*DOI: https://doi.org/10.36059/978-966-397-308-1-31*

# ПОСИЛЕННЯ БЕЗПЕКИ ЛОКАЛЬНОЇ МЕРЕЖІ IOT З ВИКОРИСТАННЯМ ПРИСТРОЇВ MERAKI

**Скопень Микола Максимович**
*кандидат економічних наук, доцент,*
*викладач-методист кафедри*
*загальнотеоретичної та прикладної підготовки*
*Київського фахового коледжу туризму та готельного господарства*
**Будя Олександр Петрович**
*кандидат технічних наук доцент,*
*викладач-методист кафедри*
*загальнотеоретичної та прикладної підготовки*
*Київського фахового коледжу туризму та готельного господарства*

У відомих літературних джерелах достатньо добре розглянуто загальні принципи організації та моделювання мереж, архітектура та налаштування керування пристроями Інтернету речей (Internet of Things, IoT) [1 та ін.]. Деякі джерела розкривають технології посилення безпеки бездротових мереж шляхом підключення пристроїв Meraki до дротових [2] та бездротових мереж (Wireless Local Area Network, WLAN) [3]. Однак, аналіз видань свідчить про відсутність розкриття технології посилення безпеки шляхом дистанційної організації захисту WLAN IoT на платформі пристроїв Meraki. Саме ця технологія і пропонується авторами нижче для розгляду.

Слід зауважити, що пристрої Meraki розробляються IT-компанією Cisco-Meraki (м. Сан-Франциско, штат Каліфорнія) для посилення безпеки бездротових мереж, поліпшення їх структуризації та забезпечення можливості віддаленого адміністрування за допомогою хмарних технологій.

Припустимо, що треба побудувати локальну мережу IoT системи спостереження за рухом навколо будинку та організувати віддалено її захист. В даному випадку порядок дій буде складатися з наступних етапів:

– побудова топології системи спостереження (рис. 1);

– налаштування роутера для забезпечення зв’язку пристрою безпеки Meraki-MX65W з Meraki – сервером;

– налаштування параметрів пристрою безпеки Meraki-MX65W;

– налаштування через хмарний сервер Meraki бездротового зв’язку користувачів та шифрування даних;

– підключення пристроїв IoT та програмування дій при спостеріганні за рухом навколо будинку.

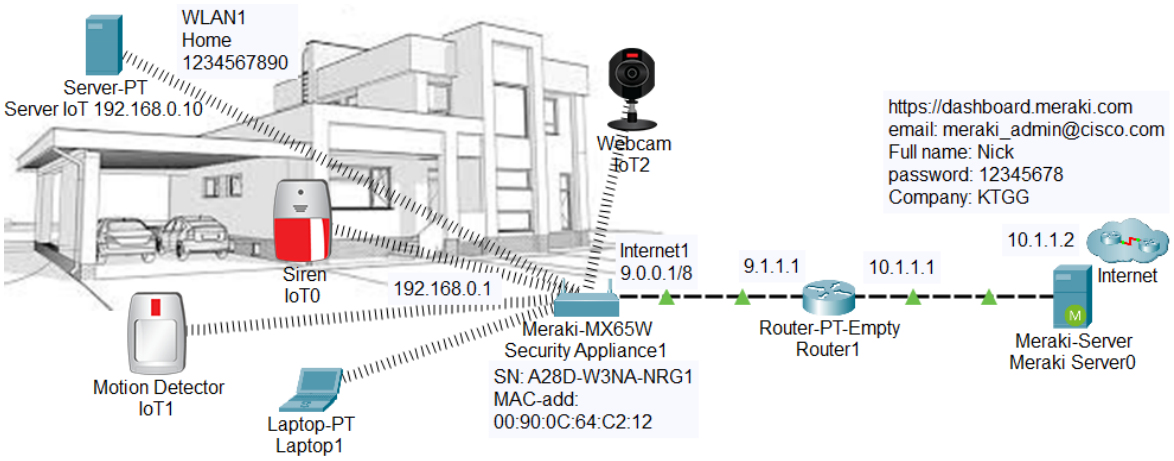


**Рис. 1. Топологія WLAN з пристроями IoT на базі Meraki-MX65W з віддаленим адмініструванням на Meraki - сервері**

Побудова топології системи спостереження на базі Meraki-MX65W з віддаленим адмініструванням за допомогою Meraki – сервера передбачає:

– встановлення Meraki – сервера та налаштування його IP-конфігурації: IPv4 Address – 10.1.1.2, Subnet Mask – 255.0.0.0, Default Gateway – 10.1.1.1, DNS Server – 10.1.1.2;

– встановлення роутера з двома мережевими картами PT-ROUTER-NM-1CGE (Cisco Gigabit Ethernet Network Module) і налаштування його IP-конфігурації: шлюз GigabitEthernet0/0 – IPv4 Address – 10.1.1.1, Subnet Mask – 255.0.0.0; шлюз GigabitEthernet1/0 – IPv4 Address – 9.1.1.1, Subnet Mask – 255.0.0.0. З′єднання роутера кросовером з Meraki – сервером (порт Gig0/0) та Meraki-MX65W (встановлення POWER-ADAPTER і підключення до порту Internet1);

– встановлення серверу IoT з мережевою картою WMP300N та увімкненими режимами: DHCP (вкладка Desktop / IP Configuration) для підключення до пристрою безпеки; IoT (вкладка Services) для аутентифікації пристроїв IoT. Створення аккаунту на сервері (вкладка Desktop), тобто введення 192.168.0.10 у вікно Web Browser і натискання Sign up now. Далі введення у вікно Registration Server Account Creation: admin, admin і натискання кнопки Create. Встановлення Laptop та пристроїв IoT: Siren, Motion Detector, Webcam.

**Налаштування роутера** – це запуск служби DHCP (Dynamic Host Configuration Protocol) для встановлення IP-адреси порту Internet1 пристрою безпеки WLAN1 – 9.0.0.1. В даному випадку підключені вузли (Laptop, Server, пристрої IoT) будуть мати зв’язок з Meraki – сервером. Для цього треба відкрити роутер і на вкладці CLI (Command Line Interface) ввести програмний код:

– Router(config)#ip dhcp pool Nic;

– Router(dhcp-config)#network 9.0.0.0 255.0.0.0;

- Router(dhcp-config)#default-router 9.1.1.1;
- Router(dhcp-config)#dns-server 10.1.1.2.

Для налаштування параметрів пристрою безпеки Meraki-MX65W (WLAN1) треба встановити Laptop з адаптером бездротової мережі Linksys-WPC300N і за допомогою вкладок Desktop / IP Configuration увімкнути режим DHCP для отримання параметрів (в даному прикладі): IPv4 Address – 192.168.0.6, Subnet Mask – 255. 255. 255.0, Default Gateway – 192.168.0.1, DNS Server – 10.1.1.2. Фіксуємо на вкладці Config серійний номер пристрою, наприклад, A28D-W3NA-NRG1. Далі відкриваємо вкладку Desktop на Laptop і у вікно Web Browser вводиться IP-адреса 192.168.0.1 WLAN пристрою безпеки, а у поле User Name – серійний номер. При відкритті пристрою на вкладці Connection фіксуємо MAC-адресу пристрою для подальшої реєстрації на Meraki – сервері, наприклад: Hardware address 00:90:0C:64:C2:12, а на вкладці Configure для Internet1 вибираємо у списку режим: IP assignment – DHCP та натискуємо нижче кнопку Save.

Для налаштування через хмарний сервер Meraki бездротового зв′язку користувачів та шифрування даних у вікні Web Browser Laptop вводиться https://dashboard.meraki.com, а при відкритті сервера, натискається Create an account для реєстрації. При цьому і діалогове вікно вводяться, наприклад, наступні параметри: Email: meraki_admin@cisco.com; Full name: Nick; Password: 12345678; Confirm Password: 12345678; Company: KTGG. Натискається кнопка Create Account. Далі з метою створення мережі WLAN1 та реєстрації пристрою безпеки натискається вгорі посилання here (тут) і ліворуч – Create a network. У поле Network name вводиться WLAN1 і натискається кнопка Create network. Нижче у відповідні поля вводяться параметри реєстрації пристрою безпеки (серійний номер, MAC-адреса, назва мережі) та натискається кнопка Add devices. Якщо натиснути ліворуч посилання Security Appliance / Appliance Status / Uplink, тоді можна побачити стан та конфігурацію інтерфейсу Інтернет порту пристрою безпеки.

За посиланням Security Appliance / Appliance Setting здійснюється шифрування доступу вузлів до WLAN1, тобто встановлення параметрів: Status – Enabled, SSID Name – Home, Security – WPA2 PSK, WPA Key – 1234567890, WPA encryption mode – WPA2 only. Натискається кнопка Save Changes. Після цього можна до WLAN1 підключати до 50 вузлів.

Підключення пристроїв IoT та програмування дій при спостеріганні за рухом навколо будинку. Для цього спочатку відкривається Motion Detector, активізується вкладка Config / Wireless0 і у поле SSID вводиться: Home. Далі встановлюється перемикач WPA2-PSK і у вікно PSK Pass Phrase вводиться ключ 1234567890 шифрування. На вкладці Config/Setting встановлюється перемикач Remote Server, Server Address – 192.168.0.10, User Name – admin і Password – admin. Натискається кнопка

Connect (при успішній реєстрації на сервері перетворюється на Refresh). В даному випадку сенсор буде підключено до пристрою безпеки та отримає в режимі DHCP IP-адресу, а також буде зареєстрований на сервері IoT. Аналогічним чином налаштовуються пристрої Siren та Webcam. Для Laptop задається лише SSID та ключ шифрування.

Для програмування дій при спостеріганні за рухом навколо будинку активізується на сервері або Laptop режим IoT Monitor та вкладка Conditions, натискається кнопка Add і задається режим спрацювання Siren та Webcam. В даному випадку програмується модуль Motion_On (рис. 2).

Після безпомилкового виконання налаштування параметрів на Meraki-MX65W Security Appliance та Meraki-сервері буде забезпечено успішне підключення IoT та контроль їх працездатності.

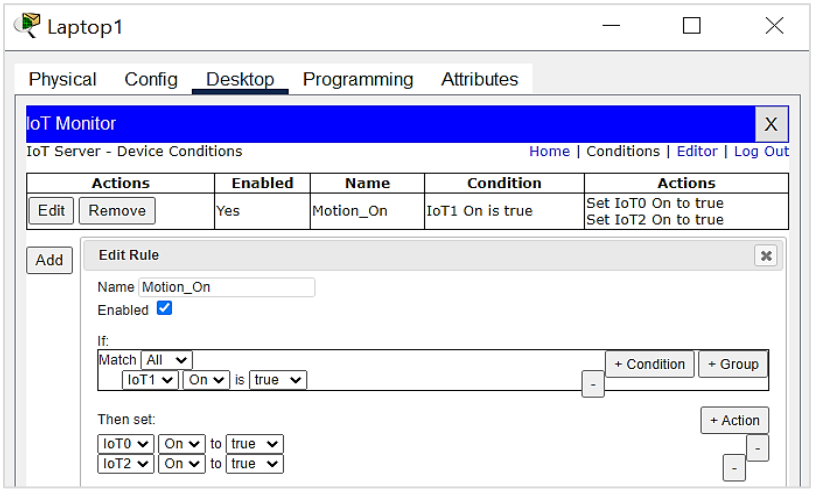


**Рис. 2. Програмування реакції Siren та Webcam на спрацювання Motion Detector**

Отже, запропонована технологія побудови та захисту бездротових мереж з використанням пристроїв Meraki дозволяє вирішити питання посилення безпеки WLAN IoT. Представлену технологію можна рекомендувати для використання в навчальному процесі, а також моделювання мереж на стадії проектування.

## Список використаних джерел:

1. Ли Перри. Архитектура интернета вещей / пер. с англ. Райтмана М.А. Москва : ДМК Пресс, 2019. 454 с. URL: http://surl.li/gzijz (дата звернення: 12.05.2023).

2. Налагодження та дослідження роботи CISCO MERAKI. URL: http://surl.li/fvmsb (дата звернення: 12.05.2023).

3. Скопень М.М., Будя О.П., Стародуб О. П. Особливості побудови та захисту бездротових мереж з використанням пристроїв Meraki. Матеріали Міжнародної науково-практичної конференції "Трансформаційні процеси національної економіки в умовах сьогодення" (м. Київ, 8 квітня 2023 р.). Львів-Торунь : Liha-Pres, 2023. С. 133–138. URL: http://surl.li/gpkcg (дата звернення: 12.05.2023).