**УДК 004.031.6**

**О. Р. Оробчук, доктор філософії, І. М. Кивацький**
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

## АНАЛІЗ РИЗИКІВ ТА ВРАЗЛИВОСТЕЙ В СИСТЕМАХ КЕРУВАННЯ РОЗУМНИМ БУДИНКОМ

**O. R. Orobchuk, Dr, I. M. Kyvatskyi**

## ANALYSIS OF RISKS AND VULNERABILITIES IN SMART HOME MANAGEMENT SYSTEMS

На сьогодні кількість розумних будинків у світі налічує більше 500 мільйонів, що робить повсякденне життя набагато зручнішим. Однією з найбільших переваг технологій розумного будинку є використання пристроїв, підключених до Інтернету, для дистанційного захисту особистих помешкань. Незважаючи на те, що розумні домашні пристрої безпеки забезпечують легкість захисту будинків від крадіжки, пошкодження чи нещасного випадку, вони також створюють ризик зниження безпеки персональних даних.

Розумні будинки вразливі до різного роду кібератак через вразливі локальні мережі та недосконалі пристрої IoT. В цьому контексті безпеку розумного пристрою розглядатимемо як функцію управління ризиком того, що пристрій буде зламано, з урахуванням збитків внаслідок зламу, а також часу і ресурсів для забезпечення необхідного рівня захисту.

Загалом, можна виокремити такі ризики, як ботнети, man-in-the-middle атаки, DoS-атаки, крадіжки даних, дистанційний запис, централізація мереж IoT. Перехоплення та злом шифрування є найпоширенішими способами хакерського проникнення в мережу. Під час атаки хакери викрадають будь-який пакет даних, що передається між пристроєм і маршрутизатором, передають його на свій пристрій і використовують brute-force атаку, щоб розшифрувати його. Зазвичай це займає лише хвилини. Wi-Fi може бути вразливим до атак через стандартні або слабкі SSID або паролі та вразливі протоколи шифрування. Облікові дані за замовчуванням дозволяють зловмиснику отримати доступ до маршрутизатора без зусиль. Надійні паролі Wi-Fi змушують хакерів шукати складніші шлюзи для проникнення в мережу. Більшість маршрутизаторів Wi-Fi використовують WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) або протокол безпеки WPA2. WEP — це потоковий шифр RC4. Слабкою стороною WEP є малий розмір вектора ініціалізації (24-розрядний IV), що спричиняє його повторне використання. Це повторення робить його вразливим.

Постачальники IoT не можуть надати необхідні спеціальні рішення безпеки. Крім того, розумні домашні пристрої часто працюють під управлінням невеликих операційних систем, таких як INTEGRITY, Contiki, FreeRTOS і VxWorks, чиї рішення безпеки не такі надійні, як рішення систем на базі Windows або Linux. Оскільки розумні домашні пристрої все більше розширюються у функціональності, розуміння ризиків безпеки персональних даних і способів їх зменшення є критично важливим і вимагає поєднання технологій, процесів і політик. Важливо, щоб пристрої мали вбудовану безпеку як основну, а не як додаткову функцію.

**Література**

1. Джермен Галеґуа. Розумні міста — ArtHuss 2021. — 129 р.
2. Mads Kristensen. The Automated Home: A practical guide to automating your smart home – London : A Book Apart 2023 – 55 p.