

БЕЗПЕЧНІСТЬ «РОЗУМНОГО» БУДИНКУ ЯК МІСЦЯ ПОСТІЙНОЇ РОБОТИ. ПРОГРАМНА ОБРОБКА ВИНЯТКОВИХ СИТУАЦІЙ СИСТЕМИ «РОЗУМНИЙ» БУДИНОК

*Даніленко Н.О., студентка (гр. ІО-43, ФІОТ КПІ ім. Ігоря Сікорського);
Качинська Н.Ф., асистент (каф. ОППЦБ КПІ ім. Ігоря Сікорського);
Прахівнік Н.А., к.т.н., доцент (каф. ОППЦБ КПІ ім. Ігоря Сікорського)*

Комп'ютери та технічні прилади стали невід'ємною частиною повсякденного життя людини. Останнім часом з'явилися і набирають все більшої популярності так звані «розумні» будинки. Вони побудовані повністю за новими технологіями та адаптуються до потреб свого власника [1]. Нескладно передбачити, що рано чи пізно «розумні» будинки будуть не лише житловим помешканням, а й місцем роботи, де одночасно перебуватиме велика кількість людей. Створити належні умови праці, забезпечивши комфорт та безпеку для кожного працівника, - це основне завдання «розумного» будинку як постійного місця роботи. Тому при створенні програмного забезпечення такої системи найбільшу увагу потрібно приділяти не лише її комфортності, а й безпеці.

«Розумний» будинок (або smart house) – це термін, яким зазвичай позначають місце проживання, яке має технічні прилади, системи освітлення, опалення, кондиціонування повітря, оснащене комп'ютерними, аудіо- та відеосистемами, системами безпеки та камерами (рис. 1), причому усі прилади передають сигнали головному комп'ютеру (або комп'ютерам), що координує їхню роботу за наперед визначеним алгоритмом [2].

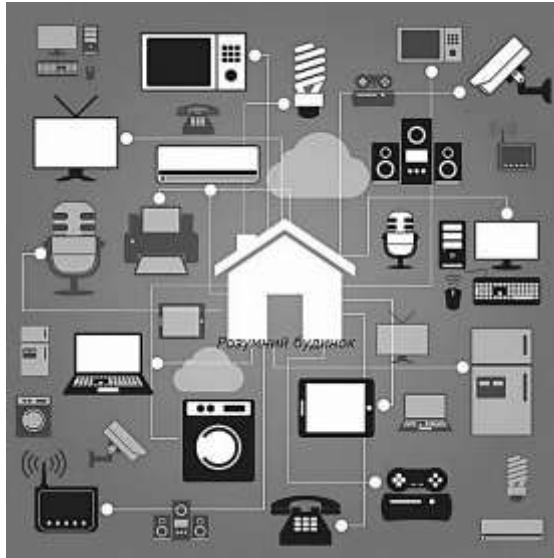


Рис. 1. «Розумний» будинок

Зазвичай smart house має свій власний запасний електрогенератор, вітряк-електрогенератор або ж оснащений сонячними батареями. Такий будинок може

бути дистанційно керований, тобто будь-яка система в кожен момент часу повністю доступна його власнику, який може змінювати заданий алгоритм функціонування відповідно до своїх потреб. Заздалегідь розроблений алгоритм має включати набір виняткових ситуацій, тобто інструкцію, як повинна діяти система в критичному стані. Критичним можна назвати такий стан системи, за якого людині, що перебуває в «розумному» будинку, загрожує небезпека.

Задля запобігання або зменшення дії небезпечних факторів[3], таких, що можуть призвести до травми, гострого захворювання або навіть смерті, у «розумному» будинку, необхідно розподілити систему керування на блоки, що будуть поєднані між собою.

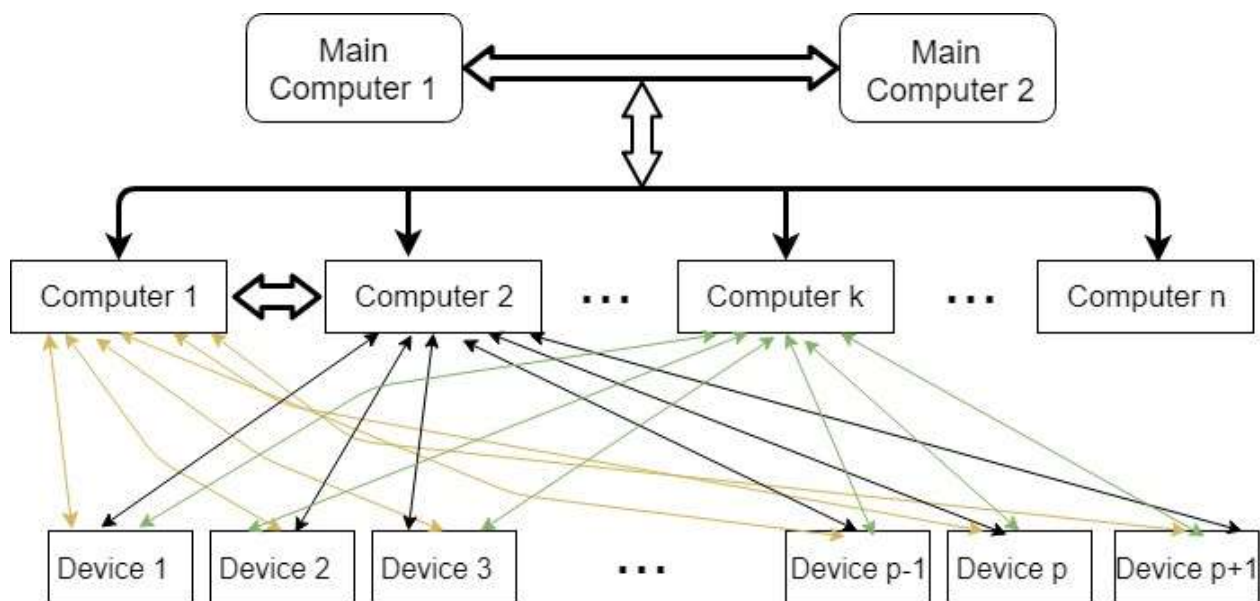


Рис.2. Спрощена схема взаємодії пристроїв та системи керування

На рис.2 зображено спрощену схему взаємодії пристроїв (Device 1 – Device p+1) та системи керування, що складається з n «комп'ютерів» та двох «головних комп'ютерів», що представляють собою розподілений на два «блоки» центр керування. Аналогічний підхід зазвичай використовують для створення об'єктів «Internet of Things» (IoT) [4], де кожен пристрій взаємодіє з іншим через центральний пристрій управління. Задля додаткового захищення системи IoT, а також для того, щоб не перенавантажувати канали передачі інформації (тим самим не збільшувати час прийому/відправки пакетів інформації), бажано використовувати не один пристрій управління, а два [5]. У такому підході є кілька суттєвих переваг: по-перше, в будь-який момент за допомогою одного з пристроїв управління (будь-якого) можна вимкнути потрібний пристрій (пристрої), а в разі «злому» одного з пристроїв управління інший пристрій блокує всі процеси.

При розробці програмного забезпечення «розумного» будинку програмний код, що реалізує певний алгоритм, для кожного пристрою пишуть окремо. Потім кожна написана програма тестується з урахуванням виняткових

ситуацій. Після цього усі програми поєднують в одне ціле – повне програмне забезпечення, яке так само тестується. При «об'єднанні» частин програмного коду в один рідко враховуються виняткові ситуації [6], які при цьому виникають. Це стосується, насамперед, одночасної синхронізації усіх пристроїв з пристроєм (пристроями) управління. Щоб відокремити виняткові ситуації та за можливості створити відповідний алгоритм дії, слід переглядати систему «розумного» будинку, щоразу відштовхуючись від його безпосереднього призначення. Таким чином, якщо дана система буде впроваджена на металургійному заводі, то необхідно дослідити виробниче середовище на об'єкті, вивчити умови праці при здійсненні того чи іншого технологічного процесу [7], провести аналіз нещасних випадків та професійних захворювань працівників [8]. Відповідно до Закону України «Про охорону праці» від 14 жовтня 1992 року [9], а також згідно зі ст. 25 Закону України «Про підприємства в Україні» [10] підприємство зобов'язане забезпечити всім працюючим на ньому безпечні умови праці. Задля цього кожне підприємство розробляє конкретні заходи з метою усунення або приведення до нормативних значень виявлених на підприємстві небезпечних та шкідливих виробничих факторів. Саме ці заходи, що запобігають травматизму та захворюванням, можна покласти в основу виняткових ситуацій при створенні відповідного програмного забезпечення «розумного» будинку.

Для управління «розумним» будинком як помешканням його власник та визначені ним особи використовують програму на своєму телефоні / планшеті чи іншому електронному пристрої. Причому кожна особа має різні «права» (повні чи обмежені) для зміни параметрів функціонування системи. Це зроблено для того, щоб система функціонувала злагоджено. Також такий розподіл «прав» для власників будинку забезпечує зменшення ризику появи непередбаченої заздалегідь виняткової ситуації до 60-70%. Так само при впровадженні системи «розумного» будинку в робочий простір чи на підприємство слід детально визначити «права» кожного з працівників. Це зовсім не означає, що для кожного нового працівника (користувача) потрібно модифікувати всю систему і прописувати окремо «права». Можна автоматично розподілити затверджені «права» для кожної групи користувачів. Подібну систему розподілу «прав» для користувачів використано в операційній системі Windows [11]. Так само під час хвороби працівника або після його звільнення система автоматично може блокувати частково або повністю доступні йому функції.

При впровадженні «розумного» будинку на підприємстві виникає питання підключення усіх пристроїв до системи керування. Частина пристроїв може бути підключена за допомогою бездротової локальної мережі WLAN (Wireless Local Area Network) з технологією Wi-Fi або бездротової персональної мережі WPAN (Wireless Personal Area Network) з технологією Bluetooth. Але більшість пристроїв буде підключено за допомогою дротів. У середньому для підключення стандартних пристроїв у двокімнатній квартирі (28 кв. м.) знадобиться більше 1км дротів[12]. Для підключення «розумного» будинку на

підприємстві знадобиться у 10-100 разів або й більше кілометрів дротів. Така кількість дротів утворює сильне електромагнітне поле, яке негативно впливає на здоров'я людини. Виходячи з цього, перебування працівників на підприємстві доведеться обмежити до кількох годин денно.

Дві основні засади створення smart house: постійне отримання електроенергії та доступ до мережі Інтернет. Саме тому, заздалегідь передбачаючи можливість виникнення несправностей в системі, що призведуть до повного чи тимчасового припинення подачі електроенергії, розробники закладають наявність додаткового/запасного електрогенератора. Враховуючи, що все більшої популярності набирають «зелені» види електроенергії, то все частіше встановлюють сонячні батареї або «вітряки». Для встановлення електрогенератора потрібно виділити окреме приміщення та обмежити доступ працівників до нього, щоб забезпечити їхню безпеку. При встановленні вітрогенератора звертають увагу, перш за все, на створюваний під час праці шум. Такий шум негативно впливає на людину. Тому при виборі альтернативного джерела енергії варто переглянути його недоліки, які впливають на стан здоров'я людини [13], і заздалегідь продумати методи їх усунення.

Висновки. Було проведено дослідження системи «розумний» будинок з можливістю її встановлення на підприємстві. Наведено та проаналізовано принципи програмної обробки виняткових ситуацій даної системи. Зроблено аналіз безпечного використання «розумного» будинку. Програмне забезпечення «розумного» будинку потрібно вдосконалювати окремо під кожен об'єкт. При використанні даної системи необхідно чітко описати алгоритми дій при виникненні критичних ситуацій, тим самим забезпечивши її адаптивність.

Література

1. What is a smart home [Електронний ресурс] – Режим доступу до ресурсу: <https://www.smarthomeusa.com/smarthome/>.
2. Умный Дом - охрана и безопасность. [Електронний ресурс] // Smarton – Режим доступу до ресурсу: http://smarton.com.ua/kontrol-bezopasnost-doma/upravlenie_ohrannoy_pogarnoy_signalizaciy_v_umnom_dome/.
3. Macdonald D. Practical Industrial Safety, Risk Assessment and Shutdown Systems / Dave Macdonald., 2004. – 384 с. – (Newnes). – (IDC Technology).
4. Burgess M. What is the Internet of Things? Wired explains [Електронний ресурс] / Matt Burgess // Wired. – 2018. – Режим доступу до ресурсу: <http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot>.
5. The Internet of Things (IoT): An Overview [Електронний ресурс] // Internet Society. – 2015. – Режим доступу до ресурсу: <https://www.internetsociety.org/resources/doc/2015/iot-overview>.
6. Отладка и обработка исключительных ситуаций [Електронний ресурс] // Интуит. Национальный открытый университет – Режим доступу до ресурсу: <https://www.intuit.ru/studies/courses/2247/18/lecture/584?page=4>.

7. Охорона праці / М. С.Одарченко, А. М. Одарченко, В. І. Степанов, Я. М. Черненко. – Харків: Стиль-Издат, 2017. – 334 с. – (ISBN 966-7885-84-4).
8. Серіков Я. О. Основи охорони праці / Я. О. Серіков. – Харків: ХНАМГ, 2007. – 227 с. – (ISBN 966-695-076-6).
9. Закон України Про охорону праці [Електронний ресурс]. – 1992. – Режим доступу до ресурсу: <http://zakon2.rada.gov.ua/laws/show/2694-12>.
10. Закон України Про підприємства в Україні [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: <https://docs.dtkr.ua/doc/1085.18.0>.
11. In Windows, what are local users and domain users? [Електронний ресурс] // Indiana University. – 2017. – Режим доступу до ресурсу: <https://kb.iu.edu/d/anbn>.
12. Умный Дом: 5 доводов «против» [Електронний ресурс] // tech-house.su. – 2017. – Режим доступу до ресурсу: <http://tech-house.su/umnyj-dom-5-dovodov-protiv/>.
13. Roger L. Brauer, Ph.D., CSP, PE. Safety and health for engineers / Roger L. Brauer, Ph.D., CSP, PE. – Hoboken, New Jersey, 2006. – 496 с. – (John Wiley & Sons).