Секція 1

КІБЕРБЕЗПЕКА РОЗУМНИХ БУДИНКІВ

Кіріченко Д. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Землянко Г. А.

Актуальність. Розумні будинки з інтегрованими пристроями Інтернету речей (IoT) значно підвищують комфорт і автоматизацію житлових приміщень, забезпечуючи контроль над освітленням, кліматом, безпекою та іншими системами. Кількість пристроїв IoT зростає приблизно на 18-20 відсотків на рік, і відповідний ризик кіберзагроз для приватності та безпеки також зростає [1]. Вразливості цих пристроїв, такі як недостатній захист даних, слабкі паролі та відсутність надійної автентифікації, створюють потенційні загрози для безпеки будинків. Така ситуація підкреслює важливість розробки та впровадження ефективних заходів кібербезпеки, спрямованих на захист персональних даних користувачів та мінімізацію ризику несанкціонованого доступу [2, 3].

Метою даної роботи є аналіз ризиків, загроз, вразливостей та методів захисту, що забезпечують кібербезпеку в системах розумного будинку.

Основні положення. В роботі розглядається архітектура та вразливості розумних будинків. Системи «Розумний будинок» містять мережеві пристрої, датчики та контролери, які взаємодіють через Інтернет, що підвищує ризик кіберзагроз. Основні вразливості включають слабкі паролі, недостатнє шифрування та ненадійну автентифікацію (особливо це стосується протоколів Zigbee та Z-Wave). Статистика показує, що 38% атак на пристрої IoT спричинені слабкими паролями та відсутністю двофакторної аутентифікації [2, 3]. Також в роботі представлені основні кіберзагрози для розумних будинків [2, 4]. Атаки можна розділити на: перехоплення даних, атаки на програмне забезпечення та соціальна інженерія. До атак перехоплення даних відносяться атаки на Zigbee та Z-Wave, які можуть призвести до перехоплення та фальсифікації даних. До атак на програмне забезпечення відноситься вразливості програмного забезпечення, що роблять пристрої мішенню для бот-мереж, таких як Mirai, які здійснюють DDoS-атаки. Приблизно 30% атак на домашні системи IoT успішно здійснюються з використанням методів соціальної інженерії. В роботі зазначаються наступні методи забезпечення кібербезпеки [1, 5]. Шифрування даних (наприклад, AES-256) для захисту під час передачі. Багатофакторна автентифікація для захисту віддаленого доступу.

Оновлення прошивок: Регулярні оновлення усувають відомі вразливості в Zigbee та Z-Wave. Брандмауери та фільтрація трафіку для захисту від вторгнень. Відповідність стандартам безпеки, рекомендованим Zigbee Alliance та IEEE. Відновлення після збоїв та підвищення обізнаності користувачів. Резервне копіювання, автоматичне оновлення та віддалений доступ забезпечують швидке відновлення систем у разі збою, також важливо навчити користувачів основним правилам безпеки, таким як використання унікальних паролів та оновлення програмного забезпечення [1, 5].

Висновки. Кібербезпека розумного будинку вимагає численних заходів захисту, включаючи шифрування даних, багатофакторну автентифікацію, регулярне оновлення та використання безпечних протоколів. Також важливо дотримуватися стандартів кібербезпеки і підвищувати обізнаність користувачів для захисту персональних даних і безпеки житлового простору.

Список літератури

1. Review of Smart-Home Security Using the Internet of Things / G. Vardakis et al. *Electronics*. 2024. Volume 13(16). Page 3343. DOI: https://doi.org/10.3390/electronics13163343.

2. Yin H. Wireless systems in smart home evolution and integration. *Highlights in science, engineering and technology*. 2024. Volume 111. Page 585–589. DOI: https://doi.org/10.54097/14fgga79.

3. Ehrenberg N. Smart Home Technologies: Convenience and Control. *Humane Autonomous Technology*. Cham, 2024. Page 181–198. DOI: https://doi.org/ 10.1007/978-3-031-66528-8_8.

4. Piedrahita Solorzano G.A., Flórez Gutiérrez A., Gordillo A.P. Data security threats on smart devices at home. *ARPHA conference abstracts*. 2023. Volume 6. DOI: https://doi.org/10.3897/aca.6.e106978.

5. Ansari A. M., Nazir M., Mustafa K. Smart homes app vulnerabilities, threats, and solutions: a systematic literature review. *Journal of network and systems management*. 2024. Volume 32(2). DOI: https://doi.org/10.1007/s10922-024-09803-1.

Відомості про авторів

Кіріченко Данило Володимирович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.v.kirichenko@student.csn.khai.ed

Землянко Георгій Андрійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезпеки, g.zemlynko@csn.khai.edu