2. On the practical cost of Grover for AES key recovery. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/csrc/media /Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf.
3. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. [Електронний ресурс]. – Режим доступу: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.
4. Post-Quantum Cryptography: Anticipating Threats and Preparing the Future. [Електронний ресурс]. – Режим доступу:https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future.

Аналіз енергетичної доцільності впровадження малопотужних апаратних вузлів у віртуалізовані навчальні середовища з кібербезпеки

УДК 004.056:004.738

Онищук Гліб[1] , Сергій Бабич[2]

Національний університет водного господарства та природокористування, [1]onyshchuk_ak23@nuwm.edu.ua, [2]s.v.babych@nuwm.edu.ua

Навчальні процеси з кібербезпеки вимагають розгортання складних ізольованих середовищ для тестування вразливостей, моделювання кібератак та налаштування засобів захисту. Традиційна модель забезпечення лабораторій передбачає використання повноцінних потужних робочих станцій («товстих» клієнтів), обчислювальні ресурси яких більшу частину часу використовуються неефективно, а їх обслуговування є складним та вкрай енергозатратним процесом [1].

Дане дослідження присвячене аналізу енергетичної та економічної доцільності заміни традиційних персональних комп'ютерів на малопотужні апаратні вузли («тонкі» або «нульові» клієнти) на базі інфраструктури віртуальних робочих столів (VDI). Актуальність переходу зумовлена глобальною необхідністю реалізації парадигми «зелених IT», що спрямована на зменшення енергоспоживання, а також критичною потребою в оптимізації витрат на супровід IT-інфраструктури в академічному та бізнес-середовищі [2, 3]. Принциповою особливістю цього підходу є дослідження показників малопотужних вузлів саме в умовах високодинамічних ресурсомістких навантажень, де архітектура VDI здатна одночасно знизити енерговитрати та безпрецедентно підвищити безпеку навчального середовища [1, 4].

Традиційна робоча станція разом з монітором споживає в середньому 150-200 Вт електроенергії [1]. Впровадження архітектури VDI передбачає перенесення всіх обчислювальних процесів на централізований сервер, тоді як на робочому місці студента залишається клієнтський пристрій, рівень енергоспоживання якого складає лише від 8 до 50 Вт [1, 2]. Навіть з урахуванням енерговитрат на живлення серверів та масивів зберігання даних,

сумарне зниження енергоспоживання для типової навчальної лабораторії на 30 місць становить близько 50% [1]. Крім того, апаратна простота «тонких» клієнтів (відсутність вентиляторів та жорстких дисків) збільшує середній час напрацювання на відмову (MTBF) до 70 000 годин у порівнянні з 30 000 годин для класичних комп'ютерів [1].

У контексті навчання з кібербезпеки архітектура малопотужних клієнтів також вирішує ключову проблему надійної ізоляції та швидкого відновлення стендів. Оскільки «тонкі» клієнти обмежують взаємодію із зовнішніми носіями, несанкціоноване копіювання даних або зараження локальної машини шкідливим кодом стає технічно неможливим [1, 4]. Сама ж інфраструктура VDI дозволяє ефективно використовувати технології «золотого образу» (golden image) та зв'язаних клонів (linked clones) [1]. Завдяки цьому після завершення лабораторної роботи користувацька сесія миттєво відключається, а змінена чи навіть скомпрометована віртуальна машина за кілька секунд повністю автоматично відновлюється до еталонного «чистого» стану [1, 5].

Отже, впровадження малопотужних апаратних вузлів у віртуалізовані навчальні середовища є обґрунтованим кроком, що забезпечує суттєве зниження сукупної вартості володіння (TCO) інфраструктурою [1]. Перехід від «товстих» клієнтів до спеціалізованих «тонких» пристроїв гарантує радикальне зменшення енергоспоживання на кінцевих робочих місцях, забезпечуючи при цьому централізоване керування та максимальний рівень ізоляції операційного середовища, який є критично необхідним для безпечного дослідження сучасних кіберзагроз [3, 4].

1. Rot A., Chrobak P. Benefits, Limitations and Costs of IT Infrastructure Virtualization in the Academic Environment. Case Study using VDI Technology. In Proceedings of the 13th International Conference on Software Technologies (ICSOFT 2018), 2018. P. 704-711.
2. Pattinson C., Cross R., Kor A. L. Thin-client and Energy Efficiency. JISC Green IT Technical Report, 2011. 23 p.
3. Akintunde R. A. The Benefits of Thin Clients to Business Organizations in Developing Countries “A Case Study of Nigeria”. Master’s Thesis, University of Oulu, 2017. 83 p.
4. Смирнов О.А. Сучасні підходи до побудови захищених віртуалізованих IT-інфраструктур у закладах вищої освіти. Сучасний захист інформації. – 2024. – Т. 15, №1. – С. 45-52.
5. Mell P., Grance T. The NIST Definition of Cloud Computing. NIST Special Publication 800-145, 2011. 7 p.

Гібридна модель захисту вебзастосунків на основі OWASP Top 10 і штучного інтелекту

УДК 004.056:004.8:004.77

[1]Савчук Костянтин, [2]Нємкова Олена

Національний університет Львівська Політехніка,
[1]kostiantyn.v.savchuk @lpnu.ua, [2]olena.a.niemkova@lpnu.ua