УДК 004.4

Т. О. Савчук
К. Г. Капченко

РОЗРОБКА АЛГОРИТМУ АНАЛІЗУ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

Вінницький національний технічний університет

Анотація

Запропоновано алгоритм аналізу безпеки розумного будинку, що базується на результатах досліджень за основними критеріями виявлення небезпеки, що забезпечить надійний захист управління безпекою в розумному будинку.

Ключові слова: розумний будинок, аналіз безпеки, інтелектуальна інфраструктура, автоматизація, оцінювання.

Abstract

An algorithm for analysing the security of a smart home based on the results of research on the main criteria for detecting danger is proposed, which will provide reliable protection of security management in a smart home.

Keywords: smart home, security analysis, intelligent infrastructure, automation, assessment.

Вступ

Розумний будинок, також відомий як «система домашньої автоматизації» є спроектованим житловим простором, який використовує передові технології для покращення комфорту, безпеки, зручності та енергоефективності для його мешканців. Безпека – одна з найважливіших складових розумного будинку. Завдяки здатності до автоматизації розумного будинку, управління безпекою стає більш надійним. Ключовий етап в управлінні безпекою є аналіз безпеки розумного будинку. Після проведення аналізу безпеки власник може управляти нею за допомогою відповідної інформаційної технології через додатки або спеціальні панелі керування.

Отже, розробка алгоритму аналізу безпеки розумного будинку, на основі якого буде проводитись управління, є актуальною задачею.

Результати дослідження

Розумний будинок – це інноваційне технологічне рішення, що поєднує автоматизацію та інтеграцію різних систем, пристроїв та компонентів в житловому просторі задля покращення безпеки та комфорту. У розумному будинку використовуються передові сенсори, мережі зв'язку, розподілені системи керування та програмне забезпечення для того, щоб створити інтелектуальну інфраструктуру. Технологія розумного будинку використовується для різних цілей: підвищення комфорту, тепло та енергозбереження, забезпечення безпеки [1].

Безпека є однією з найважливіших характеристик розумного будинку. Вона охоплює багато аспектів:

1. Системи відеоспостереження.
2. Системи безпеки з автоматичним оповіщенням.
3. Датчики безпеки.
4. Автоматична сигналізація.
5. Віддалений доступ та моніторинг [2].

Аналіз безпеки розумного будинку здатен мінімізувати ризики несанкціонованого доступу та досягти більш високого рівня захисту [3], за рахунок таких кроків:

1) Аудит безпеки: Проведення аудиту безпеки дозволяє ідентифікувати потенційні вразливості та ризики в системі. Може включати перевірку додатків на вразливості, аналіз мережевої безпеки, тощо;
2) Шифрування даних: Забезпечення шифрування даних може запобігти несанкціонованому доступу та перехопленню даних. Використання сильних шифрувальних алгоритмів та протоколів допомагає забезпечити конфіденційність та цілісність даних.

3) Аутентифікація та авторизація: Реалізація надійних методів аутентифікації допомагає перевірити ідентичність користувача перед наданням доступу до системи. Окрім того, важливо належно керувати правами доступу та авторизувати користувачів для запобігання несанкціонованому використанню системи.

Існуючі додатки для управління безпекою в розумному будинку «Google Home» та «Vivint Smart Home» характеризуються зручним способом перегляду відео з камер спостереження, отримання сповіщень про керування системами освітленням і термоконтролем. Проте, їх використання для забезпечення повноцінної безпеки розумного будинку потребує удосконалень щодо покращення безпеки самого додатку, наприклад, шляхом удосконалення механізмів аутентифікації та захисту персональних даних користувачів, а також розширення можливостей до автоматизації. Тому доцільним є створення відповідної інформаційної технології що дозволить користувачам налаштовувати різні сценарії безпеки за їх потребами.

Процес аналізу безпеки розумного будинку передбачає оцінювання за такими основними критеріями:

1. Підключення відеоспостереження: Цей критерій включає оцінку системи відеоспостереження в розумному будинку. Для забезпечення безпеки, система відеоспостереження повинна мати відеокамери, розташовані в стратегічних місцях, які покривають ключові зони. Важливо оцінити якість відеозапису, можливість перегляду в реальному часі та можливості зберігання записів. Крім того, важливо перевірити, чи існує захист від несанкціонованого доступу до відео.
2. Підключення до служби моніторингу безпеки: Оцінка підключення до служби моніторингу безпеки передбачає перевірку можливості підключення розумного будинку до професійної служби моніторингу. Це може включати сповіщення про події безпеки, які автоматично передаються до центру моніторингу, і можливість надсилати кваліфіковану допомогу або викликати екстрені служби при потребі.
3. Датчики пожежі (витоку газу, диму, води): Оцінка наявності датчиків пожежі в розумному будинку включає перевірку наявності датчиків витоку газу, диму та води. Ці датчики мають спрацювати при виявленні небезпеки і надіслати сповіщення користувачеві та/або активувати автоматичну сигналізацію для швидкого реагування на потенційну небезпеку.
4. Розпізнання чужої присутності: Оцінка системи розпізнання чужої присутності включає перевірку наявності датчиків руху та інших пристроїв, які можуть виявляти недозволену активність у будинку. Такі системи можуть активувати сигналізацію або сповіщення, якщо вони виявляють незвичайну активність, що може свідчити про несанкціонований доступ до будинку.
5. Автоматична сигналізація: Оцінка наявності автоматичної сигналізації передбачає перевірку системи, яка може активувати сигналізацію при виявленні небезпечної ситуації, такої як злам або вторгнення. Це може включати виклик служб безпеки або екстрені служби, якщо потрібно.

Удосконалений алгоритм аналізу безпеки розумного будинку базується на зниженні ризиків несанкціонованого доступу або виходу з ладу систем таких, як відеоспостереження, датчики пожежі і тд., та забезпеченні надійного захисту будинку. Основою для аналізу безпеки розумного будинку є використання статистичних методів, що дозволяють об'єктивно оцінити стан безпеки будинку і знизити вплив суб'єктивних факторів. Алгоритм складатиметься з таких кроків:

1. Отримання інформації про поточний стан системи безпеки розумного будинку у вигляді технічних характеристик та функціональних можливостей компонентів розумного будинку, що пов'язані з безпекою, такі як відеокамери, датчики руху, системи тривоги, датчики пожежі, тощо та визначення їх поточного стану.
2. Аналіз вразливостей – виявлення потенційних вразливостей систем безпеки розумного будинку, за рахунок визначення поточного стану компонентів розумного будинку та отримання списку потенційних вразливостей таких, як слабкі місця у захисті будинку, незахищеність мережі, слабкі паролі, несправність датчиків чи відеоспостереження і тд. Включаючи:
   - Оцінку фізичної безпеки;
   - Оцінку мережевої безпеки;
   - Оцінку кібербезпеки;
   - Оцінку систем моніторингу.
3. Розробка заходів безпеки у вигляді набору заходів безпеки у додатку для запобігання та мінімізації виявлених загроз і вразливостей. Це може включати встановлення сильних паролів, шифрування комунікацій, використання двофакторної аутентифікації, оновлення програмного забезпечення, та регулярну перевірку на наявність вразливостей. А також набор сценаріїв при виявлені певної загрози безпеці, створений власником у додатку.

4. Тестування безпеки за допомогою аудиту безпеки, основне ідея якого полягає в систематичному скануванні розумного будинку з метою виявлення потенційних вразливостей. Може включати: перевірку мережевої безпеки, перевірку наявності захисту від хакерських атак, перевірку справності датчиків безпеки та інших компонентів системи. Це допоможе виявити потенційні слабкі місця і вразливості, які можуть бути використані зловмисниками.
5. Ідентифікація загроз – визначення потенційних загроз безпеці будинку за рахунок отримання сповіщень про загрозу з відповідних датчиків або камер. Це можуть бути фізичні загрози (наприклад, крадіжки, пожежі) або цифрові загрози (наприклад, хакерські атаки, злам системи). Ідентифікація загрози відбуватиметься з використанням алгоритмів машинного навчання із урахуванням попереднього аналізу вразливостей систем розумного будинку та зібраних даних з датчиків безпеки та відеоспостереження.
6. Механізм реагування на виявлену загрозу. Реагування відбуватиметься з урахуванням автоматичних сценаріїв реагування. При виявлені загрози, власнику будинку та службі моніторингу безпеки надійде сповіщення, що демонструватиме потенційну загрозу, а також буде виконано відповідний сценарій для забезпечення безпеки.

З урахуванням означених кроків, побудовано алгоритм аналізу безпеки розумного будинку, на рисунку 1 зображено UML-діаграму розробленого алгоритму.

Рисунок 1 – UML-діаграму алгоритму аналізу безпеки розумного будинку

Висновки

Таким чином, запропонований алгоритм аналізу безпеки розумного будинку, дасть можливість виявлення вразливостей систем безпеки розумного будинку, виявлення загрози та визначення її типу. Крім того, означений алгоритм забезпечить надійне управління розумним будинком за рахунок виявлення потенційних загроз в системі безпеки та створеному набору сценаріїв власником будинку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Розумний будинок. URL: https://oxorona.com/smart-home/. (Last accessed: 16.05.2023)
2. Безпека. URL: https://www.smarthouse.ua/ua/bezopasnost.html. (Last accessed: 17.05.2023)
3. Поради щодо підвищення безпеки у вашому розумному будинку. URL: https://worldvision.com.ua/sovety-po-povysheniu-bezopasnosti-v-vashem-umnom-dome/. (Last accessed: 16.05.2023)

Савчук Тамара Олександрівна – PhD, професор кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, savchuk_t@vntu.edu.ua.

Капченко Карина Григорівна – студентка групи 1КН-22м, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця, e-mail: kkapcenko@gmail.com.

Savchuk Tamara Oleksandrivna – PhD, Professor of the Computer Sciences Chair, Vinnytsia National Technical University, Vinnytsia, savchuk_t@vntu.edu.ua.

Kapchenko Karina Grigorievna – student of group 1CS-22m, Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: kkapcenko@gmail.com.