УДК 621.396:004.056]:654.924

# СИСТЕМА ОХОРОННОЇ СИГНАЛІЗАЦІЇ НА БАЗІ WI-FI СКАНЕРА

Когогін Я. М.
email: yaroslav.kohohin@nure.ua
Науковий керівник – к.т.н., доцент Ликов Ю.В.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ

This work investigates the principle of operation of a Wi-Fi module in monitoring mode, the creation of a system that responds to malicious devices in the field of operation of such a sensor, and notifies about a threat. The result of the operation of system is the detection of devices, the comparison of their MAC address in the database and, in the absence of this device, the activation of the notification system

У сучасному світі питання безпеки набуває дедалі більшого значення, особливо в умовах зростання кількості несанкціонованих проникнень до приміщень. Традиційні системи охоронної сигналізації потребують прокладання дротових з’єднань або використання спеціальних датчиків, що може ускладнювати їхню інтеграцію в уже існуючі об’єкти. Одним із перспективних напрямків у сфері охоронних технологій є використання Wi-Fi-сканерів для контролю простору та виявлення підозрілих змін у мережевому середовищі.

Сканер Wi-Fi дозволяє зчитувати унікальні MAC-адреси клієнтського пристрою, що дозволяє відслідковувати його, якщо пристрій, що не є легітимним та приступити до ліквідації загрози. Не кожен Wi-Fi модуль підтримує режим моніторингу. Його наявність залежить від моделі чипсета та драйверів.

Деякі модулі, особливо вбудовані адаптери ноутбуків, мають обмежену функціональність, тоді як зовнішні адаптери на певних чипсетах (Atheros, Realtek, Ralink) часто підтримують цей режим тому перед придбанням модулю потрібно подивитися в специфікаціях від виробника, чи підтримує він такий режим, що потрібен для створення сканеру. Після переведення Wi-Fi модуля в режим моніторингу можна запустити скрипт, який сканує всі пристрої в зоні покриття та фіксуватиме їхні MAC-адреси. Це дозволить створити "вайт-ліст" легітимних пристроїв, зокрема персоналу, служби безпеки та працівників.

Скрипт можна реалізувати на Python за допомогою scapy або airodump-ng. Він перехоплюватиме beacon, probe request та data-пакети, зчитуватиме MAC-адреси та записуватиме їх у базу даних або файл для подальшого аналізу.

Система при виявлені MAC-адреси порівнює із тими, що є у базі даних. Якщо такої MAC-адреси немає у «вайт-листі», то запускається сповіщення. Найлегше створити телеграм-бота через те що ця платформа є досить гнучкою та написати код програми для нього не буде великою про-

блемою на сьогодення. Також, можна реалізувати сповіщення SMS на телефони співробітників, що підвищить ефективність на реагування загрози.

Для реалізації функції зловмисника на великих об’єктах пропонується встановити кілька таких модулів із режимом моніторингу (рис.1). Розподілена система моніторингу дозволяє точніше визначати місцезнаходження підозрілих пристроїв, аналізуючи силу сигналу на різних точках спостереження. Це можна реалізувати через синхронізовані вузли, які передаватимуть дані до центрального сервера для обробки. Додатково можна використовувати алгоритми триангуляції, що допоможуть визначати напрямок та місце розташування нелегітимного пристрою. Це дозволить швидко локалізувати загрозу передавши точну інформацію охоронній службі для оперативного реагування без витрачання часу на місцезнаходження порушника.

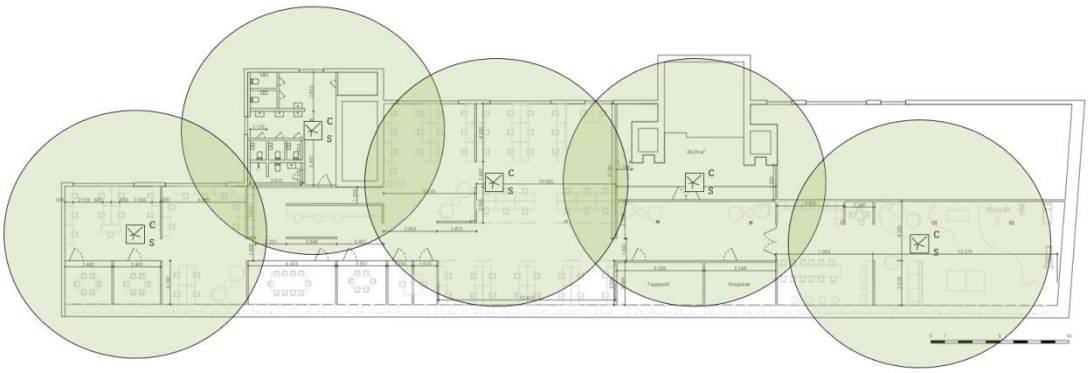

Рисунок 1 – Приклад план-схеми розташування охоронної сигналізації на базі Wi-Fi сканера

Під час тестування такої системи використовувалися 15 різних пристроїв, що мають доступ до Wi-Fi, серед яких 8 – знаходяться у «вайт-листі», інші 7 – потенційні порушники. Розташування Wi-Fi сканерів на умовному об’єкті із мінімальний радіусом у 10 метрів обрано таким чином, щоб можливі місця для входу порушників (вікна, головний вхід) були у зоні досяжності сканеру, і при потраплянні у зону їхньої дії, сповіщення про пристрій порушника надходило до служби безпеки. Сканери розташовані з урахуванням можливого перекриття зон їхнього покриття, що дозволяє усунути «сліпі зони» та підвищити точність виявлення. Ті, що є легітимними, система виявила їхню присутність та не відреагувала на них. Щодо 7 пристроїв, що не знаходяться у «вайт-листі», то система прислала повідомлення до чату, що у зоні дії сканеру знаходиться незареєстрований пристрій (ймовірний порушник).