УДК 004.738

Н. О. Черневський

КОНЦЕПЦІЯ НУЛЬОВОЇ ДОВІРИ В АРХІТЕКТУРІ ПОБУТОВИХ IOT-МЕРЕЖ

Вінницький Національний Технічний Університет

Анотація

У роботі проаналізовано проблематику захисту домашніх мереж, насичених пристроями Інтернету речей. Розкрито недоліки класичного периметрального захисту та запропоновано перехід до архітектури Zero Trust. Детально пояснено принципи мікросегментації мережі та криптографічної перевірки пристроїв. Описано методи адаптації цих складних технологій для бюджетних побутових контролерів через обмеження прав доступу.

Ключові слова: *IoT, Zero Trust, мікросегментація, VLAN, кібербезпека*.

Abstract

The paper analyzes the issues of protecting home networks saturated with Internet of Things (IoT) devices. The shortcomings of classic perimeter defense are revealed, and a transition to Zero Trust Architecture is proposed. The principles of network micro-segmentation and cryptographic device verification are explained in detail. Methods for adapting these complex technologies for budget household controllers through access rights restrictions are described.

Keywords: IoT, Zero Trust, micro-segmentation, VLAN, cybersecurity.

Вступ

Традиційний підхід до кібербезпеки часто порівнюють із середньовічною фортецею, є товсті стіни і безпечний внутрішній двір. У комп'ютерних мережах роль стін виконує маршрутизатор із брандмауером, який відділяє домашню мережу (LAN) від небезпечного Інтернету (WAN). Ця модель чудово працювала, коли вдома були лише комп'ютери та телефони. Проте в епоху Інтернету речей ця концепція працює неефективно. Сучасний будинок наповнений дешевими розумними пристроями: лампами, розетками, камерами, чайниками. Виробники часто економлять на безпеці цих гаджетів, залишаючи в них вразливості. Як наслідок, зловмиснику достатньо зламати одну слабку лампочку, щоб опинитися всередині вашої «фортеці». Опинившись там, він може вільно атакувати незахищені зсередини комп'ютери, красти дані з мережевих сховищ або перехоплювати відео з камер. Концепція Zero Trust пропонує радикальне рішення — сам факт підключення до домашньої мережі більше не робить пристрій «своїми» і безпечним.

Технічна реалізація

Поділ мережі та перевірка паспортів В основі Zero Trust лежить відмова від автоматичної довіри. На практиці це реалізується через два головні механізми. Перший це мікросегментація. Замість того, щоб всі пристрої бачили»один одного в єдиній мережі, ми розділяємо їх на ізольовані віртуальні підмережі (VLAN). Наприклад:

- сегмент А: камери відеоспостереження (не мають доступу до Інтернету, пишуть тільки на сервер);
- сегмент Б: розумні колонки та телевізори (мають доступ до стрімінгових сервісів);
- сегмент В: критичні пристрої (сервер опалення, сигналізація).

Взаємодія між цими сегментами дозволена тільки через суворий контроль шлюзу безпеки. Якщо хакер зламає розетку в Сегменті Б, він залишиться заблокованим у цій віртуальній кімнаті і не зможе дістатися до сервера опалення в Сегменті В.

Другий компонент це сувора автентифікація. Старі мережі розпізнавали пристрої за IP або MAC-адресою, але їх дуже легко підробити. Zero Trust вимагає використання криптографічних сертифікатів. Сучасний стандарт Matter використовує технологію блокчейн для атестації пристроїв. Система точно знає, що команда надійшла від сертифікованого контролера власника, а не від ноутбука зловмисника, який підробив адресу.

Виклики впровадження

Головна проблема впровадження Zero Trust у побуті це слабке залізо. Більшість датчиків працюють на простих мікроконтролерах (наприклад, ESP32 або старих ARM), які не мають потужності для постійного складного шифрування та перевірки сертифікатів без затримок у роботі. Інженерним компромісом у такій ситуації стає політика найменших привілеїв (Least Privilege). Ми налаштовуємо мережевий шлюз так, щоб дозволяти пристрою робити лише те, що йому критично необхідно для роботи, і нічого більше. Приклад: датчик температури повинен лише відправляти цифри на один конкретний сервер і на один конкретний порт. Якщо цей датчик раптом спробує завантажити щось з невідомого сайту або просканувати сусідній комп'ютер шлюз миттєво заблокує його. Це не вимагає від датчика потужного процесора, але надійно захищає мережу.

Висновки

Аналіз показує, що стара модель захищеного периметра вичерпала себе. В умовах, коли у квартирі можуть бути десятки підключених до Інтернету пристроїв сумнівної надійності, єдиним виходом є архітектура Zero Trust. Зміщуючи фокус захисту з вхідного роутера на контроль кожного окремого пристрою, сегментацію мережі та обмеження прав доступу, ми можемо створити систему, яка залишиться безпечною навіть якщо один з її елементів буде зламано.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Zero Trust deployment for technology pillars overview URL: https://learn.microsoft.com/en-us/security/zero-trust/deploy/overview (дата звернення: 14.01.2026).

2. Zero Trust security | What is a Zero Trust network? URL: https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/ (дата звернення: 14.01.2026).

3. Cisco Security Products for the IoT URL: https://www.cisco.com/c/en_ca/solutions/internet-of-things/iot-security.html (дата звернення: 14.01.2026).

4. Zero Trust IoT Security: Implementation Guide for Enterprise Networks URL: https://deviceauthority.com/zero-trust-iot-security-implementation-guide-for-enterprise-networks/ (дата звернення: 14.01.2026).

Черневський Назар Олександрович — студент групи 2КІ-25м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький Національний Технічний Університет, Вінниця, e-mail: chernevskijnazar@gmail.com

Chernevskyi Nazar Oleksandrovich — student of group 2KI-25m, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: chernevskijnazar@gmail.com