УДК 681.5:004.056

РОЗРОБКА АРХІТЕКТУРИ РЕЗЕРВНОГО КОПІЮВАННЯ АСУ ТП НА БАЗІ ZERO TRUST

Кремзуков О.В.
e-mail: oleksandr.kremzukov@nure.ua
Науковий керівник – к.т.н., доц. Сичова О.В.
Харківський національний університет радіоелектроніки, каф. КІТАРБІ
м. Харків, Україна

This paper explores the critical safety vulnerabilities of traditional backup systems in Industrial Control Systems (ICS). Given the growing risks of targeted sabotage, ensuring the continuity of technological operations is paramount. To address these enterprise risk management challenges, this study argues for the implementation of Zero Trust principles in data backup. A conceptual, cost-effective push-based architecture utilizing open-source tools is proposed to guarantee the survival of telemetry and control data, ensuring resilient operation even under complete network compromise.

В умовах стрімкої цифровізації промислові мережі та автоматизовані системи управління технологічними процесами (АСУ ТП) є основою безпечного функціонування сучасного підприємства [1, 2]. Втрата контролю над SCADA-системами або знищення баз даних телеметрії через деструктивні кібератаки може призвести до техногенних аварій, зупинки виробничих ліній та руйнування ланцюжків постачання. Традиційні корпоративні рішення для резервного копіювання, наприклад Bareos, демонструють критичну вразливість. Використання архітектури з акцентом на модель «pull» створює єдину точку відмови. З іншого боку, якщо скомпрометовано сам сервер АСУ ТП, традиційні системи часто залишають йому двосторонній доступ до сховища, дозволяючи зловмиснику знищити власні архіви.

Побудова стійкої системи вимагає ретельного проєктування архітектури на базі принципів Zero Trust (нульова довіра), яка припускає, що будь-який елемент системи може бути скомпрометований. Ключовими принципами є сегрегація повноважень та надання мінімально необхідних привілеїв [3]. Жоден компонент не має повного контролю над усім життєвим циклом архівів. Запропонована система логічно розділена на чотири ізольовані складові, що взаємодіють за допомогою Open Source інструментів (рис. 1).

Виробничий сервер АСУ ТП (джерело) створює зашифровані знімки за допомогою клієнта Restic і відправляє їх до сховища за моделлю «push». Використовується обліковий запис із правами «тільки на дозапис» (append-only). Сервер фізично не здатний модифікувати чи видалити дані, що гарантує їх виживання навіть у разі отримання хакером прав root. Сховище резервних копій (наприклад, SFTP-сервер) налаштоване для надання різних

рівнів доступу. Сервер моніторингу Zabbix працює в окремому середовищі і підключається до сховища з правами «тільки для читання» для перевірки цілісності (restic check). Щоб Zabbix не став вектором атаки, перевірки виконуються локальним планувальником (cron) цільового сервера, а агент лише зчитує вивід, не маючи прав на віддалені команди. Очищення застарілих копій виконується виключно з ізольованого хоста-бастіону через SSH з обов'язковим апаратним токеном (YubiKey), повністю відокремлюючи деструктивні операції від автоматики.

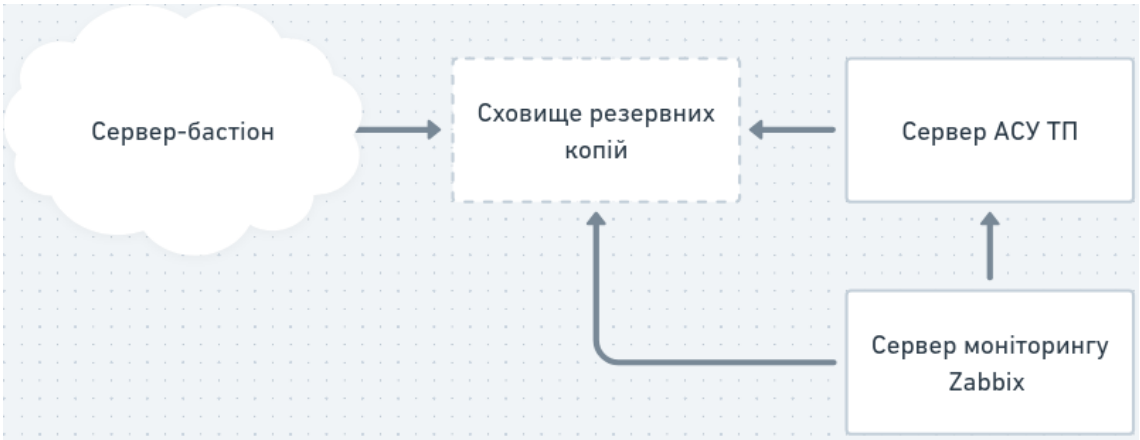

Рисунок 1 – Загальна схема взаємодії між компонентами системи резервного копіювання

Таким чином, розроблена архітектура реалізує принципи Zero Trust, створюючи багатоешелоновану систему захисту. Такий підхід апаратними та програмними засобами ізолює бекапи від основного середовища та мінімізує ризики безповоротної втрати контролю над виробництвом під час кібератак.

Список використаних джерел:

1. Невлюдов І. Ш. Промислові мережі та компоненти АСУТП : Навчальний посібник / І. Ш. Невлюдов, С. П. Новоселов, О. В. Сичова, С. І. Теслюк. – Харків: Видавництво Іванченка І. С., 2025 . – 241 с. ISBN 978-617-8332-83-9. doi: 10.30837/978-617-8332-83-9.

2. Невлюдов І. Ш. Node-RED та технологія промислового Інтернету речей : Навчальний посібник / І. Ш. Невлюдов, С. П. Новоселов, О. В. Сичова. – Харків: Видавництво Іванченка І. С., 2024. – 207 с. doi: 10.30837/978-617-8332-58-7.

3. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg : National Institute of Standards and Technology, 2020. 50 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (дата звернення: 06.03.2026).