Секція 1

РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ МЕТОДІВ І ЗАСОБІВ АНАЛІЗУ ВРАЗЛИВОСТЕЙ І ЗАХИСТУ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ РОЗУМНИХ ОФІСІВ

Молчанов А. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

Актуальність. Збільшення кількості приладів на базі інтернет речей та прагнення зробити офіси більш енергоефективними призвело до тенденції різкого поширення систем розумних офісів останніми роками. Значну роль у цьому відіграло і збільшення інвестиції у цю сферу. Розумний офіс - це комбіноване використання розумних пристроїв, які з'єднані через мережу в одну систему [1]. Згідно з наведеними звітами компаній Allied Market Research і Data Bridge Market Research розмір світового ринку у сфері смарт-офісів та програмного забезпечення для смарт-офісів до 2028-2030 років сягне 90.63 мільярдів доларів [2]. Так з появою нових рішень збільшиться й актуальність питання безпеки, як фізичної так і кібербезпеки.

Метою даної роботи є дослідження проблем безпеки, функцій, архітектур, платформ, можливих атак і загроз, а також обґрунтування необхідності в їх захисті.

Згідно річного звіту Європейського ринку систем безпеки інтернету речей (IoT), протягом наступних років, аж до 2028 року, загальний середньорічний темп зростання інцидентів досягне відмітки 12.5% у Європейському регіоні. Основним напрямком з безпеки прогнозовано стане захист від витоку даних [3].

Основні положення. Структури смарт офісів, які побудовані на технологіях інтернету речей, включають в себе: датчики, що збирають інформацію; побутові пристрої; канали зв’язку; сервери; мобільні додатки; тощо [3]. Серед основних функцій розумних офісів слід виділити: контроль енергоефективності; контроль комфортних приладів для функціоналу офісу; контроль безпеки; контроль управління офісним середовищем; контроль зчитування лічильників [1]. Платформи для розумних будинків є зв’язуючим компонентом, до якого під’єднуються всі прилади і існують у трьох типах: програмні, апаратні та комбіновані. Оскільки до платформ підключаються усі розумні пристрої, то вони повинні бути універсальні і підтримувати основні стандарти зв’язку. Єдиної схеми архітектури для смарт офісів не існує[4].

Серед загроз і атак на системи смарт офісів можна виділити наступні: атаки на інформаційні активи, можливі загрози безпеки та атаки на архітектури [5].

Висновки. Через стрімке збільшення кількості розумних приладів, які можна інтегрувати у середу смарт офісів, збільшується і актуальність в їх захисті. Проаналізувавши основні функції, платформи та архітектури смарт офісів зроблено висновок, що за основу смарт офісів береться одна з трьох платформ: програмна, апаратна чи комбінована. Єдиної архітектури для таких систем не існує, оскільки у кожному офісі можуть бути різноманітні прилади чи системи комунікації. Отже після обрання платформи можна розробляти свою архітектуру. Аналізуючи атаки на системи інтернету речей виявлено, що зловмисники можуть проводити атаки як на самі контролери та сервери, так і на пристрої, які збирають, передають інформацію, та активно взаємодіють з актуаторами.

Список літератури

1. Smart Home: Architecture, Technologies and Systems. *Sciencedirect.* URL – https://www.sciencedirect.com/science/article/pii/S1877050918305994 (дата звернення: 23.04.2023);
2. Global Smart Office Market. *Alliedmarketresearch.* URL – https://www.alliedmarketresearch.com/smart-office-market-A13723 (дата звернення: 17.04.2023);
3. Європейський ринок безпеки інтернету речей (IoT) — зростання, тенденції, вплив COVID-19 і прогнози (2023–2028роки). *Mordorintelligence.* URL: https://www.mordorintelligence.com/ru/industry-reports/europe-internet-of-things-iot-security-market (дата звернення: 22.04.2023);
4. The best smart home systems 2023: Top ecosystems explained. *the-ambient.* URL – https://www.the-ambient.com/guides/smart-home-ecosystems-152#:~:text=Google,%20Amazon,%20Apple%20and%20SmartThings,make%20home%20automation%20a%20doddle (дата звернення: 24.04.2023);
5. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Mdpi.* URL – https://www.mdpi.com/1424-8220/18/3/817 (дата звернення: 27.04.2023).

Відомості про авторів

Молчанов Артем Олегович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.o.molchanov@student.csn.khai.edu
Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, професор, v.kharchenko@csn.khai.edu