

АНАЛІЗ ВРАЗЛИВОСТЕЙ МОДУЛЯ МОНІТОРИНГУ СОНЯЧНОЇ ЕЛЕКТРОСТАНЦІЇ НА ОСНОВІ ДОСЛІДЖЕННЯ ПРОШИВКИ

М. О. Кіпер^{1,а}, В. В. Демчинський¹

¹ Навчально-науковий Фізико-технічний інститут

Анотація

У роботі розглянуто захищеність зовнішнього модуля моніторингу сонячної електростанції, який забезпечує передавання телеметрії від інвертора до хмарної платформи виробника. Такий модуль є проміжною ланкою між локальним енергетичним обладнанням, мережею користувача та зовнішнім сервісом, тому його компрометація може впливати на конфіденційність, цілісність і доступність даних моніторингу. На основі дослідження модуля Growatt Shine WiFi-F Pro та аналізу його мікропрограмного забезпечення визначено ключові ризики, пов'язані з мережевою взаємодією, локальними інтерфейсами, TLS-з'єднанням і механізмом OTA-оновлення.

Ключові слова: сонячна електростанція, сонячна енергетика, модуль моніторингу, Growatt Shine WiFi, OTA-оновлення, телеметрія.

Вступ

Поширення побутових і малих сонячних електростанцій (СЕС) підвищує вимоги до надійності та безпеки їх систем моніторингу. Зовнішні модулі моніторингу забезпечують збір даних про генерацію, споживання, стан акумуляторів і режими роботи інвертора, однак часто працюють через бездротові інтерфейси та хмарні платформи виробника.

Енергетична інфраструктура України зазнає систематичних руйнувань унаслідок масованих ракетних ударів, що зумовлює тривалі відключення електроенергії та дефіцит потужності. У відповідь домогосподарства та малий бізнес масово впроваджують децентралізовані джерела живлення — насамперед СЕС у поєднанні з акумуляторними системами та гібридними інверторами. Лише у 2024 році в Україні введено близько 800–850 МВт нових потужностей СЕС [1], що потребує ефективних і захищених рішень для моніторингу відповідного обладнання.

Описана архітектура є зручною для користувача, але створює додаткову поверхню атаки: вразливими компонентами є прошивка модуля, локальні інтерфейси, протоколи обміну з інвертором і канал передавання телеметрії. Ситуацію ускладнює те, що понад половину світового ринку інверторів контролюють китайські компанії, а хмарні сервіси моніторингу часто розміщені поза межами України. Дослідження підтверджують: найбільша частка вразливостей припадає на компоненти моніторингу та хмарні сервіси, а критичні вразливості можуть давати зловмиснику змогу отримати контроль над системою [2].

Метою роботи є оцінка захищеності зовнішнього модуля моніторингу СЕС на основі аналізу його мі-

сця в архітектурі системи, дослідження апаратної платформи та мікропрограмного забезпечення, а також формування моделі загроз і потенційних ризиків.

1. Архітектура системи моніторингу сонячної електростанції

Типова система моніторингу побутової СЕС має хмарно-орієнтовану архітектуру. Її основними компонентами є інвертор, зовнішній модуль моніторингу, локальна мережа, хмарна платформа та клієнтський інтерфейс. Інвертор виконує роль основного джерела телеметрії: він контролює параметри генерації, споживання, стан акумулятора, режими роботи та помилки обладнання.

Зовнішній модуль моніторингу є проміжною ланкою між інвертором і хмарию. Він підключається до інвертора через USB або RS-485, зчитує параметри за протоколом Modbus [3] і передає їх через Wi-Fi або Ethernet на сервер виробника. У низці реалізацій канал є двостороннім: команди керування можуть надходити від хмарного сервісу через модуль до інвертора.

З погляду кібербезпеки модуль моніторингу є мережевим шлюзом між локальним енергетичним обладнанням та Інтернетом. Він має власну прошивку, мережевий стек, механізм оновлення та локальні інтерфейси, а тому його компрометація створює ризики для конфіденційності, цілісності та доступності даних. За відсутності належної ізоляції він може стати також точкою входу до локальної мережі користувача. Узагальнену схему типової архітектури хмарного моніторингу СЕС наведено на рис. 1.

Отже, критичність модуля зумовлена тим, що він

^аmakskiper-ipt27@lil.kpi.ua

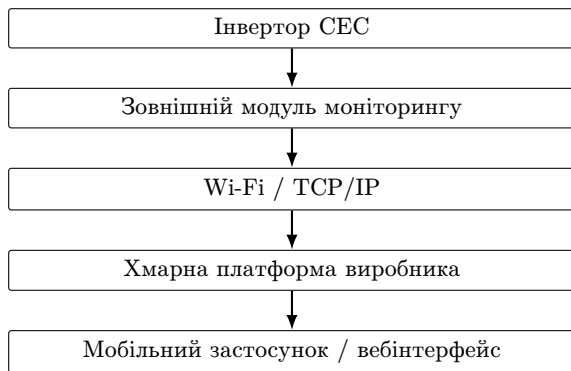


Рис. 1. Типова архітектура хмарного моніторингу СЕС.

одночасно взаємодіє з інвертором, локальною мережею та хмарним сервісом. Саме тому дослідження його програмно-апаратної структури та прошивки є необхідним етапом оцінки захищеності системи моніторингу СЕС.

2. Дослідження зовнішнього модуля моніторингу

Для дослідження було обрано зовнішній модуль моніторингу Growatt Shine WiFi-F Pro, який використовується для передавання телеметричних даних від інверторного обладнання до хмарної платформи виробника. Вибір цього пристрою зумовлений тим, що він є типовим прикладом зовнішнього телеметричного модуля для побутових і малих СЕС: підключається до інвертора, має власну мікропрограму, мережевий стек, механізм оновлення та забезпечує взаємодію між локальним енергетичним обладнанням і зовнішньою хмарною інфраструктурою. Зовнішній вигляд досліджуваного модуля показано на рис. 2.

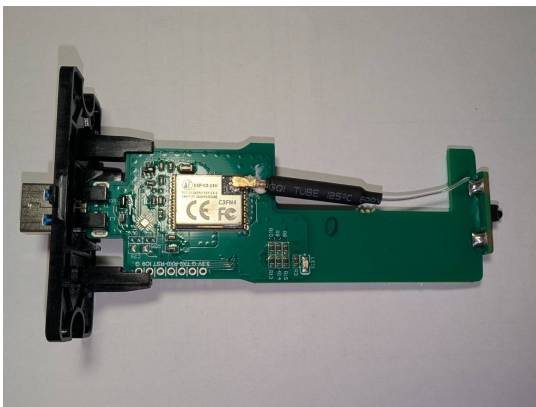


Рис. 2. Вигляд досліджуваного модуля Growatt Shine WiFi-F Pro.

Дослідження виконувалося у контрольованому лабораторному середовищі. На першому етапі було проведено зовнішній огляд модуля, розбирання корпусу та аналіз друкованої плати з метою ідентифікації основних апаратних компонентів. Особливу увагу приділено мікроконтролеру, flash-пам'яті, слу-

жбовим контактам, інтерфейсам налагодження та елементам, пов'язаним із живленням і мережевою взаємодією пристрою.

У результаті апаратного аналізу було встановлено, що досліджуваний модуль побудований на базі мікроконтролера сімейства ESP32-C3 та використовує flash-пам'ять обсягом 4 МБ. Така апаратна платформа є типовою для компактних IoT-пристроїв, оскільки поєднує підтримку Wi-Fi, низьке енергоспоживання та достатні ресурси для виконання мережевих і телеметричних функцій [4].

Для отримання мікропрограмного забезпечення було використано службовий послідовний інтерфейс пристрою. Підключення виконувалося за допомогою USB-UART адаптера з логічним рівнем 3,3 В. Після ідентифікації необхідних службових контактів модуль було переведено в режим завантажувача, що дало змогу отримати повний образ flash-пам'яті для подальшого аналізу.

Аналіз образу прошивки дав змогу встановити наявність типових для ESP-IDF компонентів: FreeRTOS, мережевого стека, MbedTLS, BLE-підсистеми, MQTT-клієнта, NVS-сховища та FOTA-механізму оновлення. Також виявлено, що прикладна взаємодія з хмарним сервісом пов'язана з передаванням телеметрії та обробкою команд через мережевий протокол, а частина локального налаштування виконується через бездротові інтерфейси.

3. Модель загроз і потенційні ризики

Модель загроз для зовнішнього модуля моніторингу охоплює три основні сценарії. Перший пов'язаний із локальним порушником, який має доступ до мережі користувача та може впливати на мережеву взаємодію пристрою. Другий передбачає фізичний доступ до модуля, наприклад під час ремонту, перепродажу або неналежного зберігання. Третій пов'язаний із хмарним контуром, коли ризики виникають через залежність від зовнішнього сервісу виробника та двосторонній канал взаємодії з інвертором.

За результатами аналізу прошивки встановлено декілька груп потенційних ризиків. Найкритичнішою є група, пов'язана із захистом каналу передавання даних між модулем і хмарним сервісом та з оновленням мікропрограмного забезпечення. Якщо пристрій некоректно перевіряє TLS-сертифікат або продовжує роботу після помилки верифікації, зростає ризик перехоплення або підміни мережевої взаємодії. Якщо ОТА-оновлення перевіряє лише контрольну суму, але не цифровий підпис образу, контроль цілісності не гарантує автентичність прошивки. Такі проблеми відповідають типовим категоріям небезпечного оновлення та недостатньої перевірки довіри в IoT-пристроях [5, 6]. Зведення основних потенційних ризиків та їх рівнів критичності наведено в табл. 1.

Окремим ризиком є те, що користувач часто сприймає дані мобільного застосунку як єдине достовірне джерело інформації про стан СЕС. Тому атака на канал моніторингу може бути небезпечною навіть без прямої зміни фізичних режимів роботи інверто-

Таблиця 1. Основні потенційні ризики зовнішнього модуля моніторингу сонячної електростанції.

Компонент	Потенційний ризик	Можливий наслідок	Рівень
TLS-з'єднання	Некоректна перевірка сертифіката або продовження роботи після помилки верифікації	Перехоплення або підміна телеметрії та службових повідомлень	Критичний
OTA-оновлення	Відсутність криптографічної перевірки підпису образу прошивки	Встановлення модифікованого мікропрограмного забезпечення	Високий
BLE-налаштування	Використання спільних або недостатньо захищених параметрів автентифікації	Несанкціоноване локальне конфігурування пристрою	Високий
UART-інтерфейс	Виведення чутливих параметрів у службовий лог	Розкриття облікових даних мережі за фізичного доступу	Середній
Хмарний сервіс	Залежність від зовнішньої платформи та двостороннього каналу обміну	Втрата доступу до моніторингу або вплив на керування інвертором	Високий

ра: спотворена телеметрія або відсутність повідомлень про помилки ускладнюють своєчасне виявлення несправностей. Для зменшення ризиків доцільно застосовувати мережеву сегментацію, обмеження вихідних з'єднань, контроль оновлень через офіційні канали, локальне дублювання критичних показників і перевірку наявності криптографічного підпису прошивки.

Висновки

У роботі розглянуто зовнішній модуль моніторингу СЕС як критичну проміжну ланку між інвертором, локальною мережею користувача та хмарною платформою виробника. Показано, що модуль має власну прошивку, мережевий стек, локальні інтерфейси та механізм оновлення, тому його компрометація може впливати на достовірність телеметрії, доступність моніторингу та безпеку локального середовища.

Проведене дослідження модуля Growatt Shine WiFi-F Pro засвідчило доцільність аналізу не лише мережевої поведінки, а й мікропрограмного забезпечення. Найважливішими зонами ризику визначено TLS-взаємодію, OTA-оновлення, локальні інтерфейси налаштування та зберігання чутливих параметрів. Для зменшення ризиків рекомендовано застосовувати криптографічну перевірку прошивки, ізоляцію модуля в окремо-

му мережевому сегменті, контроль доступу до службових інтерфейсів і локальне дублювання телеметрії.

Перелік використаних джерел

1. Асоціація сонячної енергетики України. Аналітичний звіт: ринок сонячної генерації в Україні у 2024 році : тех. звіт. / ACEY. — Київ, 2025.
2. Bort J., Jones B. Security Analysis of Solar Inverter Cloud Ecosystems: Vulnerabilities in Monitoring Infrastructure // IEEE Transactions on Industrial Informatics. — 2024. — Vol. 20, no. 3. — P. 2315–2327.
3. Modbus Organization. MODBUS Application Protocol Specification. — Version 1.1b3. — 2012. — URL: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf.
4. Espressif Systems. ESP32-C3 Technical Reference Manual. — Version 1.3. — Shanghai, 2023.
5. OWASP Foundation. OWASP Internet of Things (IoT) Top 10 2018. — 2018. — URL: <https://owasp.org/www-project-internet-of-things/>.
6. National Institute of Standards and Technology. Platform Firmware Resiliency Guidelines : Special Publication / NIST. — 2018. — No. 800–193. — URL: <https://csrc.nist.gov/publications/detail/sp/800-193/final>.