УДК 004.031

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

ПРОГРАМНІ АСПЕКТИ «РОЗУМНОГО БУДИНКУ». АНАЛІЗ ІСНУЮЧИХ ПРОГРАМ ЗАХИСТУ

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

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

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

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

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

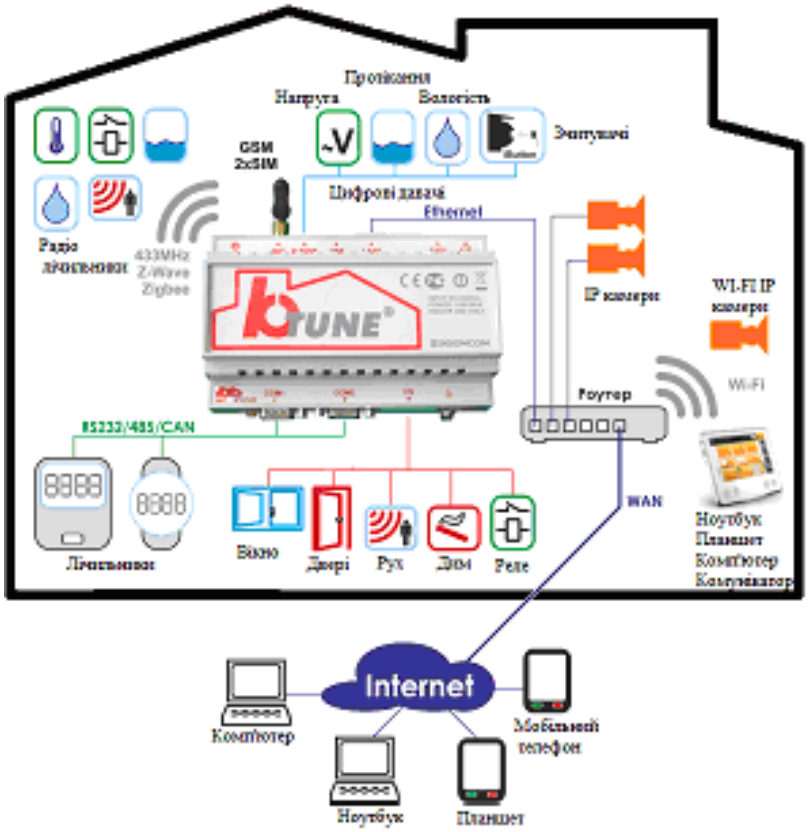

Рисунок 1- Розумний будинок

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

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

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

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

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

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

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

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

Література

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

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

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

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