

АНАЛІЗ ВРАЗЛИВОСТЕЙ ІОТ-ПРИСТРОЇВ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ. МЕТОДИ РИЗИК-МЕНЕДЖМЕНТУ ТА ЗАХИСТУ ДАНИХ

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Анотація

У доповіді представлено аналіз основних вразливостей ІоТ-пристроїв, що застосовуються в енергетичному секторі, а також розглянуто методи оцінки ризиків і заходи щодо захисту даних. Дослідження охоплює аналіз загроз, пов'язаних із несанкціонованим доступом, атаками типу Man-in-the-Middle, DoS-атаками та експлуатацією вразливостей програмного забезпечення. Запропоновано інтегрований підхід до ризик-менеджменту, який включає класифікацію вразливостей згідно з MITRE ATT&CK та CWE, застосування криптографічних протоколів, автентифікації та систем моніторингу мережевого трафіку. Результати дослідження дозволяють підвищити кібербезпеку енергетичної інфраструктури та забезпечити захист критичних даних.

Ключові слова: ІоТ, енергетика, вразливості, ризик-менеджмент, захист даних, кібербезпека.

Abstract

The report presents an analysis of the main vulnerabilities of IoT devices used in the energy sector, as well as risk assessment methods and data protection measures. The study covers the analysis of threats associated with unauthorized access, Man-in-the-Middle attacks, DoS attacks and exploitation of software vulnerabilities. An integrated approach to risk management is proposed, which includes vulnerability classification according to MITRE ATT&CK and CWE, the use of cryptographic protocols, authentication and network traffic monitoring systems. The results of the study allow to increase the cybersecurity of energy infrastructure and ensure the protection of critical data.

Keywords: IoT, energy, vulnerabilities, risk management, data protection, cybersecurity.

Вступ

В сучасному енергетичному секторі впровадження ІоТ-пристроїв стає ключовим чинником оптимізації процесів управління та моніторингу. Проте широке застосування цих технологій супроводжується низкою кіберзагроз, що можуть призвести до несанкціонованого доступу, спотворення даних або відмов у роботі систем. Актуальність проблеми зумовлена необхідністю впровадження ефективних заходів ризик-менеджменту, що дозволять мінімізувати потенційні збитки та забезпечити безперебійність роботи енергетичної інфраструктури.

Метою роботи є аналіз вразливостей ІоТ-пристроїв, що застосовуються в енергетичному секторі, з метою розробки ефективних методів ризик-менеджменту та заходів із захисту даних. Це дослідження спрямоване на визначення основних кіберзагроз та розробку рекомендацій щодо впровадження багаторівневих систем захисту, які підвищують стійкість критичної енергетичної інфраструктури до потенційних кібератак.

Результати дослідження

Проведено класифікацію вразливостей ІоТ-пристроїв у енергетичному секторі на основі стандартів MITRE ATT&CK та CWE, що дозволило виокремити основні вектори кібератак, зокрема атаки типу Man-in-the-Middle, DoS-атаки, підробку ідентифікаційних даних та експлуатацію вразливостей програмного забезпечення [1]. У таблиці 1 описана класифікація типових вразливостей ІоТ-пристроїв.

За результатами аналізу встановлено, що ІоТ-пристрої в енергетиці характеризуються низкою технічних і програмних недоліків. Серед них – недостатньо захищені канали передачі даних, слабкі методи автентифікації та відсутність сучасних алгоритмів шифрування, що створює можливості для несанкціонованого доступу та маніпуляцій з критичною інформацією [2].

Табл. 1. – Типові вразливості IoT-пристроїв згідно класифікації CWE (MITRE)

№ CWE	Назва уразливості	Опис у контексті IoT-пристроїв в енергетиці
CWE-319	Атаки типу Man-in-the-Middle	Перехоплення даних під час передачі між IoT-пристроєм та сервером, що може призвести до їх модифікації або несанкціонованого використання.
CWE-287	Підrobка ідентифікаційних даних	Фальсифікація або зміна ідентифікаційних даних пристроїв, що дозволяє зловмисникам видавати себе за легітимних користувачів і отримувати доступ до системи.
CWE-400	DoS-атаки	Атаки, спрямовані на перевантаження пристроїв або мережі шляхом надмірного споживання ресурсів, що може призвести до відмов у роботі систем або значного зниження їх ефективності.
CWE-119	Експлуатація вразливостей програмного забезпечення	Використання вразливостей, таких як переповнення буферу, що дозволяє зловмисникам виконувати довільний код або отримувати несанкціонований доступ до системи.
CWE-311	Недостатня безпека каналів передачі даних	Відсутність належного шифрування або використання незахищених протоколів передачі даних, що створює можливість перехоплення або модифікації інформації під час комунікації пристроїв.

Розроблено інтегрований підхід до оцінки ризиків, який поєднує кількісні та якісні методи аналізу. Моделювання сценаріїв потенційних кібератак дозволило визначити критичні точки в енергетичній інфраструктурі та сформувати матрицю ризиків, що є основою для подальшого впровадження заходів захисту. Матрицю оцінки ризиків описано у таблиці 2.

На основі отриманих даних запропоновано комплекс заходів із захисту інформації, який включає використання сучасних криптографічних протоколів, впровадження багаторівневих систем автентифікації та застосування технологій VPN для забезпечення захищеної передачі даних. Також рекомендовано інтеграцію систем постійного моніторингу мережевого трафіку для оперативного виявлення аномальної активності [3].

Табл. 2. – Матриця оцінки ризиків IoT-пристроїв в енергетичному секторі

Опис ризику	Ймовірність	Вплив	Рівень ризику	Заходи мінімізації
Атаки типу Man-in-the-Middle	Висока	Високий	Високий	Використання VPN, шифрування, сучасних протоколів безпеки, моніторинг мережі
Підrobка ідентифікаційних даних	Середня	Середній	Середній	Багаторівнева автентифікація, застосування цифрових підписів, контроль доступу
DoS-атаки	Середня	Високий	Високий	Фільтрація трафіку, налаштування систем моніторингу та розподілу навантаження
Експлуатація вразливостей програмного забезпечення	Висока	Високий	Високий	Регулярне оновлення програмного забезпечення, аудит безпеки, впровадження IDS
Недостатня безпека каналів передачі даних	Середня	Середній	Середній	Використання шифрованих каналів, впровадження VPN, модернізація мережевого обладнання

Застосування запропонованих підходів сприяє значному підвищенню стійкості критичної енергетичної інфраструктури до кібератак, зменшуючи ймовірність несанкціонованого доступу до даних та спотворення інформації. Отримані результати відкривають перспективи для розробки адаптивних систем автоматичного реагування на інциденти та подальшого удосконалення методів ризик-менеджменту в IoT-середовищі [4].

Додатково, інтеграція комплексних механізмів захисту з ефективними системами моніторингу дозволяє оптимізувати витрати на кібербезпеку за рахунок своєчасного виявлення критичних точок та впровадження превентивних заходів. Це забезпечує не лише високий рівень захисту, але й сприяє підвищенню операційної ефективності, що в умовах швидкого розвитку IoT-технологій є важливим фактором конкурентоспроможності енергетичного сектору

Висновки

Проведений аналіз вразливостей IoT-пристроїв у енергетичному секторі дозволяє чітко виокремити основні напрямки кібератак, зокрема атаки типу Man-in-the-Middle, DoS-атаки, підrobку ідентифікаційних даних, експлуатацію вразливостей програмного забезпечення та недостатню безпеку каналів передачі даних. Розроблена схема оцінки ризиків, яка ґрунтується на класифікації вразливостей за стандартами MITRE ATT&CK та CWE, сприяє формуванню ефективних методів ризик-менеджменту та впровадженню заходів із захисту даних.

Запропонований підхід, що включає використання сучасних криптографічних протоколів, багаторівневих систем автентифікації та постійний моніторинг мережевого трафіку, дозволяє суттєво знизити ймовірність несанкціонованого доступу до критичної інформації та спотворення даних. Подальші дослідження мають бути спрямовані на розробку адаптивних систем автоматичного реагування на інциденти, що забезпечить оперативне виявлення та нейтралізацію кібератак у динамічному середовищі IoT, тим самим підвищуючи стійкість енергетичної інфраструктури до сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. MITRE ATT&CK. [Електронний ресурс]. URL: <https://attack.mitre.org>
2. CWE – Common Weakness Enumeration. [Електронний ресурс]. URL: <https://cwe.mitre.org>
3. NIST (2010). Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid. National Institute of Standards and Technology.
4. IoT Analytics (2024). Smart Electricity Meter Market 2024: Global Adoption Landscape. [Електронний ресурс]. URL: <http://iot-analytics.com>

Буняк Віталій Михайлович — студент групи 125-23а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vetalbunjak@gmail.com

Лукічов Віталій Володимирович — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Buniak Vitalii M. — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : vetalbunjak@gmail.com

Lukichov Vitalii V. — Cand. Sc. (Eng), Assistant Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia