

СТРУКТУРНА СХЕМА СИСТЕМИ ЗАХИСТУ РОЗУМНОГО БУДИНКУ

Вінницький національний технічний університет;

Анотація

Проведено детальний огляд існуючих технологій побудови системи «Розумний будинок», для подальшої розробки та вдосконалення відомих технологій та запропоновано апаратну частину системи захисту розумного будинку.

Ключові слова: Інтернет Речей, розумний будинок, автоматизація, безпека, система, протоколи.

Abstract

The detailed review of the existing technologies of the system "smart home" is proposed for further development and improvement of known technologies. The hardware protection system for smart home is developed.

Keywords: Internet of Things, smart home, automation, security, system protocols.

Вступ

З появою Інтернету життя людини значно спростилося. З'явилася можливість миттєвого доступу до будь-якої інформації. З самого початку доступ до мережі відбувався лише за допомогою комп'ютерів, згодом смартфони надали можливість доступу до мобільного Інтернету. В даний час відбувається перехід до Інтернету Речей [1]. Даний термін застосовується для речей, які мають можливість доступу до мережі Інтернет. Під це визначення підпадають сучасні автомобілі, побутові пристрої, фітнес-трекери і інші речі, якими можна керувати за допомогою смартфона [1]. Яскравим прикладом технології Інтернет Речей є Розумний Будинок – система, що повністю аналізує та оптимізує процес управління житловим простором [1]. Важливим аспектом як Інтернету речей, так і Розумного будинку є захист даних. Практично, будь який пристрій може бути зламаний.

Тому метою даного дослідження є покращення безпеки розумного будинку за рахунок розробки апаратної частини системи захисту.

Результати дослідження

Постійний рух людства до комфорту, до винаходу технічних новинок для спрощення рутинної роботи, і усвідомлення необхідності економії природних ресурсів призвело до винаходу системи «розумний дім» [2]. Таку назву він отримав завдяки точно спланованому програмно-апаратному комплексу, що об'єднує різні побутові прилади в єдину мережу управління [3]. Основною особливістю такої технології є об'єднання окремих підсистем і пристроїв в єдиний комплекс, яким можна керувати за допомогою системи автоматизації [4][5].

До однієї з основних підсистем «Розумного будинку» відносяться системи безпеки.

Основними складовими системи безпеки є датчики руху, присутності, вібрації, розбиття скла, відкриття вікон чи дверей, відеоспостереження, відеодомофони та відеоглазки, електронні замки (розумні замки, смартлоки) і модулі керування воротами, сирени [6][7].

Ці пристрої дозволяють сконструювати оптимальну систему безпеки, від порівняно простої до достатньо складної [8].

Спроектвана система розумного будинку (рис.1) передбачає в собі використання різного виду датчиків та модулів, таких як: датчик відстані, Bluetooth-модуль, датчик руху, двоканальне реле, Arduino Uno, Arduino Nano, GSM-модуль, RFID-мітки, освітлення.

Таким чином, при запуску системи сигналізації розумного будинку, надається можливість отримання попередження про проникнення шляхом спрацювання всіх вище перерахованих датчиків, зокрема GSM-модуля. В свою чергу після спрацювання будь-якого з датчиків GSM-модуль зателефонує на вказаний номер або відправить повідомлення. Також завдяки Bluetooth-модулю,

надається можливість моніторингу системи з написаного мобільного додатку та керування всією системою в цілому. Таким чином побудована система розумного будинку є досить зручною у повсякденному використанні та полегшує виконання рутинних справ.

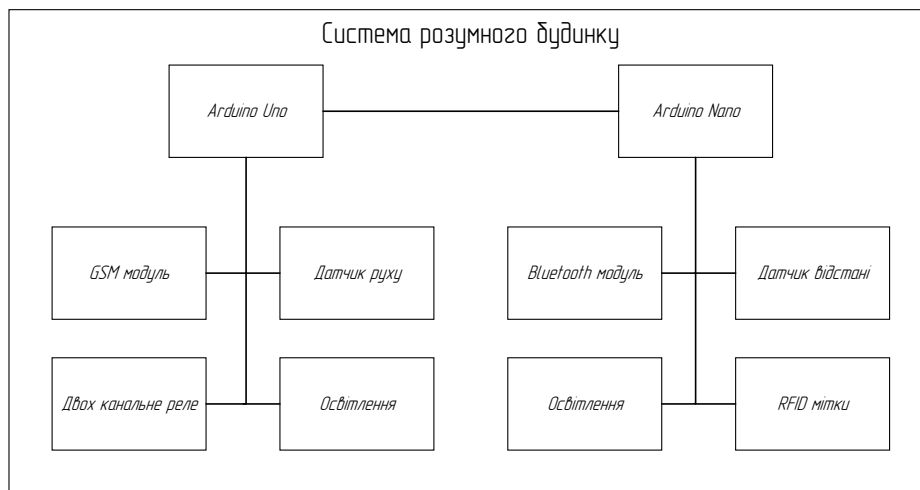


Рис 1 – Структурна схема Розумного будинку

Майже усі пристрої-представники технології Інтернет Речей, піддавалися зламу [9]. Тому для забезпечення безпеки потрібно використовувати комплексний підхід. Методологія оцінки ризиків повинна охоплювати питання забезпечення конфіденційності, безпеки, унеможливлення шахрайських дій, кібератак та викрадання інтелектуальної власності. Ключовим моментом є те, що безпека пристрою повинна враховуватися на етапі проектування [9]. Сюди відноситься безпека в кінцевих вузлах і профілактичні заходи. В тому числі створення захищеного програмного та апаратного забезпечення.

Для захисту інформації, яка зберігається на пристроях та в момент її передачі використовується строга автентифікація, шифрування і безпечне управління ключами шифрування. Одним з можливих способів підвищення стійкості Інтернету Речей і в тому ж числі Розумного будинку є створення не тільки стійкого програмного забезпечення, а й перенесення частини цієї задачі на апаратне забезпечення [9].

Висновки

Проведено детальний огляд існуючих технологій побудови системи «Розумний будинок». Проаналізовано основні аспекти безпеки системи. Запропоновано апаратну частину системи захисту Розумного Будинку. Розглянута схема є середньої складності й дозволяє забезпечити безпеку на належному рівні, також її можливо інтегрувати в систему Розумного будинку як складовий механізований елемент.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інтернет вещей: как изменится вся наша жизнь на очередном этапе развития Сети. [Електронний ресурс]. – Режим доступу: URL http://www.cisco.com/c/ru_ru/about/press/press-releases/2011/062711d.html- Назва з екрану
2. Розумний дім [Електронний ресурс]. – Режим доступу: URL <http://wiki.tntu.edu.ua> – Назва з екрану
3. Какие бывают "умные дома". Обзор. [Електронний ресурс]. – Режим доступу: URL <http://www.besmart.su/article/kakie-byvayut-umnye-doma> – Назва з екрану
4. Что такое Умный Дом. Знакомство с системой [Електронний ресурс]. – Режим доступу: URL http://smarton.com.ua/smart_home/ - Назва з екрану

5. Розумний дім [Електронний ресурс]. – Режим доступу: URL <http://sutem.com.ua/pages/7smartbus.html> – Назва з екрану
6. Центральні елементи розумного будинку [Електронний ресурс]. – Режим доступу: URL <http://sutem.com.ua/021%20inels.php> Назва з екрану
7. Smart house Розумний дім [Електронний ресурс]. – Режим доступу: URL <http://buchuk.domen.uz.ua/index.php?id=smatr-house> – Назва з екрану
8. Домашня автоматизація. [Електронний ресурс]. – Режим доступу: URL <https://ru.wikipedia.org/wiki/>– Назва з екрану
9. Что такое интернет вещей (Internet of Things, IoT) [Електронний ресурс]. – Режим доступу: URL [http://www.tadviser.ru/index.php/B9_\(Internet_of_Things,_IoT\)#](http://www.tadviser.ru/index.php/B9_(Internet_of_Things,_IoT)#) – Назва з екрану

Савченко Катерина Володимирівна — студентка, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна, e-mail: katiasv96@mail.ua

Науковий керівник:

Войтович Олеся Петрівна — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна

Savchenko Kateryna — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: katiasv96@mail.ua

Supervisor:

Voitovych Olesya — phd. Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, Ukraine