НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТімені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем
(повна назва кафедри)

«До захисту допущено»
Завідувач кафедри
_____ Сергій НАЙДА
(підпис) (ініціали, прізвище)
“01” червня 2020 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності (спеціалізації]) . 171 Електроніка (Електронні та інформаційні системи і технології телебачення, кінематографії та звукотехніки)
(код і назва)

на тему: «Захист інформації в технологіях «розумного будинку»

Виконав: студент IV курсу, групи ДВ-61
(шифр групи)

Овсієнко Кирило Миколайович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник
доцент, к.т.н., доцент. Лазебний В.С. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант
_____ _____ _____
(назва розділу) (посада, вчене звання,науковий ступінь,прізвище, ініціали) (підпис)

Рецензент .доцент каф.ЕПС, с.н.с, к.т.н. Терлецький О.В. _____
(посада,науковий ступінь,вчене звання,науковий ступінь,прізвище,ініціали) (підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет Електроніки

Кафедра акустичних та мультимедійних електронних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність (спеціалізація) 171 Електроніка. (Електронні та інформаційні системи і технології телебачення, кінематографії та звукотехніки)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій НАЙДА
(підпис) (ініціали, прізвище)
«25» травня 2020 р.

ЗАВДАННЯ
на дипломну роботу студенту

Овсієнку Кирилу Миколайовичу
(прізвище, ім'я, по батькові)

1 Тема роботи: «Захист інформації в технологіях розумного будинку»

керівник роботи Лазебний Володимир Семенович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «25»травня 2020 р. №1196-с

2 Термін подання студентом роботи 01 червня 2020 р.

3 Початкові дані до роботи: 1) Протокол Wi-Fi; 2)Протокол ZigBEE; 3) Протокол WeMo 4) Протокол Thread; 5) Протокол Z-Wave

4 Зміст роботи: 1) Розглянути основні характеристики «розумного будинку» як об'єкта захисту 2) Проаналізувати вразливості і фактори в технологіях «розумного будинку» 3) Дослідити загрози конфіденційності, цілісності та доступності інформації ІТ-системи «розумного будинку» 4)

Зробити порівняльний аналіз характеристик наявних технологій.

5 Перелік ілюстративного матеріалу: комплект презентації за матеріалами проведеного дослідження.

6. Консультанти розділів роботи

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

7. Дата видачі завдання 11 березня 2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Пошук та опрацювання матеріалів	24.03.2020	виконано
2	Аналіз основних характеристик «розумного будинку»	20.04.2020	виконано
3	Написання тексту атестаційної роботи	10.05.2020	виконано
4	Підготовка матеріалів до друку та оформлення пояснювальної записки	30.05.2020	виконано
5	Підготовка та оформлення презентації для доповіді	1.06.2020	виконано

Студент _____ Кирило ОВСІЄНКО
(підпис) (ініціали, прізвище)

Керівник роботи _____ Володимир ЛАЗЕБНИЙ
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Дипломна робота: 58 с., 15 рис., 16 табл., 1 дод., 20 джерел.

РОЗУМНИЙ БУДИНОК, ПРОТОКОЛ, ІНТЕРЕНЕТ РЕЧЕЙ, БЕЗПРОВОДОВІ, ЗАХИСТ ІНФОРМАЦІЇ, СТАНДАРТ, ТЕХНОЛОГІЯ, ПЕРЕВАГИ, НЕДОЛІКИ, ZIGBEE, WEMO , Z-WAVE, WI-FI.

Метою дипломної роботи є дослідити надійність технологій обміну інформацією у системі керування «розумним» будинком, узагальнити особливості застосування технологій передавання даних і їх захищеності щодо різних впливів, розробити рекомендації щодо їх використання.

Методами дослідження є критичний аналіз для з'ясування характеристик та особливостей захищеності інформації в технологіях «Розумного будинку», порівняльний аналіз для дослідження наявних систем.

Об'єктом дослідження є технології передавання даних в системах «Розумного будинку»

Предметом дослідження є захист інформації в технологіях та системах «Розумного будинку».

Новизна роботи полягає в узагальненні наявної інформації про захист інформації в технологіях обміну даними в системі «Розумний будинок» та розроблених рекомендаціях щодо вибору технологій для забезпечення високого рівня захищеності і надійності функціонування систем.

Отримані в дипломній роботі результати і розроблені рекомендації щодо вибору технологій передавання даних для застосування в системах розумного будинку будуть корисні розробникам зазначених систем для забезпечення високого ступеня захищеності і надійності їх функціонування. Результати роботи будуть корисними в навчальному процесі підготовки фахівців у сфері систем Інтернету речей.

ABSTRACT

The object of study is the protection of information in the technologies and systems of "Smart Home".

The subject of the study is “Smart Home” as a holistic and reliable system.

The novelty of the work is to summarize the available information on the protection of information in technologies and the developed recommendations for choosing the most reliable for use in the Smart Home system

The result of the thesis is the generalization of world experience in strengthening information protection, the formation of comparative characteristics of various protocols of the home automation system, the clarification of the positive and negative properties of protocols and their architecture.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AES – Advanced Encryption

IEEE – Institute of Electrical and Electronics Engineers

OSI – The Open Systems Interconnection model

IP – Internet Protocol

IPv6 – Internet Protocol version 6

Wi-Fi – Wireless Fidelity

USB – Universal Serial Bus

SIG – Special Interest Group

BLE – Bluetooth Low Energy

IoT – Internet of Things

UHF – Ultra high frequency

SHF – Super high frequency

ISM – industrial, scientific and medical

WPAN – Wireless personal area network

MAC – Media Access Control

CSMA – Carrier Sense Multiple Acces

CRC – Cyclic redundancy check

LAN – Local Area Network

ANT – Adaptive Network Topology

ВСТУП

Використання ІТ-технологій дозволяє створити «Розумний будинок» тобто сукупність програмно-апаратних систем, безпосередньо керуючих інженерно-технічними, енергетичними, комунікаційними та іншими підсистемами житлового приміщення.

Однак використання ІТ-інфраструктури, зокрема інформаційних систем управління нерозривно пов'язане з вирішенням питань забезпечення безпеки такої інфраструктури. Практична значимість проблеми забезпечення безпеки «розумного будинку» полягає в реалізації заходів щодо захисту ІТ-інфраструктури для забезпечення особистої безпеки проживаючих громадян, забезпечення їх здоров'я і необхідних санітарно-гігієнічних умов, захисту майна. Існує проблема, пов'язана з неповною або недостатнім опрацюванням і дослідженням загроз перш за все інформаційної безпеки «розумного будинку» і відповідно, недостатніми механізмами їм протидії.

Актуальність теми зумовлена повсюдним розвитком інформаційно-технологічної (ІТ) інфраструктури і її застосуванням для забезпечення комфортного проживання громадян в багатоквартирних та індивідуальних будинках.

Роботу виконано за тематикою наукових досліджень, здійснюваних на кафедрі акустичних та мультимедійних електронних систем, а саме «Дослідження стійкості протоколів систем доступу та віддаленого керування».

Метою дипломної роботи є дослідити надійність технологій обміну інформацією у системі керування «розумним» будинком, узагальнити особливості застосування технологій передавання даних і їх захищеності щодо різних впливів, розробити рекомендації щодо їх використання.

Методами дослідження є критичний аналіз для з’ясування характеристик та особливостей захищеності інформації в технологіях «Розумного будинку», порівняльний аналіз для дослідження наявних систем.

Об’єктом дослідження є технології передавання даних в системах «Розумного. будинку».

Предметом дослідження є захист інформації в технологіях та системах «Розумного будинку».

Новизна роботи полягає в узагальненні наявної інформації про захист інформації в технологіях та розроблених рекомендаціях щодо вибору найнадійнішої для використання в системі «Розумний будинок».

Практична цінність. Результати роботи будуть корисними для фахівців, що працюють у сфері Інтернет зв’язку і систем доступу до інформаційних ресурсів. Результати можна використати під час планування та уведення в експлуатацію мереж віддаленого доступу та внутрішнього доступу, а також у навчальному процесі під час підготовки фахівців у сфері електроніки.

1 ДОСЛІДЖЕННЯ ОСНОВНИХ ХАРАКТЕРИСТИК «РОЗУМНОГО БУДИНКУ» ЯК ОБ'ЄКТА ЗАХИСТУ

1.1 Основні положення по організації системи «розумного будинку»

«Розумний будинок» (англ. smart home) або «інтелектуальний будинок» (англ. "intelligent building") – будинок сучасного типу, організований для проживання людей за допомогою автоматизації і високотехнологічних пристроїв. Під «розумним» будинком слід розуміти систему, яка забезпечує безпеку, комфорт і ресурсозбереження для всіх користувачів.

У найпростішому випадку вона повинна вміти розпізнавати конкретні ситуації, що відбуваються в будинку, і відповідним чином на них реагувати: одна з систем може управляти поведінкою інших за заздалегідь виробленим алгоритмом. Іншими словами, це будівля, інженерні системи якої здатні забезпечити адаптацію до можливих змін в майбутньому.
Як об'єкт захисту «розумний дім» представляє собою являє собою житлове або нежитлове (яке не використовується для проживання) приміщення, оснащене засобами обчислювальної техніки і управління, що підтримують інформаційні технології, які здатні діяти про активно з метою задоволення потреби людини в комфортному та безпечному проживанні. Зазначений комплекс засобів обчислювальної техніки, управління (у вигляді виконавчих реле, актуаторів) здатний реагувати на зміни потреб людини, шляхом створення і підтримки нормативних санітарно-гігієнічних умов для повсякденної діяльності людини, а також забезпечення особистої безпеки, зниження ризику нанесення шкоди здоров'ю громадян та їх майну [16]. Таким чином, мета управління в рамках «розумного будинку» - забезпечення комфортних і безпечних умов життєдіяльності або проживання досягається за допомогою автоматизованого управління системами життєзабезпечення усередині будинку / житлового приміщення, в тому числі шляхом комунікації з навколишнім середовищем за допомогою інфокомунікацій.

Застосування комплексу засобів автоматизації та інформаційних технологій «розумного будинку» дозволяє забезпечити ефективну та безпечну експлуатацію, запобігти ризику нанесення шкоди, що приводить до відмови чи аварії устаткування інженерних комунікацій, вентиляції, опалення, систем енергозабезпечення, газопостачання, охороги, холодного і гарячого водопостачання, водовідведення, систем зв'язку та інших систем будівель і споруд [17].

Під терміном «розумний будинок» мають на увазі приміщення в офісних та житлових будівлях, квартирах, будинках з єдиною автоматизованою системою управління і моніторингу всіх підсистем життєзабезпечення і безпеки (рис. 1.1).

Рисунок 1.1 – Основні підсистеми «розумного будинку»

Докладніший список підсистем, контрольованих і керованих в рамках «розумного будинку», виглядає наступним чином:

- управління освітленням;
- управління опаленням і гарячим водопостачанням;
- управління холодним водопостачанням і контроль протікання трубопроводів;
- управління медичними системами життєзабезпечення (в разі їх установки в будинку);

- управління електричними мережами для подачі електроенергії і вторинними джерелами електроживлення;
- домашній кінотеатр і системи аудіо- і відео розваг;
- система телефонного зв'язку, включаючи бездротові телефони DECT та радіотелефонні трубки;
- система супутникового і / або ефірного і / або кабельного телебачення;
- система інтернет-доступу (локальна обчислювальна мережа) обладнання доступу;
- система охоронно-пожежної сигналізації;
- система відеоспостереження;
- системи інженерної безпеки і захисту від перевантажень;
- система контролю і управління доступом в приміщення;
- віддалене управління «розумним будинком»;
- система кондиціонування і вентиляції;
- управління прибудинкової інфраструктурою (освітлення, датчики контролю периметра будівлі / ділянки, дистанційне керування в'їзними воротами або воротами в гараж).

У той же час можна зустріти використання терміна «інтелектуальний будинок» (intellectual building), який вживається, коли мова йде про комплексної автоматизації управління будівлями, не призначеними для проживання або багатоквартирних житлових будинках [1].

Таким чином, термін «розумний дім» тут і далі буде вживатися перш за все щодо житлових (індивідуальних) будинків, квартир в багатоквартирному будинку або для ізольованих приміщень в будівлях, не призначених для проживання, які не входять в контур управління «інтелектуальним будинком».

За способом організації та побудови систем «розумний дім» можна виділити два способи або підходу:

- децентралізований спосіб;
- централізований спосіб.

Система «розумний будинок», побудована з централізованого способу, складається з елемента управління, центрального контролера і керованого устаткування, об'єднаних в єдину телекомунікаційну мережу для прийому та передачі сигналів або команд управління (рис. 1.2).

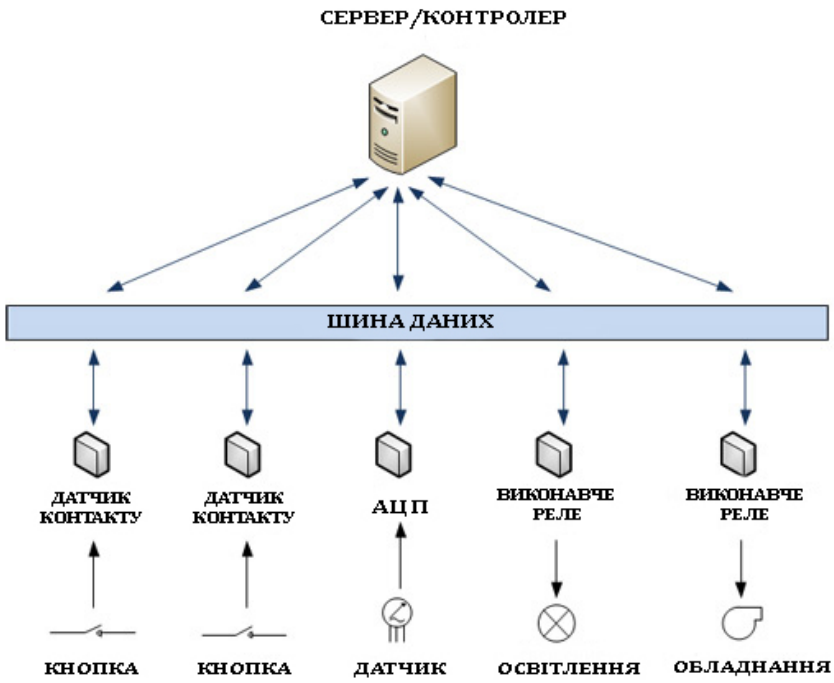

Рисунок 1.2 – Схема централізованої системи «розумного будинку» з головним комп'ютером

Елемент управління - це обчислювальний або командне пристрій (пульт), за допомогою якого можна передати виконавчу команду системі «розумного будинку». Елементом управління може бути пульт управління, touch-панелі, смартфони і різні датчики (освітленості, присутності, температури, вологості і т.д.) [3].

Центральний контролер управляє системою в цілому і кожним окремим елементом. Це обчислювальний пристрій, який зберігає в пам'яті і виконує всі команди від користувача або по виконуваній програмі. До керованого обладнання «розумного будинку» в цілому ставляться всі побутові прилади і домашня техніка, починаючи від електролампочки і закінчуючи складними системами охорони і контролю складу повітря.

Децентралізований підхід має на увазі розгортання системи з розподіленою логікою виконання команд. На відміну від централізованого підходу, в децентралізованому підході відсутній центральний контролер. В цьому випадку система складається з датчиків, сенсорів і активаторів (рис. 1.3). Датчики виявляють зміна будь-яких характеристик в будинку, руху або зміни заданих в програмі параметрів, і реагують на ці зміни командою виконуючим пристроям, які включаються активаторами [6].

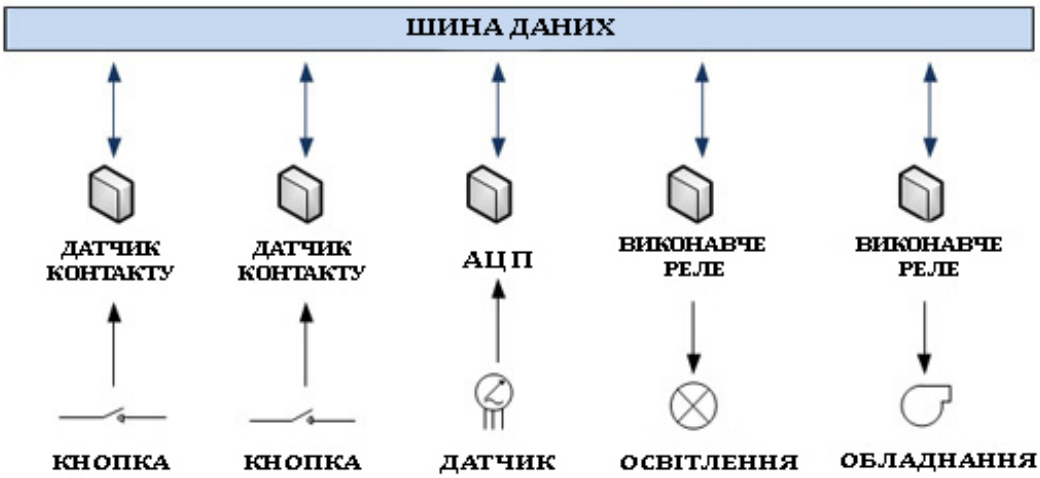

Рисунок 1.3 – Схема децентралізованої системи «розумного будинку» без контролера керування

1.2 Дослідження характеристик основних підсистем «розумного будинку»

Як вже говорилося раніше, до основних підсистем «розумного будинку» відносяться системи: освітлення, клімат-контролю, безпеки і моніторингу, комунікаційних мереж і мультимедіа (рис 1.4). Для визначення та аналізу загроз інформаційній безпеці потрібно визначити характерні особливості підсистем «розумного будинку».

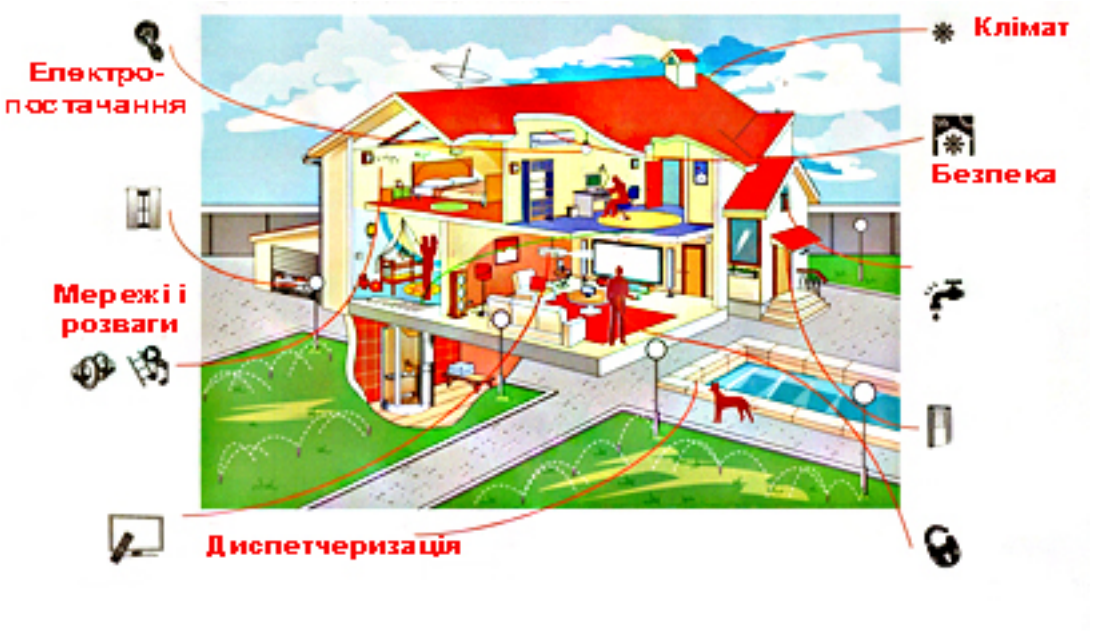

Рисунок 1.4 – Основні системи «розумного будинку»

Розглянемо кожну з цих підсистем докладніше.

Підсистема освітлення (Lighting control systems, LCS), об'єднує всі освітлювальні прилади в приміщенні і на прилеглій території в єдину мережу. Це забезпечує контроль над процесом їх взаємодії і гарантує значну економію енергоресурсів.

Можливості підсистеми освітлення «розумного будинку» великі, в їх число входить:

– економія енергоресурсів, коли «розумний будинок», завдяки інтелектуальному автоматичному управлінню освітленням дозволяє значно збільшити термін служби електроламп і знизити використання електроенергії;
– дистанційний і централізований контроль над освітленням, коли включення і відключення всіх освітлювальних приладів в системі «розумний будинок» може здійснюватися за сигналом, який скеровується з одного автоматизованого пристрою, використовуючи які можна безпосередньо біля виходу з будинку відключити світло у всіх кімнатах;

– регулювання яскравості світіння ламп, коли в «розумному будинку» автоматизовані освітлювальні прилади, як правило, оснащуються диммерами. «Розумний будинок» з системою діммірованія дозволяє робити світло яскравішим, коли це необхідно, або приглушеним, коли не потрібно, щоб лампи працювали на повну потужність;
- автоматична робота, коли «розумний дім» виходячи з тих даних, які надходять з датчиків присутності, руху і освітленості, або в залежності від часу доби автоматично регулює освітлення в будинку (включення вуличних світильників відбувається у вечірній час, а поступове зменшення їх яскравості до повного відключення - рано вранці, включення / вимикання освітлення за фактом наявності / відсутності людей в приміщенні).

Підсистема клімат-контролю, де реалізація цієї системи досягається шляхом інтеграції та узгодження роботи трьох кліматичних систем - опалення, вентиляції та кондиціонування (Heating, Ventilation and Air Conditioning, HVAC). Підсистема забезпечує підтримку температури, вологості і надходження свіжого повітря в приміщеннях в заданих межах, спираючись на показники датчиків, контрольно-вимірювальних приладів і обладнання [4].

Також можлива настройка зонального еко-клімату для різних кімнат житлового будинку. У кожному приміщенні «розумного будинку» може бути заданий власний режим життєзабезпечення, згідно з такими припущеннями (для зимового періоду):

– на кухні досить нагрівати повітря до +19 ° С, але при цьому вентиляція повинна працювати більш інтенсивно, ніж у вітальні або спальні.
– нормальний сон при +25 ° С некомфортний, тому вночі в спальних приміщеннях краще знизити температуру повітря до 18 ° С;
– в передпокої, в коридорах і на сходових майданчиках мешканці зазвичай надовго не затримуються, тому з метою економії енергії, піднімати там температуру вище +17, +18 ° С нераціонально;

- в підсобних приміщеннях, таких як гараж і бойлерна, комора досить підтримувати плюсову температуру на рівні + 7 ... + 9 градусів.

Підсистему безпеки та моніторингу умовно можна розділити на наступні підсистеми:

- система відеоспостереження пропонує здійснення візуального контролю за внутрішніми приміщеннями житла та / або дворової територією. Алгоритм включення камер може бути різним: безперервна робота або реакція на рух (при спрацьовуванні відповідного датчика - автоматично включати запис і оповіщати тривожним сигналом). Також зображення з відеокамер можна переглядати віддалено через Інтернет;
- система контролю доступу та охорони периметра покликана обмежувати і реєструвати людей, що входять в приміщення і / або на вашу ділянку, за рахунок встановлених датчиків (руху, розбиття скла і т.п.) і відеоспостереження;
- система охоронно-пожежної сигналізації (ОПС) призначена для цілодобового контролю об'єкту, що охороняється, а зокрема для раннього оповіщення власника про виявлення ознак пожежі або задимлення і включення засобів пожежогасіння;
- система контролю витоків газу та захисту від протікання води - автоматичне блокування при виявленні протікання;
- GSM / UMTS моніторинг - видалене інформування про інциденти в будинку (квартирі, офісі, об'єкті) і управління системами «розумного будинку» через смартфон.

Підсистема комунікаційних мереж, яка заснована на телекомунікаційній мережі, яка є основним елементом, що забезпечує функціонування системи «розумного будинку».

Підсистема комунікаційних мереж, яка заснована на телекомунікаційній мережі, яка є основним елементом, що забезпечує функціонування системи «розумного будинку». Через неї здійснюється збір інформації з різних датчиків і

передача їх головного сервера для обробки (при централізованому підході в побудові «розумного будинку»). Сервер після обробки інформації передає сигнали управління на виконавчі елементи (датчики перекриття води, включення засобів пожежогасіння, блокування дверей і т.д.).

Така телекомунікаційна мережа може бути побудована з використанням як провідних, так і бездротових каналів зв'язку. Для бездротового зв'язку застосовуються технології Wi-Fi, Bluetooth, LTE, що є основою для таких протокол передачі інформації як ZigBee, WirelessHART, LPWAN і т.п. Серед провідних технологій виділяють Ethernet і PLC рішення (Power line communication) - технологія побудови мереж передачі даних по лініях електропередач [5].

Підсистема розваг (мультимедіа) надає єдиний інтерфейс, за допомогою якого можна керувати різними цифровими пристроями і відтворювати на них фільми, музику, переглядати метеозведення або інший контент. Дану систему можна розділити на 4 підсистеми:

- мультирум - система розподілу аудіо - або відеосигналів (A / V) с різних джерел в безліч зон. В даному випадку під зонами розуміються не тільки приміщення всередині будинку, а й прилегла територія;
- телебачення - система домашньої автоматизації поширюється також на супутникове та ефірне телебачення, яке в «розумному будинку» розподіляється за допомогою одного ресивера на всі пристрої відображення;
- медіасервер - сукупність програмного та апаратного забезпечення, яка дозволяє комутувати, зберігати і транслювати медіа контент (аудіозаписи, відеозаписи, зображення) на різні пристрої (телевізори, проектори, акустичні системи й т. Д.);
- джерела контенту - це різні цифрові пристрої, які необхідні для відтворення, передачі і зберігання відео і аудіо даних (кіно, музика, телебачення, радіо).

Таким чином, основою системи «розумний дім» є телекомунікаційна (комп'ютерна) мережа, тому загрози інформаційної безпеки в першу чергу можуть виникати за рахунок вразливостей мережевої структури:

- коди операційної системи (наприклад, вразливість при переповненні пам'яті, управління оновленнями операційної системи);
- транспортні протоколи, наприклад, протокол TCP, DNS, SMTP або ICMP;
- дефекти прикладних програм (firmware, наприклад, Apache);
- помилки в програмах користувача;
- програмне забезпечення, вбудоване в апаратні пристрої, наприклад, в маршрутизатори, BIOS;
- перехоплення повідомлень і управління в бездротових системах.

2 АНАЛІЗ ВРАЗЛИВОСТЕЙ І ФАКТОРІВ В ТЕХНОЛОГІЯХ «РОЗУМНОГО БУДИНКУ»

2.1 Аналіз вразливостей і факторів, що впливають на датчики контролю і захисту в системі «розумний дім»

Ефективна і багатофункціональна система «розумного будинку» включає в себе різноманітні датчики, які реєструють і передають параметри середовища, і іншу важливу інформацію. Датчики автоматизації представляють собою автономний самостійний пристрій, що змінює свій сигнал відповідно відстежувати параметру.

Ці обов'язкові елементи «розумного будинку» розрізняються за призначенням і принципом дії, умовно їх можна умовно розділити на дві групи: датчики, які відстежують рух і датчики, що реагують на параметри середовища. Датчики, які відстежують рух, які використовуються в охоронних системах і для побудови інтелектуального освітлення. Такі датчики поділяються на датчики руху і датчики присутності. Датчики присутності відрізняються від датчиків руху тим, що фіксують навіть дуже дрібні рухи, що відбуваються в межах робочої зони датчика, в іншому принцип їх роботи однаковий [14].

В даний час найбільшого поширення набули такі види датчиків руху і присутності:

1) інфрачервоні датчики (ІК) (рис. 2.1)

Рисунок 2.1 – Приклад загального вигляду інфрачервоного датчика

Принцип роботи інфрачервоних датчиків руху полягає в виявленні змін інфрачервоного (теплового) випромінювання навколишніх об'єктів. Кожен об'єкт має температуру випускає інфрачервоне випромінювання, яке через систему лінз або спеціальних увігнутих сегментованих дзеркал, потрапляє на розташований всередині датчика руху чутливий сенсор, що реєструє це.

Вразливістю даного датчика є т.зв. «Сліпа зона», при якій він не зможе фіксувати об'єкти певної висоти. Крім того, датчик має обмеження по діапазону робочих температур, наприклад, тільки в діапазоні від -10 0С до + 40 0С;

2) ультразвукові датчики (УЗ) (рис. 2.2).

Рисунок 2.2 – Приклад загального вигляду ультразвукового датчика

Принцип роботи ультразвукового датчика руху полягає в дослідженні навколишнього простору за допомогою звукових хвиль, частотою знаходиться за межами чутності людським вухом - ультразвуком (в залежності від виробника і моделі зазвичай генерується частота звукової хвилі 20-60 кГц). При виявленні зміни частоти відбитого сигналу, внаслідок руху об'єктів, датчик запускає закладену в неї функцію, це може бути включення освітлення або розрив сигнальної мережі охоронної системи [7].

Вразливістю даного датчика є обмежений по відстані діапазон чутливості, наприклад, від 200 мм до 8 м. Якщо об'єкт знаходиться на відстані менше 200 мм, відбуваються помилкові спрацьовування. Якщо кілька датчиків знаходяться в безпосередній близькості, що може зробити їх уразливими для перехресних перешкод, що запобігає спеціальним контролером для включення датчиків по

одному;

3) мікрохвильові датчики (СВЧ) (рис. 2.3).

Рисунок 2.3 – Приклад загального вигляду мікрохвильового датчика

Мікрохвильовий датчик руху випромінює високочастотні електромагнітні хвилі (частота хвиль може бути різною в залежності від виробника, зазвичай вона становить 5,8 ГГц), які відбиваючись від навколишніх об'єктів, реєструються сенсором і в разі виявлення найменших змін відбитих електромагнітних хвиль, мікропроцесор пристрою пускає в хід закладену в нього функцію. Вразливістю мікрохвильового датчика є невірне визначення порогу чутливості.

Поріг - якесь значення, нижче якого сигнали інтерпретуються як шуми. Поріг регулюється під час налаштування датчика. Чим більше чутливість, тим більша ймовірність виявлення. Але при збільшенні чутливості зростає і частота помилкових тривог, що знижує довіру до системи в цілому. Також поява помилкових тривог може бути викликано недоліками конструктивних і схемотехнічних рішень; неправильною установкою і налаштуванням датчика; недоліками алгоритму обробки сигналів.

Недоліки конструктивних і схемотехнічних рішень можуть призвести до наведенням в ланцюгах передачі даних, наприклад, через погане екранування, поганий фільтрації, застосування дешевої неякісної елементної бази. Типовою проблемою є зміна параметрів електронних компонент при наближенні до кордонів допустимого температурного діапазону. Для вирішення цієї проблеми доводиться розробляти спеціальні схеми термостабілізації параметрів і т.д [12].

Неправильне налаштування датчика може привести до виходу зони виявлення датчика за межі зони, що охороняється, особливо в приміщеннях зі

складною конфігурацією. Це призведе до того, що такий датчик буде спрацьовувати, наприклад, при знаходженні людей в сусідніх приміщеннях.

Уразливість датчика може бути обумовлена збуреннями середовища, в тому числі електромагнітними наведеннями, паралельною роботою кількох датчиків. Далі розглянемо т.зв. комбіновані датчики, які мають можливість об'єднувати в системі безпеки функції різних методів реєстрації зміни стану навколишнього середовища, розглянуті вище;

4) комбіновані датчики (рис. 2.4).

Рисунок 2.4 – Загальний вигляд комбінованого датчика

Комбіновані датчики руху поєднують в собі відразу декілька технологій виявлення рухів, наприклад, інфрачервоний датчик і мікрохвильовою. Це найбільш вдале рішення, якщо потрібно більш точне визначення переміщень в зоні дії датчика.

Також існують магнітноконтактние датчики, що діють при зміні відстані між магнітом і герконом (змикання і розмикання складових частин) і датчики розбиття скла. За принципом дії датчики пошкодження скла класифікуються:

- електроконтактні датчики - сповіщають про порушення цілісності скляного полотна за допомогою механічного впливу, наприклад, удару або вирізання отвору;
- п'єзоелектричні датчики, які реєструють механічні коливання, що виникають при ударі скла;
- акустичні датчики, що реагують на звукові коливання, які видаються при руйнуванні скла.

Датчики, що реагують на параметри навколишнього середовища. Дані пристрої застосовуються для регулювання роботи інженерних систем і комунікацій будівель. Існує кілька типів даних датчиків:

- датчики температури;
- датчики рівня освітленості;
- датчики витоку газу;
- датчики протікання води;
- протипожежні датчики (датчики задимлення, датчики температури);
- датчики тиску води, газу;
- датчики дощу і атмосферних опадів;
- датчики - індикатори вогкості / вологості;
- комбіновані.

Всі типи цих датчиків знімають показання навколишнього середовища і передають інформацію про неї в систему «розумного будинку». Перераховані вище датчики можуть передавати цю інформацію по різних каналах зв'язку, за допомогою дротового або бездротового з'єднання, використовуючи різноманітні протоколи передачі інформації.

В цілому для всіх перерахованих типів датчиків характерні уразливості, пов'язані з обмеженням конструкції датчиків, що використовуються фізичними принципами, невірної установкою.

Уразливості проявляється в зв'язку з впливом наступних факторів:

- електромагнітного випромінювання;
- електричного шуму
- акустичні перешкоди;
- перепади освітленості;
- перепади вологості;
- наявність в повітрі хімічних речовин;
- наявність в повітрі пилу і суспензій;
- екранування поля, випромінюваного активними датчикам і об'єктами в зоні виявлення.

Серед перерахованих загроз відсутні в явному вигляді загрози інформаційній безпеці. Проте, захист розглянутих датчиків в зв'язку з виділеними уразливими необхідна, оскільки загроза імітації помилкових спрацьовувань є закономірним наслідком реалізації розглянутих вразливостей і являє собою спосіб впровадження в ІТ-систему «розумного будинку» помилковою або зловмисно-спотвореної інформації. Внаслідок цього при розробці та впровадження прикладного та програмно-апаратних засобів в рамках ІТ-систем «розумного будинку» слід передбачити програмні процедури перевірки працездатності і режиму функціонування датчиків і реалізувати механізм верифікації оброблюваних показань згідно вимог ГОСТ Р МЕК 61508-3 -2007 «Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних з безпекою. Частина 3. Вимоги до програмного забезпечення ». Відповідно до даної завданням в план верифікації згідно п. 7.9.2 ГОСТ Р МЕК 61508-3-2007 потрібно внести положення, що стосуються перевірки достовірності оброблюваних показань для розробленої моделі інформаційної безпеки. Зокрема, згідно з п. 7.9.2. 13 ГОСТ Р МЕК 61508-3-2007 структури даних, специфіковані під час проектування, повинні бути перевірені на захист від зміни або пошкодження [11].

Всі параметри ІТ-системи, які пов'язані з обробкою показань датчиків, які можуть бути змінені, повинні бути перевірені на захист:

- від помилкових, несумісних або необґрунтованих значень;
- несанкціонованих змін;
- пошкодження даних.

2.2 Аналіз вразливостей і факторів, що впливають на виконавчі пристрої «розумного будинку»

Виконавчі пристрої призначені для перетворення керуючих (командних) сигналів в регулюючі дії на об'єкт управління. Сигнальна сирена, сервоприводи перекривають подачу води або газу, що відкривають вентиляційні вікна, різні

силові реле і таймери - відносяться до виконавчих пристроїв. Розглянемо кілька з цих пристроїв докладніше в контексті аналізу загроз «розумному будинку».

Електромагнітні клапани (рис. 2.5) встановлюються на трубопроводах подачі води і газу для дистанційного керування відкриттям або закриттям потоку робочого середовища, як правило, рідини.

Рисунок 2.5 – Загальний вигляд електромагнітного клапана «Гідролок WINNER»

Варіанти застосування електромагнітних клапанів:

1) в якості аварійного крана в системі подачі води. У цьому випадку управління здійснюється від датчика, вмонтованого в підлогу і спрацьовує від попадання води;

2) в системі клімат-контролю електронний (електромагнітний) кран буде регулювати подачу гарячої води, в залежності від температури в кімнаті (керуючий сигнал подається від датчика температури в приміщенні);

3) електромагнітний клапан може використовуватися в системі поливу присадибної ділянки. Подача води буде здійснюватися відповідно до встановленого тимчасовим графіком або від сигналу датчика вологості;

4) також існують електромагнітні клапани для установки на трубопроводах подачі газу. Такий клапан, підключений до датчика загазованості, перекриє подачу газу і при аварійній ситуації.

Вразливістю є можливість виведення датчика з ладу шляхом впливу зовнішнім електромагнітним випромінюванням.

Електромеханічні приводи відкриття / закриття воріт, хвірток, дверей (рис 2.6), вікон, жалюзі і штор тощо.

Рисунок 2.6 – Загальний вигляд електромагнітного замка компанії Samsung

Робота приводів може здійснюватися за сценарієм, наприклад, вночі - закриття жалюзі і приглушення світла; при постановці на сигналізацію - закриття всіх вікно і дверей, включення датчиків руху.

Вразливістю приводу є недостатній захист від механічних пошкоджень. Також вразливість таких приводів істотно зростає при відключенні напруги електроживлення.

2.3 Аналіз вразливостей і факторів, що впливають на безпеку центральних пристроїв «розумного будинку»

Центральний пристрій «розумного будинку» координує всі його функції і керує всіма його компонентами. Як обчислювальної платформи центрального пристрою можуть виступати: персональні комп'ютери, ноутбуки, сервери, але найбільш часто використовуються контролери різних типів. Завдання контролера

полягає в зборі інформації про функціонування обладнання, перевірці отриманих параметрів, пошук аварійно-функціонуючих пристроїв і висновок обробленої інформації на панелі управління. Сьогодні на ринку представлена велика кількість контролерів для «розумного будинку» від різних фірм виробників, нижче розглядаються типові контролери та їх вразливості. датчик інтелектуальний розумний будинок [13].

Контролер виробництва фірми AMX NX-1200 (рис. 2.7) створений для вирішення завдань управління і автоматизації невеликих систем «розумного будинку», цей контролер обладнаний дев'ятьма портами управління для підключення до чотирьох пристроїв у вигляді, наприклад, інфрачервоних датчиків (ІК) і одного послідовного пристрою сторонніх виробників, а також може підтримувати шину типу Ethernet.

Рисунок 2.7 – Загальний вигляд контролера AMX NX-1200

Уразливість даного контролера була виявлена експериментальним шляхом в ході перевірки процедури аутентифікації: дослідники виявили у внутрішній базі даних користувачів приховану адміністративну обліковий запис, для якої були задані незмінний логін і пароль. Отримавши доступ до цього облікового запису можна отримати контроль над пристроєм оскільки даний адміністративний акаунт дозволяє отримати доступ до web-консолі управління, а також інтерфейсу командного рядка і здійснювати різні дії, наприклад, перехоплення і підміну трафіку.

Інший типовий зразок, контролер фірми X10 MT10 (рис. 2.8), використовується для управління по часу електропобутовими та освітлювальними приладами в мережі X10, підключається по електропроводці.

Рисунок 2.8 – Загальний вигляд контролера X10 MT10

Можливі такі режими роботи приладу:

- автоматичний режим - контролер вмикає і вимикає електроприлади по заздалегідь введеної програми;
- ручний режим - в будь-який момент можливо безпосереднім натисканням кнопок на приладі управляти підключеними електроприладами;
- режим безпеки (імітація присутності господарів в будинку) - автоматичний режим з довільними моментами включення і виключення електроприладів в межах встановленого інтервалу часу.

Контролер вразливий при електромагнітних перешкодах або розриві зовнішньої електропроводки, пропажі електроживлення.

Контролер фірми Honeywell Tuxedo Touch (рис. 2.9) забезпечує централізоване управління освітленням, термостатом, замками, камерами, і т.п. використовуючи бездротову технологію Z-Wawe.

Рисунок 2.9 – Контролер Honeywell Tuxedo Touch

У контролера є ряд вразливостей, які суттєво впливають на безпеку використання, в тому числі обхід аутентифікації користувача і підміна міжсайтових запитів.

Як видно з перерахованих вище прикладів, центральні контролери «розумного будинку» схильні до різних видів вразливостей, реалізація яких може призвести до виведення з ладу фрагмента або всієї системи в цілому [14].

2.4 Аналіз вразливостей і факторів, що впливають на систему зв'язку «розумного будинку».

В даний час з усіх представлених на ринку технологій побудови IT-систем «розумний дім», можна виділити кілька готових до застосування комплексних систем, які є типовими представниками в своєму класі:

- централізовані, наприклад, системи фірми Creston;
- децентралізовані системи, наприклад, EIB.

Також системи можна класифікувати на:

- провідні, наприклад, X10;
- бездротові, наприклад, Z-Wave.

На прикладі цих комплексних систем розглянемо основні фактори, що впливають на безпеку інформації, що захищається «розумного будинку», побудованого на основі готових систем.

Зазначені фактори поділяються на:

1) за ознакою ставлення до природи виникнення:

- об'єктивні;
- суб'єктивні.

2) по відношенню до об'єкта інформації:

- внутрішні;
- зовнішні.

Система управління будинком фірми Crestron - це централізована система управління. Як правило, вона будується на основі застосування широкого спектра керуючих центральних контролерів і безлічі виконавчо-командних блоків. Керуючі контролери Crestron володіють великим набором вбудованих можливостей, сумісні з безліччю поширених протоколів передачі інформації [8].

Для даної системи фактори, що впливають на безпеку інформації, що захищається, представлені в табл. 2.1 і табл. 2.2.

Таблиця 2.1 – Об'єктивні чинники, що впливають на безпеку інформації, що захищається централізованої системи управління «розумним будинком».

Внутрішні чинники	**Зовнішні чинники**
Випромінювання акустичних сигналів супутні виголошуваної технічним засобом (ТЗ) мови	Збої, відмови і аварії систем забезпечення об'єкта інформації (ОІ)
Модуляція паразитного електромагнітного випромінювання інформаційними сигналами	Термічні фактори (пожежі і т.д.)
Дефекти, збої і відмови, аварії ТС і систем обробки інформації	Кліматичні чинники (повені і т.д.)

Таблиця 2.2 – Суб'єктивні чинники, що впливають на безпеку інформації, що захищається централізованої системи управління будинком.

Внутрішні чинники	**Зовнішні чинники**
Розголошення інформації, що захищається особами, які мають до неї право доступу через передачу інформації за відкритими лініях зв'язку	Доступ до інформації, що захищається з застосуванням ТС знімання інформації
Несанкціонований доступ до інформації шляхом підключення до технічних засобів і систем ОІ	Несанкціонований доступ до інформації, що захищається шляхом використання закладних засобів
Використання програмного забезпечення (ПО) технічних засобів ОІ через внесення програмних закладок	Блокування доступу до інформації, що захищається шляхом перевантаження ТС обробки інформації помилковими заявками на її обробку

Система управління будинком EIB (European Installation Bus) - це децентралізована відкрита мережева технологія, підтримана десятками провідних компаній виробників електротехнічної продукції - членів європейської неурядової організації EIBA (European Installation Bus Association (рис. 2.10).

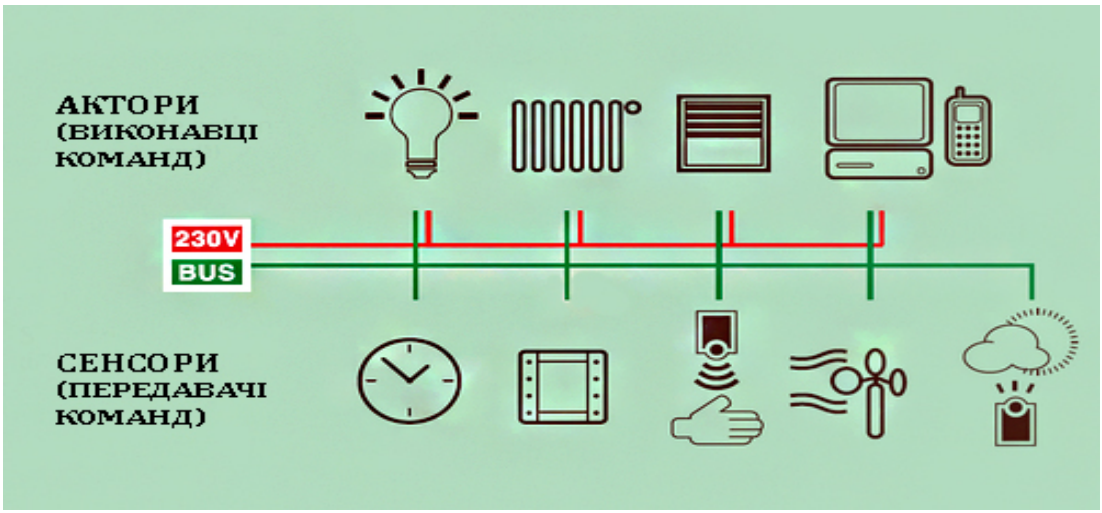

Рисунок 2.10 – Загальна схема підключення системи EIB

Пристрої (передавачі або приймачі) в EIB зв'язуються один з одним безпосередньо, без ієрархії або центрального контролюючого приладу. Компоненти здійснюють передачу послідовно, асинхронно, конфлікти при

передачі повідомлень вирішуються розстановкою пріоритетів повідомлень. Призначена для передачі інформація збирається в пакети- «телеграми» і через шину передається приймачу або групі приймачів. Повідомлення отримують всі абоненти, але реагують на нього тільки ті, кому воно адресоване. Сьогодні EIB-протокол підтримує обмін по кручений парі, безпосередньо по силової лінії, по радіо і по ІЧ-каналу. До децентралізованим системам також відносяться такі готові системи, як Gira, Berker, Bticino, Vimar і ін.

Для систем з децентралізованим управлінням фактори, що впливають на безпеку інформації, що захищається, представлені в табл. 2.3 і табл. 2.4.

Таблиця 2.3 – Об'єктивні чинники, що впливають на безпеку інформації децентралізованої системи управління «розумним будинком»

Внутрішні чинники	**Зовнішні чинники**
Дефекти, збої і відмови ПО	Збій, відмови і аварії систем забезпечення ОІ
Наведення в лініях зв'язку, викликані побічними електромагнітними випромінюваннями, що несуть інформацію	Термічні фактори (пожежі і т.д.)
Наявність акустоелектричних перетворювачів в елементах ТС ОІ	Кліматичні чинники (повені і т.д.)

Таблиця 2.4 – Суб'єктивні чинники, що впливають на безпеку інформації децентралізованої системи управління «розумним будинком»

Внутрішні чинники	**Зовнішні чинники**
Неправомірні дії з боку осіб, які мають право доступу до інформації, що захищається, шляхом несанкціонованого зміни інформації.	Доступ до інформації, що захищається з застосуванням ТС технічної комп'ютерної розвідки.

Продовження таблиці 2.4 – Суб'єктивні чинники, що впливають на безпеку інформації децентралізованої системи управління «розумним будинком»

Недоліки організаційного забезпечення захисту інформації при завданні вимог щодо захисту інформації.	Спотворення, знищення або блокування інформації шляхом розкрадання носія інформації.
Несанкціонований доступ до інформації шляхом внесення програмних закладок.	Спотворення, знищення або блокування інформації шляхом використання програмних або програмно-апаратних засобів при здійсненні мережевої атаки.

Система управління будинком X-10 - міжнародний відкритий промисловий стандарт, застосовуваний для зв'язку електронних пристроїв в системах домашньої автоматизації. Стандарт X10 визначає методи і протокол передачі сигналів управління електронними модулями, до яких підключені побутові прилади, з використанням звичайної електропроводки або бездротових каналів [9]. Мережа X10 включає в собі наступні основні компоненти: передавачі, приймачі, трансивери, пульти дистанційного керування та лінійні компоненти. Системам використовують провідні технології побудови системи «розумний дім» (зокрема стандарт X10) притаманні фактори, що впливають на безпеку інформації, що захищається представлені в табл. 2.5 і табл. 2.6.

Таблиця 2.5 – Об'єктивні чинники, що впливають на безпеку інформації, що захищається провідної системи управління «розумним будинком»

Внутрішні чинники	**Зовнішні чинники**
Модуляція паразитного електромагнітного випромінювання інформаційними сигналами	Ненавмисні електромагнітні опромінення ОІ

Продовження таблиці 2.5 – Об'єктивні чинники, що впливають на безпеку інформації, що захищається провідної системи управління «розумним будинком»

Наведення в електричних ланцюгах ТС викликана побічними електромагнітними випромінюваннями, що несуть інформацію	Електромагнітні фактори (грозові розряди і т.д.)
Наведення в ланцюгах заземлення викликана побічними електромагнітними випромінюваннями, що несуть інформацію	Кліматичні чинники (повені і т.д.)

Таблиця 2.6 – Суб'єктивні чинники, що впливають на безпеку інформації, що захищається провідної системи управління «розумним будинком»

Внутрішні чинники	**Зовнішні чинники**
Розголошення інформації, що захищається особами, які мають до неї право доступу через осіб, які не мають права доступу до інформації, що захищається	Доступ до інформації, що захищається з застосуванням ТС радіоелектронної розвідки
Несанкціонований доступ до інформації шляхом порушення функціонування ТС обробки інформації	Спотворення, знищення або блокування інформації шляхом навмисного електромагнітного впливу по мережі електроживлення
Помилки користувачів або обслуговуючого персоналу при експлуатації ТЗ	Спотворення, знищення або блокування інформації шляхом навмисного силового впливу фізичної природи

Система управління будинком Z-Wave є запатентованим бездротовим протоколом зв'язку, розробленим для домашньої автоматизації, зокрема для контролю і управління в житлових і комерційних об'єктах. Технологія використовує малопотужні і мініатюрні радіочастотні модулі, які вбудовуються в побутову електроніку і різні пристрої, такі як освітлювальні прилади, прилади опалення, пристрої контролю доступу, розважальні системи і побутову техніку. Більшість систем використовують бездротові канали зв'язку схильні до факторів, що впливають на безпеку інформації.

Таблиця 2.7 – Об'єктивні чинники, що впливають на безпеку інформації, що захищають бездротові системи управління «розумним будинком»

Внутрішні чинники	**Зовнішні чинники**
Електромагнітні випромінювання і поля в радіодіапазоні	Ненавмисні електромагнітні опромінення ОІ
Побічні електромагнітні випромінювання на частотах роботи високочастотних генераторів пристроїв, що входять до складу ТС ОПИ	Радіаційні опромінення ОІ
Побічні електромагнітні випромінювання на частотах самозбудження підсилювачів пристроїв, що входять до складу ТС ОПИ	Природні явища, стихійні лиха

Таблиця 2.8 – Суб'єктивні чинники, що впливають на безпеку інформації, що захищається бездротової системи управління «розумним будинком»

Внутрішні чинники	**Зовнішні чинники**
Несанкціонований доступ до інформації шляхом підключення до ТЗ і системам ОІ	Доступ до інформації, що захищається з застосуванням ТС радіоелектронної розвідки

Продовження таблиці 2.8 – Суб'єктивні чинники, що впливають на безпеку інформації, що захищається бездротової системи управління «розумним будинком»

Розголошення інформації, що захищається особам, які не мають до неї право доступу	Доступ до інформації, що захищається шляхом використання шкідливого ПО
Помилки обслуговуючого персоналу при експлуатації ТЗ	Спотворення, знищення або блокування інформації шляхом здійснення мережевої атаки

Таким чином розроблена система суб'єктивних і об'єктивних факторів, що впливають на систему «розумного будинку». Надалі ця система буде використана для аналізу загроз «розумного будинку».

3 АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ «РОЗУМНОГО БУДИНКУ»

3.1 Загрози конфіденційності, цілісності та доступності інформації ІТ-системи «розумного будинку»

Під загрозою безпеки інформації (УБІ) будемо розуміти сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації. Під вразливістю розуміється властивість інформаційної системи, що обумовлює можливість реалізації загроз безпеки оброблюваної в ній інформації.

Базовими загрозами інформаційній безпеці «розумного будинку» є:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності інформації (всі разом КЦД).

У контексті аналізу «розумного будинку» під конфіденційністю мається на увазі такий стан ІТ-системи управління «розумним будинком», при якому відсутня можливість витоку інформації через підсистеми. Приклад реалізації загрози - витік персональної інформації або витік інформації про конфігурацію ІТ-систем «розумного будинку».

Цілісність інформації - це достовірність і повнота інформації отримується системою від різних датчиків і пристроїв, встановлених в системі, наприклад, при отримання невірної інформації системою про наявність в приміщенні людини може привести до помилкового спрацьовування системи контролю доступу [10].

Доступність інформації стосовно «розумному будинку» - це стан інформації або ресурсів ІТ-системи, при якому суб'єкти або сама система, що мають права доступу, можуть реалізувати різні дії відповідно до сценарію роботи (вимикати / включати датчики, відкривати замки і т.д .). Приклад реалізації даної загрози - виведення з ладу комунікаційного обладнання системи.

Загрози інформаційної безпеки за своєю природою виникнення можна розділити на 2 групи: загрози, зумовлені людським фактором і загрози середовища (природні).

Зокрема, загрози першої групи розрізняються за способом здійснення: цілеспрямовані (навмисні) і випадкові (ненавмисні). Деякі приклади таких загроз наведені в табл. 3.1, варто відзначити, що загрози другої групи (загрози середовища), не піддаються прогнозуванню, і як правило, під ними мають на увазі природні катаклізми.

Таблиця 3.1 – Класифікація загроз безпеки інформації IT-системи «розумного будинку»

Загрози, обумовлені людським фактором		**Загрози середовища**
Цілеспрямовані	**Випадкові**	
Модифікація інформації	Помилки ПО	Пожежа
Перехоплення інформації	Помилки користувача	Затоплення
Розкрадання обладнання	Помилки при обслуговуванні	Блискавка
Хакерська атака	Апаратні відмови	Землетрус
Шкідливе програмне забезпечення (ПО)	Помилки маршрутизації	Екстремальні величини температури і вологості

Іншим суттєвим фактором для визначення загроз інформаційної безпеки є ідентифікація можливих джерел загроз в залежності від їх розташування: внутрішні і зовнішні. До внутрішніх загроз відносяться загрози, розташовані всередині контрольованої зони, до зовнішніх - зовні (табл. 3.2). Більш повний список загроз можна подивитися на сайті бази даних загроз безпеки інформації.

Таблиця 3.2 – Приклади внутрішніх і зовнішніх загроз інформації ІТ-системи «розумного будинку»

Внутрішні загрози	**Зовнішні загрози**
Загроза застосування коду або даних	Загроза відключення (екранування) контрольних датчиків
Загроза використання механізмів розробника	Загроза спотворення вводиться і виводиться на периферійні пристрої інформації
Загроза підміни програмного забезпечення	Загроза несанкціонованого віддаленого внеполосного доступу до апаратних засобів
Загроза доступу / перехоплення / зміни HTTP- cookies	Загроза подолання фізичного захисту
Загроза доступу до локальних файлів сервера за допомогою URL	Загроза межсайтовой підробки запиту

3.2 Оцінювання ризиків інформаційної безпеки «розумного будинку»

Загрози інформаційної безпеки ІТ-системи «розумний дім» в першу чергу залежать від обраних способів і технологій побудови даної системи, так як на визначення можливих загроз впливає склад обладнання. Для оцінки ризиків інформаційної безпеки «розумного будинку» розглянемо найбільш ймовірні загрози, реалізація яких може призвести до порушення інформаційної безпеки «розумного будинку» побудованого з централізованого технології [18].

Далі виявлені загрози зіставляються з уразливими, і визначається, які властивості активу (конфіденційність – К, цілісність – Ц, доступність – Д) можуть порушувати ті чи інші загрози (табл. 3.3).

Таблиця 3.3 – Загрози і уразливості безпеки «розумного будинку»

№	Загроза	Уразливість	Властивості, які загроза може порушити		
			К	Ц	Д
1	Атаки на центральний сервер	Підключення мережі «розумного будинку» до Інтернету. Недостатня ефективність захисту мережі «розумного будинку»	+	+	+
2	Впровадження шкідливого коду або програми	Підключення мережі «розумного будинку» до Інтернету. Відсутність (недостатня ефективність) механізмів захисту трафіку	+	+	+
3	Перехоплення і підміна переданого сигналу	Можливість доступу зловмисника до мереж передачі інформації. Відсутність (недостатня ефективність) механізмів захисту трафіку	+	+	
4	Доступ до мережі нелегітимних користувачів	Відсутність (недостатня ефективність) механізмів аутентифікації і ідентифікації	+		

Продовження таблиці 3.3 – Загрози і уразливості безпеки «розумного будинку»

5	Використання механізмів розробника	Відсутність (недостатня ефективність) механізмів аутентифікації і ідентифікації	+	+	
6	Тривале утримання обчислювальних ресурсів користувачами	Слабкі механізми балансування навантаження і розподілу обчислювальних ресурсів			+
7	Доступ до захищених файлів з використанням обхідного шляху	Слабкості механізму розмежування доступу	+	+	
8	Відключення контрольних датчиків	Відсутність (недостатня ефективність) системи контролю доступу			+
9	Подолання фізичного захисту об'єкта	Уразливості в системі контролю фізичного доступу	+		+
10	Крадіжка апаратури чи носіїв інформації	Незахищене зберігання	+	+	+

Продовження таблиці 3.3 – Загрози і уразливості безпеки «розумного будинку»

11	Крадіжка апаратури чи носіїв інформації	Отсутствие (недостаточная эффективность) системы физической охраны объекта		+	+
12	Знищення апаратури або носіїв інформації	Відсутність системи автономного електроживлення. Чутливість до перепадів напруги			+
13	Помилки користувача	Відсутність механізмів моніторингу. Складний призначений для користувача інтерфейс		+	+
14	Помилки ПО	Використання неліцензійного ПЗ.			+
15	Стихійні лиха	Відсутність (недостатня ефективність) системи фізичної охорони об'єкта		+	+

Для оцінювання ризиків скористаємося методикою оцінки ризиків корпорації «Microsoft». Для цього складемо зведену таблицю, в якій оцінимо:

– ймовірність реалізації загрози виходячи з частоти її реалізації за певний період, де висока - ймовірність реалізації однієї або декількох загроз в межах року, середня - виникнення загрози в межах 2-3 років, і низька - поява загрози протягом 3 років малоймовірно;
– рівень схильності впливу, за наступною шкалою: високий - значний або повний збиток для активу, середній - середній або обмежений збиток, низький - незначний збиток (відсутність);

Таблиця 3.4 – Визначення рівня впливу

Клас активу	Високий вплив (ВВ)	Середній	Високий	Високий
	Середнє вплив (СВ)	Низький	Середній	Високий
	Низький вплив (НВ)	Низький	Низький	Середній
		Низький	Середній	Високий
		Рівень схильності впливу		

Підсумковий рівень ризику визначається відповідно до табл. 3.5.

Таблиця 3.5 – Визначення підсумкового ризику

Вплив (див. Табл. 3.4)	Високий	Середній	Високий	Високий
	Середній	Низький	Середній	Високий
	Низький	Низький	Низький	Середній
		Низький	Середній	Високий
		Рівень ймовірності реалізації загрози		

– клас активу відповідно до табл. 3.4, де високий вплив – вплив на КЦД інформації завдає значної або фатальний шкоди для організації (власникам), середній – середній або обмежений збиток, низький – незначний збиток або його відсутність [19].

В результаті отримаємо таблицю для якісної оцінки рівня ризиків системи «розумний дім» (табл. 3.6).

Таблиця 3.6 – Рівень ризику для загроз «розумного будинку»

№	Загроза	Імовірність реалізації	Рівень схильності впливу	Клас активу	Рівень ризику
1	Атаки на центральний сервер	Висока	Високий	Високий	Високий

Продовження таблиці 3.6 – Рівень ризику для загроз «розумного будинку»

2	Впровадження шкідливого коду або програми	Висока	Високий	Високий	Високий
3	Перехоплення і підміна переданого сигналу	Висока	Середній	Середній	Високий
4	Доступ до мережі нелегітимних користувачів	Висока	Середній	Середній	Середній
5	Використання механізмів розробника	Висока	Високий	Середній	Високий
6	Тривале утримання обчислювальних ресурсів користувачами	Висока	Середній	Низький	Середній
7	Доступ до захищених файлів з використанням обхідного шляху	Середня	Середній	Середній	Середній
8	Відключення контрольних датчиків	Висока	Середній	Середній	Високий
9	Подолання фізичного захисту об'єкта	Середня	Високий	Високий	Високий
10	Крадіжка апаратури або носіїв інформації	Низька	Високий	Високий	Середній

Продовження таблиці 3.6 – Рівень ризику для загроз «розумного будинку»

11	Знищення апаратури або носіїв інформації	Низька	Високий	Високий	Середній
12	Несправності в системі електропостачання	Середня	Середній	Середній	Середній
13	Помилки користувача	Середня	Середній	Середній	Середній
14	Помилки ПО	Середня	Середній	Середній	Середній
15	Стихійні лиха	Низька	Високий	Високий	Середній

Ґрунтуючись на результатах оцінки ризиків, найбільш небезпечними загрозами є:

- атаки на центральний сервер;
- впровадження шкідливого коду або програми;
- перехоплення і підміна переданого сигналу;
- використання механізмів розробника;
- відключення контрольних датчиків;
- подолання фізичного захисту об'єкта.

Також небезпечними є ризики, пов'язані з несправністю в роботі систем електроживлення і помилками користувача і / або ПЗ.

У зв'язку з цим необхідно застосувати такі захисні заходи, для зниження ризиків, пов'язаних з реалізацією даних загроз:

1) застосування механізмів ідентифікації і аутентифікації користувачів;

2) застосування механізмів шифрування і контролю цілісності переданих даних;

3) використання антивірусного ПО;

4) організація системи контролю управління доступом;

5) використання механізмів розподілу навантажень;

6) періодична перевірка працездатності всіх елементів систем;

7) використання резервного джерела живлення.

3.4 Аналіз протоколів передавання даних для впровадження безпечних автоматизованих систем «розумного будинку»

Для подібного критичного механізму безпеки необхідно знайти протокол передачі інформації, який би відповідав критеріям забезпечення конфіденційності, цілісності і доступності даних, важливим пунктом буде спосіб спілкування з іншими структурними елементами житлового приміщення: розвиток систем «розумний дім» і бездротових модулів домашньої автоматизації призвело до часткової уніфікації даного сегмента і є можливість використання загальної мережевої інфраструктури.

Однак, незважаючи на розвиток і поступову офіційну і неофіційну стандартизацію технологій сегмента «розумний будинок» і будь-якої домашньої автоматизації, залишається проблема вибору протоколів передачі інформації між керованими пристроями, датчиками і іншими елементами приміщень. Особливо гостро стоїть проблема, коли необхідно забезпечити конфіденційність і цілісність циркулюючих даних.

Метою дослідження є пошук захищеного мережевого протоколу, що дозволяє при його використанні в пристроях автоматичного сигналізування виключити вплив на конфіденційність, цілісність інформації без використання спеціальних програмно-апаратних рішень. Також необхідно забезпечити доступність даних пристроїв шляхом можливості вести автономну роботу. Основні захищені протоколи можна умовно розділити на два великі класи: застосовні при дротових рішеннях (наприклад, IPsec, SSL, TLS); застосовні при створення бездротових систем (ZigBee, Z-Wave, Thread, WeMo). У житлових приміщеннях застосовуються різні пристрої і технології, які, як правило, є надбудовою до вже існуючої інфраструктури, тому основним напрямком аналізу є бездротові протоколи, що дозволяють зручно реалізувати мережеве взаємодія. Провідні рішення варто розглядати тільки в умовах впровадження домашньої

автоматизації на ранніх етапах будівництва окремих приміщень або квартир, а також при проектуванні критичних елементів системи [20]. При використанні бездротових протоколів і пристроїв постає питання їх можливості забезпечити належний рівень конфіденційності і цілісності даних. Це пов'язано впливом на вже існуючі бездротові мережі в зоні застосування, поширеність протоколу зв'язку, можливість перехоплення сигналу з його подальшим аналізом або атакою. Також є додаткові вимоги щодо забезпечення доступності даних в «розумному будинку» і здатності вести автономну роботу.

Розглянемо чотири основних бездротових технології, за допомогою яких можна реалізувати систему автоматизації в захищеному виконанні. В якості порівняльних характеристик будемо досліджувати:

1) Шифрування даних: наявність і надійність технології для створення конфіденційного каналу передачі даних. Можливість використання в якості основної або додаткової можливості.

2) Топологія мережі: можливі варіанти підключення пристроїв в мережу.

3) Забезпечення доступності та автономності: наявність додаткових алгоритмів самоорганізації мережі і самовідновлення.

4) Швидкість передачі даних: висока пропускна здатність для забезпечення швидкого відгуку між запитом на дію і його виконанням, а також запасом ресурсу при завантаженні каналів передачі даних.

В першу чергу розглянемо шифрування. Для створення захищеної передачі даних, дана характеристика буде ключовою. Всі протоколи використовують шифрування, проте воно дуже сильно різниться. Якщо порівнювати Zig-Bee і Z-Wave, то вони обидва використовують AES-128, ключовою відмінністю Z-Wave є можливість використання даної технології тільки на відведених вузлах системи, а не повсюдно, як це реалізовано у Zig-Bee. Threadиспользует сучасні протоколи на основі еліптичних кривих, для яких ще не знайдено субекспоненціальное алгоритмів рішення. WeMов даному випадку суперечливий, його можливості шифрування цілком і повністю залежать від можливостей маршрутизатора, це TKIP / AES шифрування. З точки зору доступності та можливостей серед

перерахованих алгоритмів необхідно використовувати Zig-Bee. У подальшому майбутньому протокол Threadімеет шанси замінити Zig-Bee, за умови, що збережеться швидкість шифрування. Також якщо порівняти алгоритми AES (Zig-Bee, WPA2, ZWave) і связку J-PAKE + NISTP-256 на рисунку 3.1 , то можна переконатися в ефективності алгоритму AES для швидкої передачі великих обсягів даних. Однак на практиці все алгоритми прагнуть використовувати команди невеликої довжини, тому критерій швидкості буде помітний лише при використанні протоколів для нестандартних ситуацій. пристроїв шляхом можливості вести автономну роботу.

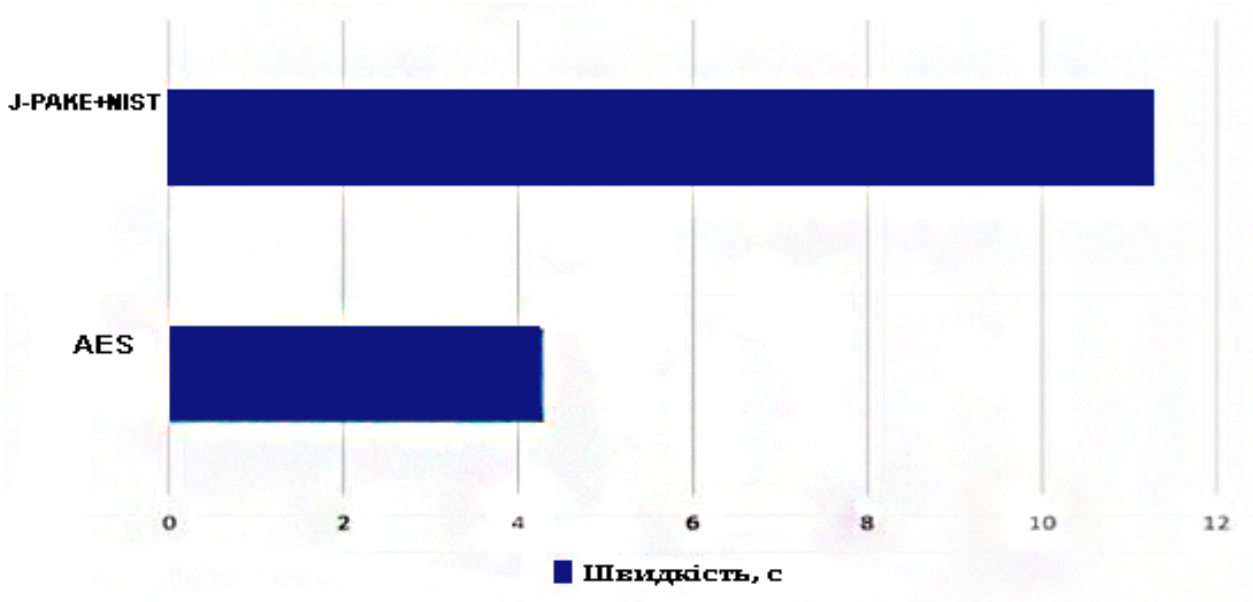

Рисунок 3.1 – Порівняння швидкості шифрування протоколів AES і зв'язки NISTP-256 + J-PAKE на прикладі кількох тестів (Менше, краще).

З точки зору створюваної топології мережі, існує два основні варіанти в пропонованих протоколах. Перший - мережа типу «зірка», є деяка центральне пристрій, який виступає в ролі єднальної ланки. Легко розгорнути, проте є наслідки у вигляді порушення доступності, при виході центрального блоку з ладу. Подібну мережу можуть розгорнути протоколи WeMo і Zig-Bee. Другий тип - чарункова, децентралізована мережа. Zig-Bee, Z-Wavei Thread підтримують цю технологію, останні два використовують як єдино можливу. Дана мережа, в силу своєї децентралізованість підвищує показники доступності всієї мережі.

Доступність є другим важливим критерієм для організації захищеного «Розумного будинку». Якщо в потрібний момент не будуть передані дані з датчиків руху, датчиків пожежі та інших, можуть статися різні надзвичайні ситуації. Протокол WeMo повністю залежить від маршрутизатора, тому в разі його відмови не має можливості забезпечення автономної роботи пристроїв «розумного будинку. Якщо розглядати Z-Wave, даний протокол зберігає працездатність при відсутності основного джерела електроживлення. Zig-Beei Thread крім харчування від акумуляторів мають алгоритми самоорганізації і самовідновлення мережі, що дозволяє зберігати доступність даних інфраструктури приміщень, в умовах недоступності окремих її вузлів [13].

Швидкість передачі даних протоколів, що працюють на малопотужних частотах, які не є їх сильною стороною, проте для передачі базових команд їх ресурсів більш ніж досить. В даному критерії виділяється лише WeMo, швидкість передачі даних в якому залежить від пропускної можливості маршрутизатора. Окремо необхідно відзначити питання про заміну захищених бездротових протоколів на російські аналоги. Незважаючи на те, що є особливі протоколи передачі інформації, що використовуються в АСУ ТП (наприклад, ОВЕН) або бездротова технологія MeshLogic, технічні особливості не дозволяють їх правильно застосовувати в системах домашньої автоматизації в поточному вигляді. Об'єднавши дані разом, ми отримаємо зведену таблицю.

Таким чином, з точки зору основних характеристик найбільше підходить технологія Zig-Bee, він максимально закриває проблеми забезпечення конфіденційності, цілісності і доступності даних в системах з автоматичним сигналізування. Протокол Thread використовує більш сучасні технології, проте недавній випуск основних специфікацій і відсутність додаткової інформації про застосовуваних пристроях не дозволяє говорити про нього, як про повноцінну заміну Zig-Bee, можливо лише в найближчому майбутньому. Протокол WeMo не підходить для створення захищених систем «розумний дім».

ВИСНОВКИ

Мета цієї дипломної роботи полягала в дослідженні захищеності IT-систем «розумного будинку» шляхом виявлення загроз і вразливостей інформаційної безпеки.

Основою системи «розумний дім» є телекомунікаційна (комп'ютерна) мережа, тому загрози інформаційної безпеки в першу чергу можуть виникати за рахунок вразливостей мережевої структури: коди операційної системи (наприклад, вразливість при переповненні пам'яті, управління оновленнями операційної системи); транспортні протоколи, наприклад, протокол TCP, DNS, SMTP або ICMP; дефекти прикладних програм (firmware, наприклад, Apache); помилки в програмах користувача; програмне забезпечення, вбудоване в апаратні пристрої, наприклад, в маршрутизатори, BIOS; перехоплення повідомлень і управління в бездротових системах.

Для зниження ризиків, пов'язаних з реалізацією даних загроз, необхідно застосувати такі захисні заходи: застосування механізмів ідентифікації і аутентифікації користувачів, застосування механізмів шифрування і контролю цілісності переданих даних, використання антивірусного ПО, організація системи контролю управління доступом, використання механізмів розподілу навантажень, періодична перевірка працездатності всіх елементів систем, використання резервного джерела живлення.

Також, в ході роботи було з’ясовано, що найбільше підходить технологія Zig-Bee, вона максимально закриває проблеми забезпечення конфіденційності, цілісності і доступності даних в системах з автоматичним сигналізування. Протокол Thread використовує більш сучасні технології, проте недавній випуск основних специфікацій і відсутність додаткової інформації про застосовуваних пристроях не дозволяє говорити про нього, як про повноцінну заміну Zig-Bee, можливо лише в найближчому майбутньому. Протокол WeMo не підходить для створення захищених систем «розумний дім».

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Michael S., Ulf L., 7 Smart-Home-Starter-Kits imSicherheits-Test // AV-TEST-Studie. 2014. pp. 16-41.

2. Yang, L. (2012) Design of Monitoring and Controlling System of Smart Home based on ZigBee. Master’s Thesis, Beijing Jiaotong University, Beijing.

3. Ruan, X. (2010) Analysis and Comparison of Several Smart Home Wireless Networking Technology. Science & Technology Information, 27, 39-42.

4. Liu, Y. Study on smart home system based on internet of things technology. In Informatics and Management Science IV; Du, W., Ed.; Springer: London, UK, 2013; Volume 207, pp. 73–81.

5. Mendes, T.D.P.; Godina, R.; Rodrigues, E.M.G.; Matias, J.C.O.; Catalao, J.P.S. Smart home communicationtechnologies and applications: Wireless protocol assessment for homearea network resources. Energies 2015, 8, 7279.

6. IEEE. IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs); Technical Report; IEEE: New York, NY, USA, 2006.

7. Tompros, S.; Mouratidis, N.; Draaijer, M.; Foglar, A.; Hrasnica, H. Enabling applicability of energy saving applications on the appliances of the home environment. IEEE Netw. 2009, 23, 8–16. 30. Zadeh, L.A. The concept of a linguistic variable and its application to approximate reasoning—II. Inf. Sci. 1975, 301–357.

8. Adams, C. E. (2002). Home area network technologies. BT Technology Journal, 20(2), 53–72.

9. Valtchev, D., & Frankov, I., & ProSyst Software AG. (2002). Service Gateway Architecture for a Smart Home. IEEE Communications Magazine, 126–132.

10. F. Liu and H. Zhao, "The Design of WIFI-Based Smart Home Communication Hardware Adapter," 2015 Fifth International Conference on

Instrumentation and 55 Measurement, Computer, Communication and Control (IMCCC), Qinhuangdao, 2015, pp. 1193-1197.

11. H. Jiang, B. Liu and C. W. Chen, "Performance analysis for ZigBee under WiFi interference in smart home,"2017 IEEE International Conference on Communications (ICC), Paris, 2017, pp. 1-6.

12. Гололобов В.Н. «Умный дом» своими руками. М.: НТ Пресс, 2007. с. 9-12, SBN 5- 477-00484-3

13. Стариковский А.В. Исследование уязвимостей систем умного дома [Текст] /А.В. Стариковский, И.Ю. Жуков, Д.М. Михайлов, А.М. Толстая, Ф.В. Жорин, В.В. Макаров, А.Б. Вавренюк // Спецтехника и связь. 2012. №2. С. 55-57.

14. Mobile Marketer. (2020). Smart speaker ownership hit 60M US adults in 2019. URL: https://www.mobilemarketer.com/news/smart-speaker-ownership-hit-60m-us-adults-in-2019/570186/

15. Протоколи зв'язку для "розумного будинку" // Аналітичні огляди комп'ютерів. URL: https://www.ferra.ru (дата звернення 11.04.2020).

16. Спеціальні можливості системи "Розумний будинок". Електронний збірник статей переможців V Міжнародної науково-практичної конференції «EUROPEAN SCIENTIFIC CONFERENCE» 30 липня 2017р. в м Пенза. Електронний збірник МК-196 / Алімовнін С.Г., Мільчаков С.А., Сиротинина Н.Ю. // Наука і Просвітництво. - Пенза, 2017. URL: http://naukaip.ru (дата звернення 18.04.2020).

17. Розумний будинок: Розвиток і тенденції // Geektimes. URL: https://geektimes.ru (дата звернення 10.04.2020).

18. Протоколи «Інтернету речей»: основні відомості // Засоби і системи автоматизації. URL: https://www.rtsoft.ru (дата звернення 14.04.2020).

19. BelkinWeMoSystem. URL: http://www.theaustralian.com.au/life/personal-technology (дата звернення 16.04.2020).

20. Mario B.B., Candid W, Insecurity in the Internet of Things // SECURITY RESPONSE. 2015. pp. 9-14.

ДОДАТОК А
SUMMARY

The potential of home automation in the mass market has long been recognized, and finally today we see the beginning of a new era when many large operators, service providers and utilities are launching SmartHome programs. Smart home is one of the buzzwords of 2020, but what exactly does it mean? In a nutshell, a smart home means a home where certain items are connected to the Internet, otherwise known as Internet of Things (IoT) devices. This could be everything from light bulbs that you can turn on with your voice to smart security cameras that let you livestream your footage from a mobile application. When it comes to home security, smart home products include cameras, sensors, touch panels, video doorbells, and more.

There’s so much you can do with a smart home, from voice commands through Alexa or Google Assistant to automating actions, like having your thermostat dip when your security system is armed, meaning you’re not home. Ideally, smart home products make your life more convenient so you can focus on what matters— doing the things you love, which probably doesn’t include house work. This guide will tell you everything you need to know about a smart home: what it is, what it may include, and how you can get one for yourself.

In short, a smart home is any home that includes WiFi-connected devices. Otherwise known as Internet of Things or IoT devices, being connected to the Internet means that you’ll be able to control them through a mobile application on your phone. Many devices are also connected to voice assistants so you can control them through voice commands. Anyone can have a smart home, which can be anything from a small apartment with a smart speaker to a large house with automated devices built in.

Of course, no home is completely automated, but the industry is getting closer and closer to this point. With a diverse array of devices ranging from smart security systems to smart smoke detectors, there’s very few devices you can’t get an IoT version of.

IoT devices can connect to the Internet in a few different ways, with Wi-Fi being the most common. Cellular backup and landline backup is typically used with smart

security cameras and systems, while Z-Wave, ZigBee and Bluetooth are less commonly used.

Sometimes spelled Wi-Fi, WiFi is a wireless technology that allows IoT devices to connect to the web with super-fast speeds. Using radiofrequency technology, most connected devices use some form of WiFi to connect to your app. However, if it's an important device like a security motion sensor, you may want to add in cellular or landline backup in case the WiFi is faulty, which we also discuss below.

Bluetooth: it's what you use to connect your AirPods or your smart speaker to your car's radio. A wireless technology, Bluetooth works by using short-wavelength radio waves. It's most commonly used with car stereo systems, hands-free headsets, mouses, keyboards, printers, and gaming consoles, and it's less common in smart home security.

Z-Wave is the name of a wireless communications protocol that lets devices connect with each other and the app using low-energy radio waves. In 2019, there were over 26,000 products that worked with Z-Wave, making it an increasingly popular connectivity option.

Now, we're not buying smart home products just for the sake of it. Unlike regular products that aren't connected to the Internet, smart devices have many capabilities and are all controllable through an app. Here are some of the things you can do with IoT devices:

Remote control: The main feature of smart home technology is that you'll be able to control your devices remotely through their respective mobile applications. This comes in handy, especially if you forgot to do something before you left home, be it to turn off your air conditioning unit, to arm your security system or to make sure your doors are locked.

Notifications: You'll also be notified on your mobile app of any events that happen with your smart device. This mainly applies to security cameras, systems and smart locks. You can be notified the second someone opens your front door, walks in front of your video doorbell or unlocks your basement. As you can see, notifications are especially useful when it comes to the security and safety of your home.

Voice commands: Most smart devices work with one of the voice assistants, either the two most common, Alexa and Google Assistant, or the less common Siri or Microsoft Cortana. That means you'll be able to command them using your voice alone, but it's important to make sure that all the devices in your home work with the same voice assistant for consistency's sake.

Geofencing with Smart Thermostats

Geofencing: Geofencing is a feature we've seen with smart locks, primarily. It means taking the GPS from your phone and connecting it to your device so that it turns off or on based on your location. For example, you could have your door automatically unlock when you're within a certain distance, or have your thermostat heat up your home to a temperature when you're near.

Schedules: This one's pretty obvious; many devices can be set onto schedules so that you don't have to control them manually every day. For example, if you know that you always get up on weekdays at seven AM, you could have your bedroom lights turn on to wake you up automatically.

Scenes: Scenes are groups of IoT devices that you've joined together to easily access them at once. We have different scenes for lighting, from reading to bedtime to dance parties, and since we've already customized the colors and brightness, we can get this setup with a touch of a button.

Smart home integrations: Aside from working with voice assistants, many smart home devices also work with devices from other brands. For example, Nest Secure, a security system from Google Nest, works with smart bulbs from LIFX and Philips Hue, meaning we can have our lights turn on once our system is disarmed, meaning we're home. This kind of action is sometimes referred to as an automated trigger or simply as home automation. If the product works with If Then Then That (IFTTT), that means it works with any other product that's integrated with IFTTT, which makes integrating devices from different brands more simple than ever.

Sunrise and Sunset Mode with Smart Bulbs. Sunrise and sunset mode: Mainly applying to smart bulbs, sunrise and sunset mode has connected devices turn on and off

at the beginning and end of the day, syncing with nature. If you want to get back to a Circadian rhythm, a smart bulb with sunrise and sunset mode is a beautiful thing!

Event log: An event log is simply a list of the IoT devices' activity, like what times the smart locks were opened, when the lights were on, and more. This is very useful for smart locks and security systems, in particular, but may not be as necessary for bulbs and other devices.

Energy monitoring: Finally, energy monitoring tells you exactly how much energy your IoT devices are using up. This is really useful for smart thermostats and plugs connected to appliances using 1,800 watts or less, as well as smart bulbs.

Smart homes let you customize your life by automating actions. Have your coffee ready for you in the morning and your electric blanket heated up for you at night, or simply get notified the second your kids come home. With literally thousands of devices available, the possibilities are endless. Getting a smart home is more popular than ever, with more smart speaker owners growing by the second. Here are some statistics you should know about smart home technology in the United States:

76% of people are familiar with smart home technology

53% of people own a smart home device

33% of people said they will buy a smart home device in the next three years7

66% of consumers said that they were most likely to buy or already owned smart home products from Amazon, while 55% said Google and 32% said Apple8

The smart home market will reach $123 billion by 2022, an increase of $67 billion from 20189

62.1% of smart security camera owners check their phones daily to view the camera's footage.

People paid an average of $276 for smart security cameras and an average of $390 for smart security systems

The smart security brands that received the highest customer satisfaction were Arlo, Ring, SimpliSafe and Brink's

63% of Americans track their health using an IoT device, with 13% using connected scales10

A fourth of all broadband households in the United States plan to purchase a smart lock within the next year

35% of all U.S broadband households think smart locks are affordable11

60% of security systems are self-installed12

Amazon will continue to dominate the smart speaker market, expected to hold 70% of total smart speaker ownership in the United States in 2021

In an IQ test, Google Assistant performed better than Alexa and Siri, answering questions correctly 93% of the time13

Smart home technology can make your life easier, more convenient, and even more cost-effective, with the right devices. The good thing about smart home technology is that you don’t have to spend thousands of dollars to get it; there are low-cost devices you can start off with, gradually adding to your collection in the future.