СЕКЦІЯ XV.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

DOI 10.62731/mcnd-24.05.2024.001

ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ

Тимощук Віталій Дмитрович
ORCID ID: 0009-0007-2858-9434
здобувач першого (бакалаврського) рівня вищої освіти
факультету прикладних інформаційних технологій та електроінженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Долінський Андрій Михайлович
ORCID ID: 0009-0003-4230-0183
здобувач третього рівня вищої освіти
факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Науковий керівник: Тимощук Дмитро Іванович
ORCID ID: 0000-0003-0246-2236
старший викладач кафедри кібербезпеки
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Безпека ІТ-інфраструктури є однією з найбільш критичних і складних задач для бізнесу та організацій будь-якого розміру. Зростання загроз кібербезпеки породжує потребу у постійному удосконаленні та підвищенні захисту інфраструктури. Створення безпечної ІТ-інфраструктури вимагає комплексного підходу, що охоплює різноманітні технології, процедури та політики безпеки.

Використання віртуалізації в сфері безпеки відкриває широкі можливості для підвищення рівня захисту інформації. Технологія дозволяє створювати віртуальні екземпляри обчислювальних ресурсів, мереж та зберігання, які ізольовані один від одного та від основної фізичної інфраструктури.

Гіпервізори є основою віртуалізації. Використання гіпервізорів першого типу, таких як VMware ESXi, Hyper-V, KVM та XEN є ключовим елементом для створення віртуалізованої захищеної ІТ-інфраструктури [1]. Вони встановлюються безпосередньо на фізичні сервери та забезпечують ізольоване виконання віртуальних машин, що робить їх ідеальними для побудови безпечних середовищ. Віртуальні машини функціонують на одному фізичному сервері у відокремлених середовищах [2].

Можна віртуалізувати різні операційні системи, такі як Linux, Unix і Windows. Це відкриває широкі можливості для побудови різноманітних середовищ, що відповідають потребам конкретного бізнесу чи проекту. Наприклад, віртуалізація поштових серверів та вебсерверів є хорошою практикою з точки зору ефективності,

безпеки та управління ресурсами. Віртуалізація цих сервісів дозволяє оптимізувати використання апаратних ресурсів, забезпечуючи при цьому високий рівень надійності та доступності послуг. Також віртуалізація Windows Server з роллю RDS є ефективним способом забезпечення доступу до робочих столів та додатків для користувачів з різних місць і пристроїв. Remote Desktop Services надає централізоване управління та розгортання віддалених робочих середовищ, що дозволяє організаціям забезпечити надійний, безпечний та ефективний доступ до інформації та додатків для своїх співробітників [3].

Одним із важливих моментів захисту IT-інфраструктури є застосування маршрутизаторів з функцією брандмауера. Такі маршрутизатори, як Cisco csr1000v, IPFire, OPNsense, pfSense, MikroTik CHR, Juniper Cloud-Native Router, FortiGate VM та Palo Alto VM-Series, використовуються для створення захищених віртуальних середовищ. Ці рішення дозволяють будувати захищені мережі та контролювати потік даних між віртуальними машинами та зовнішніми мережами. Вони забезпечують фільтрацію пакетів, виявлення та запобігання атакам, а також реалізують різні VPN-з'єднання, таких як site-to-site і remote access, для захищеного з'єднання між різними частинами інфраструктури та віддаленими користувачами. Використання шифрованого VPN забезпечує конфіденційність та цілісність даних, гарантуючи, що вони залишаються захищеними від несанкціонованого доступу під час передачі через незахищені мережі, такі як Інтернет.

Висновки. Застосування гіпервізорів першого типу для створення захищеної IT-інфраструктури є ефективним підходом до забезпечення безпеки, надійності та ефективності управління ресурсами. Побудова інфраструктури з використанням таких технологій дозволяє організаціям ефективно захищати свої ресурси від різноманітних кіберзагроз, забезпечуючи при цьому надійність та доступність послуг для користувачів.

Список використаних джерел:

1. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. *Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології "Тернопільського національного технічного університету імені Івана Пулюя*, 95-95.
2. Тимощук, В., Чех, Т., Фіялка, А., & Луцик, Н. (2023). Методи віртуалізації в кластерах високої доступності. *Матеріали X I науково-технічної конференції „Інформаційні моделі, системи та технології "*, 186-187.
3. Чех, Т., Тимощук, В., Кітчак, Н., & Луцик, Н. (2023). Застосування гіпервізора KVM в кластерах високої доступності. *Collection of scientific papers «ΛΌГОΣ»*, (December 22, 2023; Boston, USA), 234-235.