

УДК 004.75

Н.В. Гавриляк¹, А.Б Бик¹, В.П. Павлюс²¹*Тернопільський національний економічний університет*²*Галицький коледж ім. В. Чорновола***МЕРЕЖЕВИЙ ШЛЮЗ ІНТЕРНЕТ РЕЧЕЙ НА ОСНОВІ
ОДНОПЛАТНОГО КОМП'ЮТЕРА**

Вступ. У зв'язку з широким впровадженням інформаційних систем у різні галузі економіки захист інформації, яка передається та обробляється у даних системах є актуальним та важливим завданням. Враховуючи той факт, що офіси багатьох компаній є географічно розподілені, захищена передача даним має надзвичайно важливе значення. Для вирішення вказаного завдання використовують технологію VPN (Virtual Private Network – віртуальна приватна мережа). VPN розширює приватну мережу через загальнодоступну мережу та дає можливість користувачам надсилати та отримувати дані через загальнодоступні мережі, так якби їхні обчислювальні пристрої були безпосередньо підключені до приватної мережі.

Завдяки VPN, підключеному до маршрутизатора, можна створити захищене зашифроване з'єднання з будь-якої точки світу до своєї домашньої мережі. Це має ряд переваг, таких як можливість доступу до файлів у своєму NAS без будь-якої чіткої конфігурації, або коли з'єднання зашифровано, можливість використовувати свій ноутбук на загальнодоступній точці Wi-Fi, не переймаючись тим, хто перехопить дані, які передаються. Найкраще, контролювати все, і можна бути впевненим, що наші дані повністю безпечні і що ми не покладаємось ні на які інші послуги [1].

З розвитком технології Інтернет – речей (IoT - Internet of Things) виникає гостра проблема безпечного підключення десятків пристроїв IoT до мережі Інтернет. Враховуючи, що IoT використовують різні інтерфейси та протоколи передачі даних, доцільно для їх підключення до Інтернету використовувати спеціалізовані IoT - шлюзи. Великі компанії та корпорації пропонують широкий асортимент захищених мережеских шлюзів Інтернет речей, проте ціни на них стартують від 1000\$. Таким чином, розробка захищеного мережевого шлюзу на основі одноплатного

комп'ютера є актуальним завданням, яке дозволить значно здешевити його вартість [2].

Метою роботи є розробка захищеного мережевого шлюзу Інтернет речей на основі одноплатного комп'ютера.

1. Структура шлюзу Інтернет речей

Порівнявши характеристики найбільш популярних моделей мережевих IoT шлюзів можна зробити наступний висновок. Для того щоб мережевий шлюз Інтернет речей був здатен швидко виконати поставлене завдання він повинен бути обладнаний швидкісним процесором. Обчислювальні вузли доповнює оперативна пам'ять, яка може бути представлена у вигляді модуля на 2 чи 4 ГБ. Передача даних здійснюється за допомогою модулів введення / виведення. Система має підтримувати різні мережні стандарти, тому потрібні інтерфейси: порт RJ45 і роз'єм USB, I2C, UART та інші. Згідно з поставленим завданням, для реалізації захищеного мережевого шлюзу Інтернет речей вибрано одноплатний комп'ютер Raspberry Pi 3 model B від компанії Raspberry Pi Foundation [3].

Структура захищеного IoT шлюзу приведена на рисунку 1. Для забезпечення безперебійного живлення використаємо резервний акумулятор з інвертором напруги.

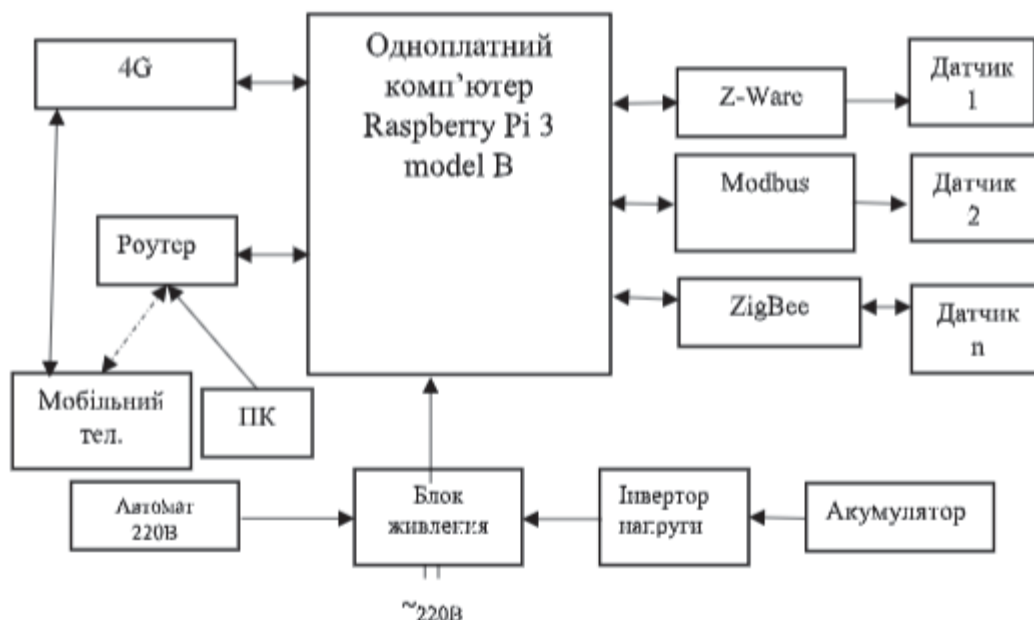


Рисунок 1 – Структура захищеного IoT - шлюзу

В якості програмного забезпечення з відкритим вихідним кодом використаємо OpenVPN. Для цього вводимо: `sudo apt-get install openvpn`. Підвищуємо свої привілеї до root: `sudo -i`. OpenVPN поставляється з Easy_RSA, легким і простим пакетом для використання методу

шифрування RSA. З Easy_RSA, запускаємо алгоритм, який поставляється разом з програмним забезпеченням для створення нового унікального ключа. Вводимо: `cp -r /usr/share/doc/ovpn/examples/easy-rsa/2.0/etc/ovpn/easy-rsa`. Редактор nano є вбудованим інструментом для редагування на Raspbian - `nano vars`. Міняємо змінну EASY_RSA на: `export EASY_RSA="/etc/ovpn/easy-rsa"`. Створюємо сертифікати CA Certificate і Root CA

Наступним кроком завантажуюємо файл конфігурації та встановлюємо OpenVPN: `cd /tmp && wget https://files.ovpn.com/raspbian/ovpn-se-gothenburg.zip && unzip ovpn-se-gothenburg.zip && mkdir -p /etc/ovpn && mv config/* /etc/ovpn && chmod +x /etc/ovpn/update-resolv-conf && rm -rf config && rm -f ovpn-se-gothenburg.zip` Вводимо дані для входу: `echo "CHANGE TO YOUR USERNAME" >> /etc/ovpn/credentials, echo "CHANGE TO YOUR PASSWORD" >> /etc/ovpn/credentials`. Запускаємо OpenVPN і дивимось чи все працює: `sudo ovpn --config /etc/ovpn/ovpn.conf --daemon`. Перевіряємо чи з'єднання було успішним, чекаємо приблизно хвилину після запуску останньої команди і набираємо: `curl https://www.ovpn.com/v2/api/client/ptr | python -m json.tool`.

В результаті отримуємо:

```
"status":true,"ip":"172.20.32.41","ptr":"cliXXX.ovpn.com"}
```

Розроблений IoT шлюз з можливістю організації захищеного з'єднання на основі OpenVPN може знайти ефективне застосування при проектуванні розумних будинків.

Висновки.

В роботі розроблено структуру мережевого шлюзу Інтернет речей на базі одноплатного комп'ютера, який забезпечує під'єднання до мережі Інтернет пристроїв з різними інтерфейсами, протоколами та каналами зв'язку.

Перелік джерел.

1. Сэмюэл Грингард. Интернет вещей: Будущее уже здесь. Издательство: Альпина Паблишер, 2011. –180 с.
2. Зараменских Е., Артемьев И. Интернет вещей. Исследования и область применения. – М: Инфра-М, 2016. — 188 с
3. Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 2. Modelling and Development /V.S. Kharchenko (ed.) - Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 547 p.