2. Palaniappan R., Sundaraj K., Ahamed N., Arjunan A., Sundaraj S., Computer-Based Respiratory Sound Analysis: A Systematic Review. IETE Technical Review. 33. (2013). 248-256. 10.4103/0256-4602.113524.

УДК 004.056.5:378.147
В.С. Пиж, ст.гр. СБмд-61
(Тернопільський національний технічний університет, імені Івана Пулюя, Україна)

ІННОВАЦІЙНИЙ ПІДХІД ДО ПОБУДОВИ ЗАХИЩЕНОГО ВІРТУАЛЬНОГО СЕРЕДОВИЩА ДЛЯ ОСВІТНЬОГО ПРОЦЕСУ

V. S. Pyzh, st. gr. SBmd-61

INNOVATIVE APPROACH TO BUILDING A SECURE VIRTUAL ENVIRONMENT FOR THE EDUCATIONAL PROCESS

Стрімка цифровізація освіти вимагає нових підходів до створення безпечних віртуальних платформ, здатних підтримувати якісний навчальний процес. З огляду на зростання кіберризиків важливим є розроблення рішень, що поєднують інноваційні технології та ефективні механізми захисту. У роботі розглядається концепція побудови захищеного віртуального середовища, яке відповідає сучасним викликам та потребам учасників освітнього процесу.

Для побудови навчального середовища було обрано Proxmox Virtual Environment (PVE).

Proxmox Virtual Environment (PVE) є потужним рішенням Type 1 ("bare-metal") для віртуалізації, що базується на Debian Linux та поєднує KVM, LXC та функції кластеризації. Завдяки відкритому коду (GNU AGPLv3) та відсутності обов'язкових ліцензійних платежів , PVE ідеально підходить для малого та середнього бізнесу, освітніх установ та домашніх лабораторій, пропонуючи функціонал рівня Enterprise з обмеженим бюджетом.

Ключові перевагами та архітектурою Proxmox VE є настпне:

Proxmox VE об’єднує два типи віртуалізації в одному веб-інтерфейсі: KVM для повної апаратної віртуалізації будь-яких ОС і LXC для легких контейнерів Linux із мінімальними накладними витратами. Такий підхід дозволяє ефективно ізолювати сервіси та одночасно підтримувати широкий спектр операційних систем.

Система підтримує вбудовану кластеризацію та високу доступність (HA). Corosync синхронізує конфігурацію між вузлами, менеджер HA автоматично перезапускає критичні ВМ або контейнери у разі збою, а жива міграція забезпечує переміщення працюючих ВМ без простою.

Proxmox VE також пропонує гнучку роботу зі сховищами: ZFS забезпечує цілісність даних, миттєві знімки та управління дисковими пулами, а інтеграція з Ceph дозволяє створити розподілене відмовостійке сховище на базі локальних дисків усіх вузлів, замінюючи потребу у дорогому зовнішньому SAN.

Передбачається встановлення та налаштування Proxmox Virtual Environment (PVE).

Важливим в роботі є питання захисту та рекомендації (кроки), покликані зробити навчальне середовище максимально безпечним. В наступній таблиці приведені основні напрямки безпеки та описано їх вирішення

Таблиця 1. Ключові напрями та кроки забезпечення безпеки в середовищі Proxmox

Напрямок безпеки	**Ключові кроки**
Доступ по SSH	Вимкнути вхід для root. Використовувати автентифікацію на основі SSH-ключів. Застосувати Fail2ban проти брутфорсу.
Мережевий Екран	Увімкнути фаєрвол Proxmox. Встановити політику заборонити все за замовчуванням (deny-all) та додати винятки лише для необхідних портів (8006/TCP, SSH).
Автентифікація	Увімкнути 2FA (TOTP, WebAuthn) для всіх адміністративних облікових записів.
Управління Доступом (RBAC)	Уникати root для повсякденних завдань. Створювати окремі облікові записи з мінімально необхідними ролями та дозволами.
Оновлення та Моніторинг	Регулярно встановлювати оновлення безпеки. Перенаправляти системні журнали (syslog) на централізований сервер журналювання.
Резервні Копії	Використовувати клієнтське шифрування та незмінні резервні копії (immutable backups) через Proxmox Backup Server (PBS).
Веб-Інтерфейс	Замінити самопідписаний сертифікат на сертифікат від довіреного ЦС (наприклад, Let's Encrypt).

Забезпечення інформаційної безпеки у віртуалізованому середовищі Proxmox є одним із ключових етапів його впровадження в освітній або корпоративній інфраструктурі. Використання широкого набору вбудованих механізмів захисту дозволяє підвищити стійкість системи до зовнішніх та внутрішніх загроз. Основна увага приділяється організації автентифікації користувачів, зокрема впровадженню двофакторної автентифікації (2FA), що є обов’язковою умовою для адміністративних облікових записів, включаючи root@pam.

Важливою складовою є захист каналу віддаленого доступу, який передбачає зміну стандартного SSH-порту, відмову від використання паролів та дозвіл доступу виключно за SSH-ключами. Додатково рекомендується створення окремого користувача з правами sudo та повне відключення входу під обліковим записом root, що зменшує ризики експлуатації вразливостей.

Суттєве значення має налаштування вбудованого фаєрвола Proxmox на рівні датацентру, встановлення політики DROP за замовчуванням та дозвіл лише критично необхідних портів, включно з обмеженням доступу за визначеними IP-адресами. Для підвищення стійкості до brute-force атак впроваджується Fail2ban, який контролює активність на SSH та веб-інтерфейсі Proxmox, встановлюючи низькі ліміти на кількість спроб входу та подовжені періоди блокування.

Регулярний аудит системи забезпечується через використання інструментів rkhunter та Lynis, що дозволяють виявляти потенційні вразливості конфігурації та стежити за станом системної безпеки. Завершальним елементом комплексного підходу виступає продумана стратегія резервного копіювання, яка включає щотижневі повні та щоденні інкрементальні копії з визначеною політикою зберігання, що гарантує відновлюваність критичних даних та безперервність роботи інфраструктури.

Proxmox VE є повноцінною альтернативою комерційним гіпервізорам, лідируючи в ніші Open Source платформ. Його переваги — інтеграція KVM/LXC, безкоштовна кластеризація та відсутність Vendor Lock-in — роблять його ідеальним вибором для SMB, яким потрібна висока продуктивність, гнучкість і значна економія коштів.

Література

1. Alfaif, Aam Kholid, Puspanda Hatta, and Endar Suprih Wihidayat. "Performance Analysis of Proxmox and Virtualbox with Overhead and Linearity Parameters to Support Server Administration Practice." *Journal of Informatics and Vocational Education* 7, no. 2 (2024): 35–41. https://doi.org/10.20961/joive.v7i2.2399. URL: https://doi.org/10.20961/joive.v7i2.2399.
2. Ramdhani, Muhammad Dzikri, Muhammad Barez Sapado Siregar, Hilma Hayati, Riki Maulana, and Muhammad Febristo Robidullah. "Meningkatkan Efisiensi dan Skalabilitas Infrastruktur TI dengan Proxmox VE: Studi Kasus Implementasi dan Konfigurasi."*Karimah Tauhid* 3, no. 8 (2024): 8631–36. URL: http://dx.doi.org/10.30997/karimahtauhid.v3i8.14326.

УДК 656.098

О.Б Пйонтковський ст.групи ЕА-324
Науковий керівник: Недошитко Л.М., викладач-методист
(Відокремлений структурний підрозділ "Тернопільський фаховий коледж" Тернопільського національного технічного університету імені Івана Пулюя, Україна)

ЕНЕРГОЕФЕКТИВНІ МІКРОКОНТРОЛЕРИ ДЛЯ АВТОНОМНИХ ІОТ–ПРИСТРОЇВ

PiontkovskuyO.B. student of group EA-324
Scientific supervisor: Nedoshytko L.M., teacher-methodologist

ENERGY-EFFICIENTMICROCONTROLLERSFORAUTONOMOUSIOTDEVICES

Отже, що ж таке мікроконтролер для IoT? Це компактний малопотужний електронний пристрій, відомий як мікроконтролер для Інтернету речей, створений для управління зв’язаними пристроями та датчиками в системі Інтернету речей. Мікроконтролер діє як мозок пристроїв IoT, дозволяючи їм збирати дані про навколишнє середовище, обробляти їх та підключатися до інших пристроїв або систем IoT через мережу.

Найкращі енергоефективні мікроконтролери для автономних IoT-пристроїв — це STM32U5, ESP32-S3, Nordic nRF52 та RP2040. Вони поєднують низьке енергоспоживання з високою продуктивністю та безпекою.

Таблиця 1. Порівняльна характеристика мікроконтролерів

Модель	Ядро	Частота (МГц)	Пам’ять (Flesh/Ram)	Бездротові інтерфейси	Енерг-оспоживання	Особливості
STM32U5	ARM Cortex-M33	До 160	до 2MB / до 786KB	через зовнішні модулі	Наднизьке (Stop<1µA)	TrustZone, AES, USB, LCD, ADC
ESP32-S3	2× Xtensa LX7	До 240	до 8MB / до 512KB	Wi-Fi 4, BLE 5.0	DeepSleep ~20µA	AI підтримка, голос, камера
Nordic nRF52	ARM Cortex-M4	До 64	до 1MB / до 256KB	BLE 5.0, ANT, NFC	наднизьке (Sleep ~1µA)	BLE маячки, медичні пристрої
RP2040	2×	До 133	2MB	через	~1.5mA	Дешевий,