ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ «РОЗУМНОГО БУДИНКУ»

Маслакова Н.Ю., Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Під «розумним будинком» розуміють систему, яка забезпечує безпеку та ресурсозбереження (зокрема і комфорт) всіх користувачів. У найпростішому випадку вона повинна вміти розпізнавати конкретні ситуації, що відбуваються в будинку, та відповідним чином на них реагувати: одна із систем може керувати поведінкою інших за заздалегідь виробленим алгоритмам.

Система може самостійно відключати електроприлади, переводити їх у сплячий режим за відсутності людей. За потреби система дозволяє в будь-який час переводити автоматичне керування обладнанням у ручному режимі.

Метою доповіді є виявлення загроз інформаційної безпеки, які є порушенням конфіденційності, цілісності та доступності інформації, а також позбавлення таких загроз як: атака хакерів, перехоплення інформації, віруси у системі, доступ зловмисника у зв'язку з крадіжкою прав.

В роботі було розглянуто основні вразливості системи «розумний будинок»: підключення мережі «розумного будинку» до Інтернету, неефективний захист трафіку, вразливості системи автентифікації [1] та ідентифікації. Також оцінені можливі наслідки загроз, таких, як порушення роботи центрального сервера, порушення конфіденційності інформації, збої в ПО системи. Дослідження були проведені з використанням шкали оцінки впливу загроз(високий, середній та низький вплив на систему).

Запропоновано варіанти того, як зробити розумний будинок безпечнішим за рахунок підвищення захищеності усіх слабких ланок, підвищення надійності під час автентифікації, надання доступу за спеціальними картами або чіпами [2], тощо.

Виходячи з результатів оцінки впливу загроз, найнебезпечнішими є ті загрози, у яких зловмисник може брати під контроль всю систему. Тому вкрай важливим є проведення заходів щодо захисту телекомунікаційної мережі, розмежування прав доступу користувачів.

Список літератури

1. G. Liashenko, A. Astrakhantsev, Implementation Biometric Data Security in Remote Authentication Systems via Network Steganography, Conference on Mathematical Control Theory, 2019, 257-273 pp. DOI: https://link.springer.com/chapter/10.1007/978-3-030-58359-0_14

2. Від розумних інструментів до інтелектуального простору. [Електронний ресурс]. Режим доступу: http://umnydom.kiev.ua/index.php?nma=catalog&fla=stat&cat_id=3&page=1&nums=24/