНИХ НАУК

ЦУБЕРА ВІТАЛІЯ ІВАНІВНА

УДК 004.89

ФУНКІОНАЛЬНІ СКЛАДОВІ ІНТЕЛЕКТУАЛЬНОГО КЕРУВАННЯ ТА ПІДСИСТЕМА ЗАХИСТУ «РОЗУМНОГО БУДИНКУ»

126 «Інформаційні системи та технології»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2019

Роботу виконано на кафедрі копм'ютерних наук Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, доцент
Мацюк Олександр Васильович,
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: кандидат технічних наук, доцент
Цуприк Галина Богданівна,
Тернопільський національний технічний університет імені Івана Пулюя,

Захист відбудеться 24 січня 2019 р. о 9^{30} годині на засіданні екзаменаційної комісії №1 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул.. Руська, 56, навчальний корпус №1, ауд. 702

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи: аналіз функціональних складових інтелектуального керування та підсистем захисту «розумного будинку» на сьогодні є досить актуальним, тому що така техногія дозволяє підвищити рівень безпеки. Створення інтелектуальних будинків і захист обладнання є актуальною тематикою у наш час.

«Розумний будинок» – являється інтелектуальною системою автоматики, яка керує всіма інженерними системами. Кожна людина хоче відчувати комфорт та безпеку, будучи в квартирі чи в офісі. Комфорт та безпека являються основними цілями розумного будинку, а також ектетика вигляду приладів.

На сьогоднішній день інтеграція сучасних комунікаційних та інформаційних технологій у житло призвела до появи «Смарт–домів». Ці технології полегшують створення умов для «розумного будинку», в яких пристрої та системи можуть взаємодіяти один з одним і можуть контролюватися автоматично. Тим не менш, багато проблем з безпекою викликає те що він завжди пов'язаний з зовнішнім світом через Інтернет і «відкриті задні двері» безпеки, отримані від користувачів. Нарешті, переглянувши наявну літературу про «розумні будинки» та питання безпеки, які існують у середовищі, передбачається забезпечити базу для розширення досліджень у сфері безпеки «розумного будинку»

Мета роботи: пошук та проведення аналізу функціональних складових інтелектуального керування та підсистем захисту «розумного будинку», що має допомогти зрозуміти призначення «розумного будинку» в даний час.

На сьогодні існує велика кількість програм для інтелектуального середовища «розумного будинку» які треба проаналізувати та згідно аналізу обрати кращі.

Об’єкт, методи та джерела дослідження. сукупність теоретично-практичних досліджень та основних питань щодо розвитку системи «розумного будинку».

Підсистеми захисту «розумного будинку», орієнтовані на дослідження та опрацювання інформації з урахуванням особливостей систем та підвищення ефективності їх реалізації.

Наукова новизна отриманих результатів: новий підхід щодо опрацювання матеріалу, вирішення поставлених задач. Оцінка та аналіз літературних джерел щодо актуальності дослідження, а також питання забезпечення безпеки будинку.

Результати отримані в роботі можуть бути практично реалізовані.

Практичне значення отриманих результатів. в ході виконання дипломної роботи було проведено загальний аналіз функціональних складових інтелектуального керування та підсистем захисту «розумного будинку», який допоможе визначити головні переваги та недоліки в даній

області та знайдено удосконалене програмне рішення, яке буде дуже просте та зрозуміле для користувачів.

Апробація. Окремі результати роботи доповідались на VI II Міжнародної студентській науково-технічній конференції «Природничі та гуманітарні науки. Актуальні питання» , 25-26 квітня 2019 року. — Т. : ТНТУ.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 6 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 105 арк. формату А4.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі проведено огляд «розумного будинку», та проблематику його захисту та охарактеризовано основні завдання, які необхідно вирішити, обґрунтовано актуальність роботи, визначено мету та завдання роботи.

В розділі **«Аналіз існуючих рішень для «розумного будинку»** проведено аналіз стану питання за літературними та іншими джерелами. Оглянуто існуючі рішення, концепцію та створення перших «розумних будинків», розглянута система інтелектуальної автоматизації та розглянуто підсистеми «розумного будинку», наведені вимоги безпеки інтелектуального середовища, розглянуто технології безпеки для «розумних будинків», виконано постановку задачі на дипломну роботу.

В розділі **«Огляд апаратних та програмних рішень для системи безпеки «розумного будинку»** було досліджено та аналізовано основні складові функціоналу будинку (датчики, сенсорні панелі, та інше), та проведено аналіз існуючих платформ, таких як Google Cloud Platform. Samsung Smart Home та GL SmartHome Smart Solution щодо захисту будинку.

В розділі «**Спеціальна частина**» класифіковано загрози безпеки інформації, наведено види найбільш поширених загроз, проаналізовані програмні атаки та класифікація заходів забезпечення безпеки комп'ютерних систем та систем «розумного будинку».

В розділі **«Обґрунтування економічної ефективності»** було розраховано норми часу на виконання науково–дослідної роботи, визначено витрати на оплату праці та відрахування на соціальні заходи, було розраховано матеріальні витрати, витрати на електроенергію, розраховано суму амортизаційних відрахувань, обчислено накладні витрати, складено кошторис витрат та визначено собівартість роботи, розраховано вартість проведення дослідження та визначено економічну ефективність і термін окупності капітальних вкладень.

В розділі «**Охорона праці та безпека в надзвичайних ситуаціях»** проаналізовано поняття щодо комісії з питань охорони праці: склад, основні

завдання та права. Було досліджено режим праці та відпочинку працівників, які використовують у своїй роботі персональний комп'ютер. Також було проаналізовано питання безпеки в надзвичайних ситуаціях, таких, як комп'ютерне забезпечення процесу оцінки радіаційної та хімічної обстановки та ергономічні вимоги до робочого місця користувача персональним комп'ютером.

В розділі **«Екологія»** була досліджена статистична оцінка екологічного стану навколишнього природного середовища та закономірностей його розподілу та роль матеріало– та ресурсозбереження у вирішенні екологічних проблем.

У загальних висновках щодо дипломної роботи описано прийняті заходи, що забезпечують захист «розумного будинку», прийняті автором в процесі роботи.

ВИСНОВКИ

Під час виконання магістерської роботи було досягнуто поставленої мети дослідження, а саме було проведено дослідження по системах та підсистемах захисту «розумного будинку».

В ході виконання дослідження отримано такі результати:

– проведено аналіз літературних джерел та розглянуто проблемні питання;

– розглянуто основні програми інтелектуальної автоматизації;

– були представлені існуючі механізми безпеки, що забезпечують функції безпеки в середовищі «розумного будинку»;

– наведено приклади пристроїв для комфортабельності дому;

– проведено аналіз програмних рішень для «розумного будинку»;

– розглянуто питання забезпечення безпеки користувачів в середовищі дому.

У багатьох випадках більшість домашніх користувачів недостатньо обізнані з безпекою, щоб усвідомити наслідки середовища. Однак важливість безпеки буде піднята в майбутньому через зростаючу складність та неоднорідність внутрішніх мереж та все більш широке використання віддалених робочих звичок для домашніх користувачів. Таким чином, існують вимоги, для зменшення ризиків атак на безпеку в середовищі «розумного будинку». Перш за все, основними вимогами забезпечення безпеки в середовищі є правильне проектування та побудова мереж, а також правильна конфігурація мережевих приладів професіоналами з питань безпеки мережі.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Цубера В.І., Програмні аспекти «Розумного будинку». Аналіз існуючих програм захисту / Цубера В.І,Янковська, Квач С.М., // Збірник тез конференції II Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання» , 25-26 квітня 2019 року. — Т. : ТНТУ, 2019. — С. 53-54.

2. Цубера В.І., Аналіз існуючих розумних парковок для розумного міста / Цубера В.І.,Янковська Д.А, Квач С.М., // Збірник тез конференції II Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання» , 25-26 квітня 2019 року. — Т. : ТНТУ, 2019. — С. 59-60.

АНОТАЦІЯ

У дипломній роботі проведено дослідження по функціональних складових інтелектуального керування та підсистем захисту “розумного будинку”».

У першому розділі було проведено аналіз наукових статей та публікації по темі дипломної роботи. Розглянуто основні терміни та концепцію «розумного будинку».

Під час виконання другого розділу було проведено аналіз основних програм інтелектуальної системи «розумного будинку», а саме: апаратні та програмні рішення щодо безпеки та комфорту користувачів в середовищі «розумного будинку».

Ключові слова: БУДИНОК, СИСТЕМА, ДОСЛІДЖЕННЯ, АНАЛІЗ, ІНТЕЛЕКТ.

ANNOTATION

The diploma work conducted research on the Intelligent Control Functional Components and Smart Home Subsystems.

The first section of the analysis of scientific articles and publications on the topic of diploma work was carried out. The basic terms and concepts regarding «smart house».

During the implementation of the second section, the main programs of the intelligent System of "smart home", namely: hardware and software solutions for user safety and comfort in a «smart home» environment.

Keywords: HOUSE, SYSTEM, RESEARCH, ANALYSIS, INTELLECT.