DOI: https://doi.org/10.33216/1998-7927-2026-299-1-5-15

УДК 004.45: 004.38

СТВОРЕННЯ ВІРТУАЛЬНОГО НАВЧАЛЬНОГО СЕРЕДОВИЩА НА ЗАСАДАХ VMWARE VCENTER

Могильний Г.А., Переяславська С.О., Донченко В.Ю., Швець І.М., Донченко С.М., Самотіс С.І.

CREATING A VIRTUAL TRAINING ENVIRONMENT BASED ON VMWARE VCENTER

Mohylnyi H.A., Pereiaslavska S.O., Donchenko V.U., Shvets I. M., Donchenko S.M., Samotis S.I.

У сучасних умовах функціонування системи вищої освіти України, що характеризуються необхідністю забезпечення безперервного змішаного навчання, питання створення гнучких та відмовостійких навчальних середовищ набуває критичного значення. Для IT-спеціальностей наявність високопродуктивних комп'ютерних лабораторій є базовою вимогою для формування професійних компетенцій у галузі системного адміністрування, кібербезпеки та мережевих технологій.

У роботі розглядаються шляхи створення віртуального навчального середовища на засадах комплексного аналізу можливостей програмного компоненту VMware vCenter.

Методологія. У ході дослідження було застосовано комплексний системний підхід, що включає порівняльний аналіз сучасних гіпервізорів та платформ управління віртуалізацією. У процесі реалізації використовувалися методи проєктування мережевої топології віртуальних машин, налаштування прав доступу на основі рольових моделей.

У роботі проведено дослідження програмно-апаратних вимог для розгортання середовища VMware vSphere (включаючи гіпервізори ESXi та центр керування vCenter Server).

Наукова новизна дослідження полягає у розробці та адаптації моделі віртуальної лабораторії для потреб закладів вищої освіти. На відміну від стандартних корпоративних рішень, запропонована архітектура, що оптимізована за умов обмежених апаратних ресурсів та специфічних сценаріїв використання. Запропоновано механізм інтеграції віртуальної інфраструктури з існуючими системами управління надання доступу до віртуальних робочих місць. Обґрунтовано використання специфічних конфігурацій ролей для сховищ даних, віртуальних ресурсів та віртуальних мереж для забезпечення ізоляції навчальних проєктів студентів один від одного за умови збереження загальної керованості системи.

Отримані результати. Успішно впроваджено та апробовано навчальне віртуальне середовище, яке базується на використанні технологій серверної віртуалізації від компанії VMware by Broadcom. Це найбільш ефективний шлях до створення «приватної хмари» університету, здатної задовольнити потреби освітнього процесу незалежно від фізичного місцезнаходження викладачів та студентів.

***Ключові слова**: VMware by Broadcom, vCenter, ESX, рольова модель, Access Control, віртуальні ресурси, навчальне середовище, віддалений доступ, роутер, VPN.*

Вступ. В умовах стрімкої цифровізації та переходу бізнес-процесів у хмарні середовища, технології віртуалізації стали фундаментальною складовою сучасної IT-інфраструктури. Наразі роботодавці вимагають від випускників не лише знання архітектури віртуалізації, але й практичних навичок адміністрування, розгортання кластерів та управління віртуальними мережами. Проте розгортання фізичних лабораторних стендів для кожного студента є фінансово витратним та складним в обслуговуванні завданням. Рішенням такої проблеми є впровадження віртуальних освітніх середовищ (ВОС) як цифрових платформ, що розроблені для сприяння інтерактивному

практичному освітньому досвіду за допомогою технологій віртуалізації.

На сьогоднішній день рішення VMware by Broadcom, є де-факто промисловим стандартом у галузі корпоративної віртуалізації, що забезпечує надійність, масштабованість та гнучкість управління ресурсами центрів обробки даних. Використання VMware vCenter у навчальному процесі частково вирішує зазначену проблему, що дозволяє реалізувати концепцію хмарного навчального полігону. Критично важливою перевагою такого підходу є можливість забезпечення віддаленого доступу до лабораторних потужностей за умови додаткових налаштувань мережевої інфраструктури. В умовах поширення дистанційних та змішаних форм навчання, можливість працювати з інфраструктурою підприємства через вебінтерфейс (vSphere Client) із будь-якої точки світу набуває особливого значення та сприяє глибшому засвоєнню матеріалу. Крім того, при певних налаштуваннях vCenter може гарантувати безпеку та ізоляцію: виконання складних налаштувань відбувається у віртуальному просторі, що усуває ризики пошкодження основного обладнання, навіть при віддаленому підключенні через VPN або захищений шлюз.

Аналіз останніх досліджень і публікацій. Проблематика підготовки майбутніх фахівців у закладах вищої освіти засобами віртуального освітнього середовища (ВОС) активно досліджується зарубіжними і вітчизняними науковцями. Д. Костенко та ін. [1] розглядають віртуальне освітнє середовище як відкриту систему, в рамках якої на основі застосування технологій віртуальної реальності забезпечується ефективне інтерактивне самонавчання в освітньому процесі. У роботі [2] проведено порівняльний аналіз таких термінів, як «віртуальне освітнє середовище», «віртуальне навчальне середовище», «інформаційне освітнє середовище», та виділено спільний системний підхід, згідно з яким середовище – це система взаємопов’язаних, взаємозалежних компонентів, яка виконує якісно нову функцію, не властиву її окремим елементам. H. Lin та ін. [3] розглядають віртуальні освітні середовища як трансформаційний підхід до організації та реалізації освітнього процесу, що характеризується створенням нового мережевого комунікаційного простору, який підтримує динамічну взаємодію між здобувачами освіти та викладачами за допомогою комплексних систем управління. V. R. Kebande [4] досліджує віртуальні лабораторії з позиції технології віртуалізації. Такі віртуальні лабораторії являють собою специфічну реалізацію ВОС, яка дозволяє здобувачам освіти брати участь у практичних завданнях шляхом дистанційного виконання на комп'ютерних системах, що є віртуальною емуляцією.

Технічні питання створення віртуальних ВОС, таких як кіберполігони, досліджувалися D. Tymoshchuk та V. Yatskiv [5]. Автори проаналізували різні аспекти використання гіпервізорів, зокрема типи гіпервізорів, їх основні функції та специфіку їх застосування в моделюванні кіберзагроз. У статті показана здатність гіпервізорів, таких як VMware ESXi, Microsoft Hyper-V, Xen та KVM підвищувати ефективність апаратних ресурсів, створювати складні віртуальні середовища для детального моделювання мережевих структур та симуляції реальних ситуацій у кіберпросторі.

Питанням розробки віртуальних навчальних центрів за технологією VMware vSphere, керуванню доступом до ресурсів та пов’язаними з цими проблемами, присвячені дослідження [6, 7, 8]. Milan K. розглядає актуальні питання побудови, експлуатації та підготовки консолідованих центрів обробки даних для навчання технологіям адміністрування та експлуатації віртуалізації за допомогою VMware vSphere. Окрему увагу автор приділяє апаратній та програмній інфраструктурі, зокрема можливостям автоматизації підготовки навчальних середовищ за допомогою PowerCLI та PowerShell [6]. Fazuludeen N. та ін. у своєму дослідженні визначають проблеми з плануванням потужностей, безпеки віртуальної системи, технічні проблеми з віртуалізації на рівні мережі, платформи VMware vSphere, віртуального сховища та наводять приклади рішення зазначених ситуацій [7]. Akuthota, A. K. досліджує вплив моделі керування доступом на основі ролей (RBAC) у сучасній хмарі на безпеку та оптимізацію адміністративних процесів та забезпечення відповідності нормативним вимогам. Крім того, у статті оцінюється вплив RBAC на організаційну ефективність, управління ризиками та масштабованість в контексті найкращих практик впровадження та тенденцій в системах контролю доступу. Увага приділяється конвергенції RBAC з новими технологіями, такими як блокчейн та архітектура нульової довіри (Zero Trust), що дало змогу

запропонувати перспективний погляд на еволюцію управління хмарною безпекою [8].

Проведений аналіз доводить актуальність теми дослідження й водночас свідчить про недостатній обсяг дослідження проблеми створення віртуальних освітніх середовищ за допомогою платформи VMware vCenter в умовах обмежених апаратних ресурсів та специфічних сценаріїв використання, що потребують налаштування прав доступу за допомогою конфігурації ролей з метою забезпечення ізоляції користувачів за умови збереження загальної керованості системи.

Мета статті. На засадах комплексного аналізу можливостей програмного компоненту VMware vCenter розробити шляхи створення віртуального навчального середовища.

Виклад основного матеріалу дослідження. Після поглинання компанією Broadcom значна кількість ліцензій було скасовано. Наразі лінійку платформ VMware vSphere було скорочено до двох ключових версій: vSphere Foundation (VVF) та Cloud Foundation (VCF) [9,10,11]. Нині існують два основні пакети передплати та один додатковий:

- VMware Cloud Foundation (VCF) — "Все включено";
- VMware vSphere Foundation (VVF) — "Основна віртуалізація";
- vSphere Standard / Essentials Plus. — тільки для невеликих організацій, які починають працювати з віртуалізацією.

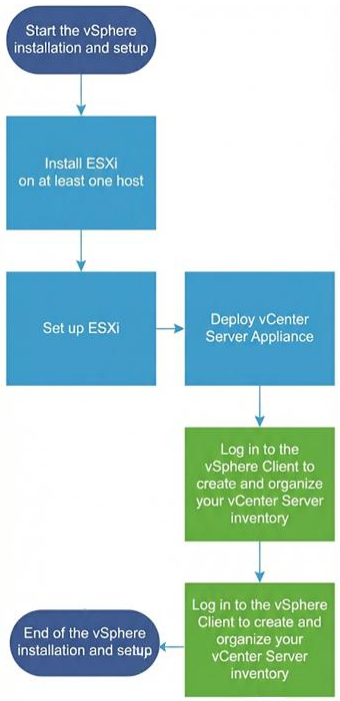

Рис. 1. Послідовність інсталювання [12]

Загальну послідовність інсталювання VMware vSphere показано на рис. 1. Ця послідовність використовується для всіх типів ліцензій.

До кожного типу ліцензії входить компонент ESXi – найнижчий шар програмного забезпечення. Слід відзначити, що в цей час Broadcom пропонує дві версії: ESX v8 та ESX v9. Однак ці версії більш вимогливі до апаратного забезпечення, працюють тільки на процесорах останніх моделей, але версія ESX v7, підтримка якої вже завершена працює стабільно та її достатньо для навчальних цілей (рис. 2). Таким чином, компонент ESXi 7 – перший базовий елемент навчального середовища, що пропонується. Після встановлення буде доступний основний засіб налаштувань ESXi – доступ через браузер на адресу мережевого адаптеру (рис. 3), що налаштована при розгортанні на Management.

Характеристика	ESXi 7.0	ESXi 8.0	ESXi 9.0
Статус (2026)	EGS (End of General Support)	Mainstream (Стабільна)	Latest (Найновіша)
Модель драйверів	Native Only (vmklinux видалено)	Native + DPU Support	Native + Enhanced Offload
Завантажувальний диск	USB/SD допустимі (але ненадійні)	USB/SD Deprecated (потрібен дод. диск)	NVMe/SSD Обов'язковий (USB блокується)
Управління конфігом	Host Profiles (XML)	Configuration Profiles (JSON)	VCF Configuration Integration
Підтримка DPU (SmartNIC)	Hi	Так (Project Monterey, v1)	Так (Gen 2, повне розвантаження NSX/vSAN)
Максимум vGPU	Обмежена підтримка MIG	Покращена робота з Multi-Instance GPU	AI/ML Optimization (Shared Pass-Through)

Рис. 2. ESXi – базовий компонент навчального середовища

vCenter Server — це централізована платформа управління інфраструктурою VMware vSphere. Це ключовий компонент, без якого неможливі кластеризація (HA, DRS), vMotion та управління життєвим циклом (Lifecycle Manager). vCenter Server – це другий базовий компонент навчального середовища. В цей час існують наступні версії:

- vCenter Server 7.x;
- vCenter Server 8.x;
- vCenter Server / VCF 9 (The Future / New Standard).

Слід враховувати сумісність версій ESXi та vCenter. У таблиці 1 наведено перелік сумісних версій [13]. Встановлення vCenter 8.0/9.0 відбувається методом "Installer з клієнтської машини" (Windows/Mac/Linux) на цільовий хост ESXi. Після двоетапного встановлення використовуємо вебсторінку за адресою, що вказана при встановленні vCenter де виконується остаточне налаштування та створення різноманітних об'єктів (рис. 4). Фактично у цьому додатку буде створено віртуальне навчальне середовище.

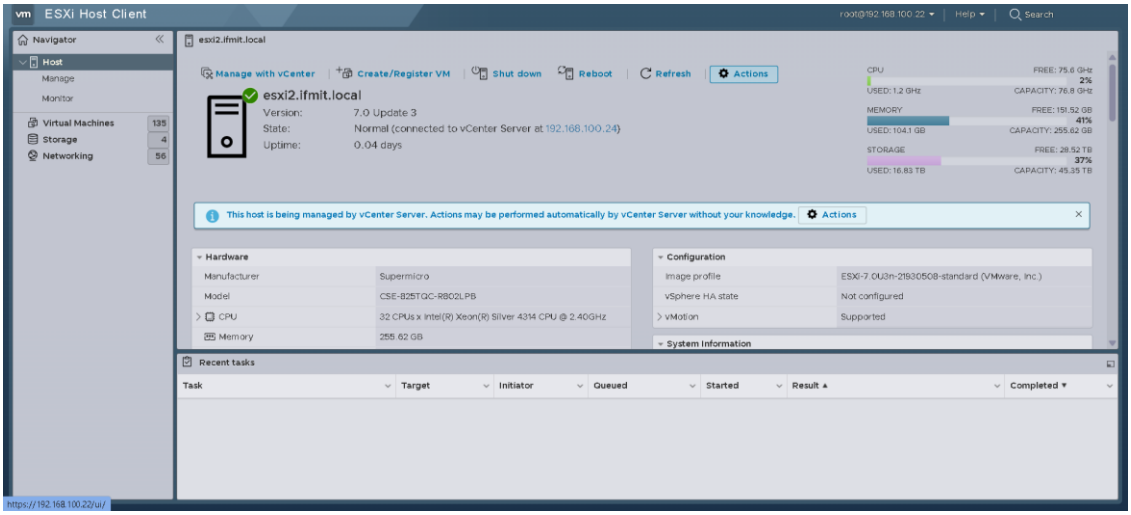

Рис. 3. Налаштування Хоста ESX v7

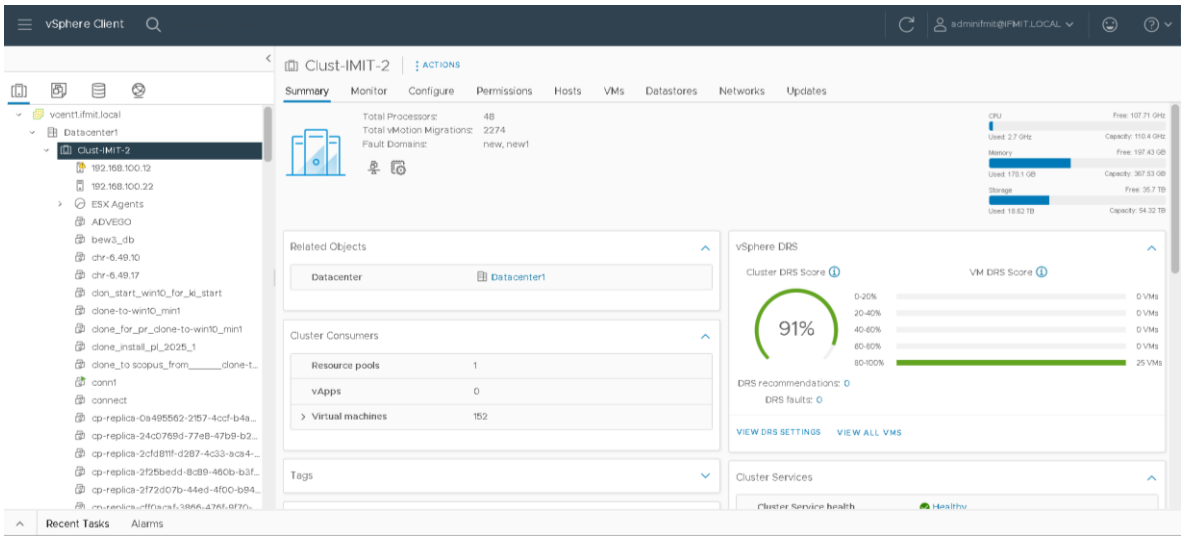

Рис. 4. Приклад налаштувань vCenter

Таблиця 1

Матриця сумісності [4] (Interoperability Matrix)

Версія vCenter Server	Підтримувані версії ESXi	Коментар
vCenter 9.0	ESXi 9.0 ESXi 8.0 U3	Підтримка ESXi 7.0 та старіших повністю вилучена. Перед апгрейдом vCenter до 9.0 переконайтеся, що всі хости мінімум версії 8.0 U3.
vCenter 8.0	ESXi 8.0 ESXi 7.0 ESXi 6.7 (до EOL)	Найбільш універсальна версія для перехідного періоду. Дозволяє керувати змішаним кластером під час міграції.
vCenter 7.0	ESXi 7.0 ESXi 6.7 ESXi 6.5	Не підтримує ESXi 8.0. Якщо ви купили новий сервер з ESXi 8.0, ви не зможете підключити його до старого vCenter.

Встановлено, що підсистема розмежування доступу у vCenter 7 базується на ієрархічній моделі рольового управління (Role-Based Access Control — RBAC). Коректна конфігурація цього компонента є критичною умовою забезпечення цілісності та конфіденційності даних, оскільки більшість інцидентів безпеки у віртуальних середовищах пов'язані саме з помилками конфігурації прав доступу, а не з вразливостями програмного коду.

Архітектура безпеки будується на взаємозв'язку трьох фундаментальних сутностей (рис. 5): Суб'єкт — Роль — Об'єкт [12]. Глибоке розуміння їх взаємодії є необхідним для побудови захищеного середовища управління та уникнення ефекту «надлишкових привілеїв».

Рис. 5. Модель RBAS у vCenter

Суб'єктами доступу виступають сутності, що ініціюють запит на виконання операції.

1. Користувачі та Групи: локальні та зовнішні.

- Локальні суб'єкти – облікові записи в домені vsphere.local, або аналогічному, що налаштовується під час інсталювання. Їх використання має бути зведене до мінімуму (переважно для аварійного доступу «break-glass», коли зовнішні служби недоступні).
- Зовнішні суб'єкти – користувачі з AD/LDAP або федеративні провайдери (IDP). При цьому, рекомендується призначення привілеїв виключно на рівні Груп. Призначення прав індивідуальним користувачам робить аудит безпеки дуже складним та ускладнює процедуру редагування прав .

2. Сервісні акаунти, які використовуються для систем резервного копіювання, моніторингу, автоматизації. Для них не діє принцип MFA, тому парольні політики та обмеження прав мають бути максимально жорсткими.

Роль у vCenter — це не просто набір прав, а визначення функціонального профілю. Існують наступні типи ролей:

1. Системні ролі (System Roles): Administrator, Read-Only та No Access:

- Administrator – надає повний контроль, включаючи керування правами доступу. Використання цієї ролі для щоденних операцій є грубим порушенням безпеки.
- Read-Only – забезпечує можливість моніторингу. Важливо розуміти, що ця роль дозволяє переглядати конфігурацію мережі та сховищ, що може бути використано зловмисником для розвідки (Reconnaissance).
- No Access – блокуюча роль. Використовується для створення «сліпих зон». Наприклад, адміністратори продуктивного середовища не повинні бачити об'єкти середовища розробки або секретного проєкту.

2. Шаблонні ролі (Sample Roles), які містять попередньо сконфігуровані набори прав (наприклад, Virtual Machine Power User). Слід відзначити, що після оновлення vCenter ці ролі можуть бути перезаписані до значень за замовчуванням. Тому їх застосування у «чистому» вигляді заборонено в Production-середовищах. Перед використанням треба клонувати у нову роль (наприклад, CORP_VM_PowerUser).

3. Користувацькі ролі (Custom Roles), які дозволяють реалізувати принцип найменших привілеїв (Least Privilege). Створюються шляхом вибору конкретних атомарних операцій (понад 500 доступних привілеїв) і, таким чином, можуть бути використані для створення віртуального навчального середовища.

До об'єктів у vCenter належать певні об'єкти інвентарю. Це найбільш складний і часто неправильно зрозумілий аспект vSphere. Ключовою концептуальною помилкою є сприйняття vCenter як єдиного ієрархічного дерева. Фактично, vCenter керує чотирма паралельними вимірами (деревами) об'єктів (рис. 6):

1. Hosts and Clusters (Хости та Кластери), яке відображає фізичні обчислювальні ресурси.
2. VMs and Templates (ВМ – віртуальні машини та Шаблони), де розташована логічна організація робочих навантажень.
3. Storage (Сховища), де розташована уся ієрархія систем зберігання (Datastores, Datastore Clusters) файли та каталоги.
4. Networking (Мережі), у якому розташовано ієрархію мереж та віртуальної комутації (DVS, Port Groups).

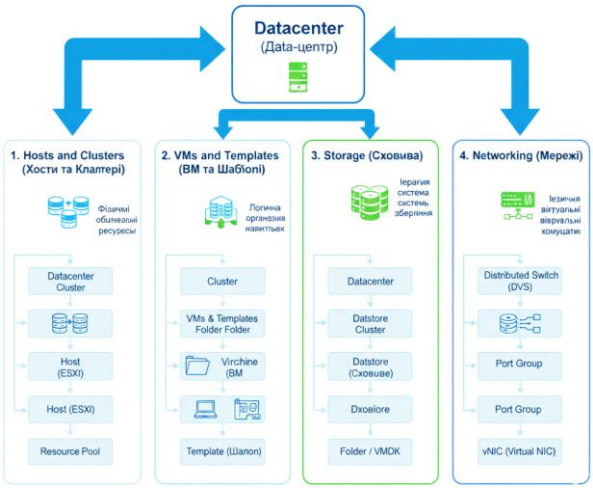

Рис. 6. Дерева інвентарю vCenter

Слід зазначити, що призначення прав в одному дереві ніколи автоматично не поширюється на об'єкти в інших деревах, навіть якщо логічно вони пов'язані. Таким чином, якщо створити папку (Folder), наприклад «Virtual X», у поданні (дереві) VMs and Templates і надати користувачеві права адміністратора на цю папку, він зможе керувати ВМ. Однак, він не побачить Datastores, на яких лежать диски цих ВМ, і мереж, до яких вони підключені, оскільки це об'єкти інших дерев.

Ґрунтуючись на виявлених ризиках в організації навчального процесу та принципі Zero Trust, розроблено деталізовану систему доступу. Основний акцент зроблено на відмові від стандартних ролей на користь користувацьких (Custom Roles), що дозволить нівелювати конфлікти між «деревами» інвентарю та забезпечити безпечну роботу.

З огляду на викладене вище, головна ідея створення навчального віртуального середовища полягає у виборі, розробці та призначенні певних нестандартних ролей (Custom Roles) на певні об'єкти програмного компоненту vCenter.

Пропонується віртуальну лабораторію розташувати у вбудованих, додаткових об’єктах (рис. 7):

- Головний каталог (Folders) та підкаталоги Віртуальних машин та шаблонів.
- Головний каталог(Folders) та підкаталоги мереж та комутаторів.

Рис. 7. Структура віртуального середовища

Folders віртуальних машин і шаблонів призначені для створення студентами (здобувачами освіти) навчально-тренувальних віртуальних машин відповідно до параметрів, визначених і контрольованих викладачем.

Folders мереж та комутаторів призначені для розташування викладачем певних віртуальних комутаторів (мереж), що використовуються здобувачами освіти для створення окремого мережевого середовища. Залежно від завдання існує можливість надати слухачам освіти право на створення певних мереж (груп портів). Однак накопичений досвід свідчить, що достатньо створити ці мережі заздалегідь та надати слухачам доступ лише на читання. Фактично це означає, що слухачі освіти мають можливість використати певні ізольовані мережі, і таким чином, отримати при виконанні лабораторних робіт свою, особисту мережу, яка не конфліктує з іншими мережами у всій інформаційній системі.

Загалом для створення віртуального середовища було розроблено п’ять додаткових ролей. Для реалізації цього середовища необхідно мати інфраструктуру, у якій є система серверів із підтримкою Ms AD (Microsoft Active Directory) та інстальовані ESXi + vCenter.

В результаті комплексного аналізу рольової моделі vCenter та особливостей організації навчального процесу було розроблено послідовність дій, необхідних для створення навчального середовища (рис. 8).

1. Приєднати компонент vCenter до Microsoft AD. Для цього потрібно знати пароль адміністратора Microsoft AD. У компоненті vCenter обираємо Системне меню Administration -> Cofiguration -> Active Directory Domain. Після такої дії vCenter буде «бачити» користувачів та групи з Active Directory Domain.

2. Створити додаткові групи у Microsoft AD на сервері– контролері AD. Запустити додаток «Диспетчер Серверів». У цьому додатку обрати «засоби» -> «Користувачі та комп’ютери». На цьому етапі треба спланувати типи та кількість доступів.

Усі інші процеси створення віртуального середовища виконуємо у компоненті vCenter у різноманітних структурах. Для переходу з однієї структури до іншої використовуємо системне меню, підменю Shortcuts.

3. Створити додаткові каталоги (Folders) віртуальних машин для розташування віртуальних машин слухачів. Спочатку переходимо в системне меню, підменю Shortcuts розділ Virtuals. Створення віртуального середовища робимо у головному каталозі (Folder) за допомогою команд: Action -> Create new folder. В межах експериментального розгортання було створено головний каталог віртуального середовища (наприклад, lab_corp_mer) та підкаталоги для певних груп користувачів-студентів (наприклад, GR2024_??), де вони мають право створювати свої віртуальні машини.

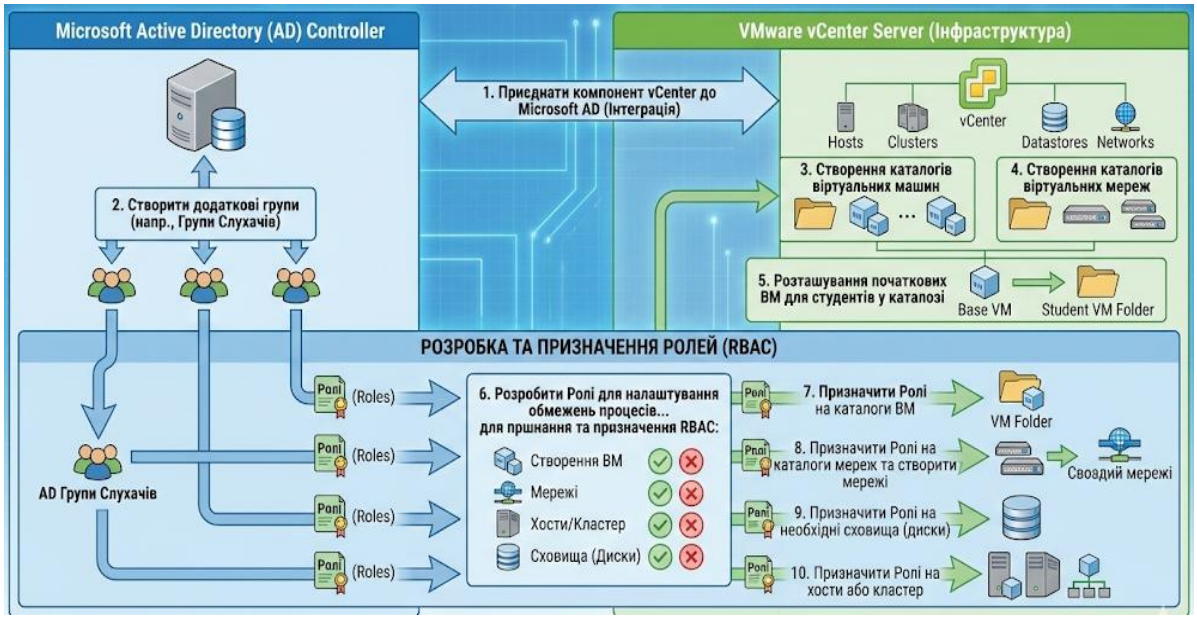

Рис. 8. Послідовність створення навчального середовища

4. Створити додаткові каталоги (Folders) для віртуальних мереж з метою використання віртуального середовища. Спочатку переходимо у системне меню, підменю Shortcuts розділ Networking. Далі застосовуються команди: Action -> Create new folder. В межах експериментального розгортання було створено головний каталог віртуального середовища (наприклад, net_folder_for_lab) та підкаталоги для певних груп користувачів-студентів (наприклад, GR2024_??), де вони мають право створювати (використовувати) свої віртуальні мережі.

5. Розташувати початкові віртуальні машини для студентів у головному каталозі віртуального середовища (в нашому варіанті це наприклад у lab_corp_mer). У даному випадку всі початкові ВМ – віртуальні машини, які студенти беруть за основу для подальшого використання.

6. Розробити Ролі для налаштування обмежень процесів створення віртуальних машин, використання або створення мереж, використання хостів або кластеру, використання певних сховищ (дисків). Створення певних ролей робиться у системному меню, підменю Administartion. Після цього обираємо меню Roles та додаємо певну Роль. Це найважливіший процес налаштування. Він потребує особливої уваги. Слід враховувати ідеологію vCenter, враховувати різні типи Дерев (див. рис.6) та призначати певні ролі. Загалом було створено 5 ролей:

- Роль на головний каталог віртуальних машин,
- Роль на особистий каталог віртуальних машин,
- Роль на підкаталог віртуальних мереж,
- Роль на сховище даних,
- Роль на хост (кластер).

Роль на головний каталог віртуальних машин (наприклад, lab_for_corp_mer) віртуального середовища робимо з обмеженнями – ТІЛЬКИ ЧИТАННЯ та можливістю КЛОНУВАТИ початкові віртуальні машини, що створені викладачем (крок 5). Можливість створення віртуальних машин на цьому рівні ЗАБОРОНЕНО. Підкаталогам для студентів (наприклад, GR2024_??) надано можливість створення віртуальних машин ТІЛЬКИ МЕТОДОМ КЛОНУВАННЯ. Створення віртуальних машин іншими засобами ЗАБОРОНЕНО. Крім того ЗАБОРОНЕНО змінювати параметри віртуальних машин (обсяг диску, процесор, ОЗУ та інші).

Окремі ролі створюємо:

- для використання певного сховища (диску) ROLE_Disk надаємо можливість ЧИТАННЯ каталогів та файлів цього диску;
- роль ROLE_Host – для використання ресурсів хосту, надаємо можливість ЧИТАННЯ РЕСУРСІВ;
- роль ROLE_Net –для ЧИТАННЯ мереж.

7-10. Призначити Ролі для певних груп Ms AD на каталоги для збереження віртуальних

машин. Потім призначаємо ROLE_Net для певних груп Ms AD на каталоги віртуальних мереж, ROLE_Disk – для певних груп Ms AD на необхідне сховище, а ROLE_Host – для певних груп Ms AD на хост (кластер).

11. За необхідністю треба провести додаткове налаштування мережевої інфраструктури для забезпечення доступу до навчального середовища з мережі Інтернет. При цьому можна виділити такі основні шляхи (рис. 9):

a. Організація доступу до локальної мережі шляхом використання VPN підключення на мережевому, пороговому роутері.
b. Використання додаткового RDP підключення на засадах ОС Microsoft Windows Server та налаштування брандмауеру для порту 3389 .
c. Прокидання службових портів vCenter на пороговому роутері: 443, 902, 80, 903,22, 5480, 9443 та ін. Цей варіант небажано використовувати з міркувань безпеки. Крім того порт 443 може бути вже використано для іншого вебсерверу.
d. Використання додаткових програмних комплексів (наприклад Omnissa Horizon) та створення спеціалізованого додатку для використання vCenter. Для цього варіанту необхідні додаткові ліцензії, що є платними.

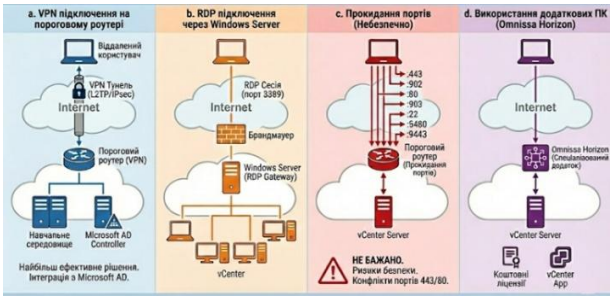

Рис. 9. Варіанти підключення до зовнішньої мережі

На підставі аналізу джерел [14-17] а також практичного досвіду, встановлено, що VPN-з'єднання з підтримкою шифрування (наприклад, типу L2TP) є найбільш ефективним рішенням. Водночас специфіка навчального процесу вимагає особливих налаштувань та інтеграції з Microsoft AD, що виходить за межі цієї роботи.

Висновки. На засадах комплексного аналізу рольової моделі vCenter досліджено шляхи створення віртуального навчального середовища, та розроблено послідовність дій процесу розгортання віртуальної інфраструктури на базі vCenter (VMware vSphere). Ключовою особливістю розгорнутого середовища є його адаптація під багатокористувацьку модель навчання, де гіпервізор ESXi та компонент vCenter Server виступають не лише технічним фундаментом, а й керованим простором. Це досягається шляхом глибокої ієрархічної структуризації інвентарю, де використання спеціалізованих папок (Folders) та призначення певних поєднань «Суб'єкт — Роль» дозволяє логічно ізолювати ресурси окремих навчальних груп та індивідуальних проєктів у межах єдиного апаратного комплексу.

Створення навчального середовища грунтується на конфігурації моделі управління доступом (RBAC), яку можна адаптувати під специфіку навчальних сценаріїв. На відміну від стандартних корпоративних налаштувань, тут основний акцент зміщений на створення «sandbox-каталогів» для студентів, що забезпечується шляхом жорсткого обмеження прав на рівні віртуальних машин, мереж, хостів та сховищ даних. Така детермінація прав доступу гарантує неможливість деструктивного впливу на загальну інфраструктуру або результати роботи інших учасників навчального процесу. За таким підходом зберігається достатній рівень автономії для виконання складних лабораторних завдань.

Література

1. Костенко Д. Впровадження віртуального інформаційного середовища у освітній процес / Д. Костенко, Н. Токуєва, О. Гречановська, М. Вереш, Ю. Кланічка. Наукові інновації та передові технології. 2023. № 6(20). DOI: 10.52058/2786-5274-2023-6(20)-462-471 .
2. 2. Bondarenko O., Pakhomova O., Lewoniewski W. The didactic potential of virtual information educational environment as a tool of geography students. Training. Augmented Reality in Education : Proceedings of the 2nd International Workshop. Kryvyi Rih, Ukraine, March 22, 2019 (2547). pp. 13-23. URL: http://ceur-ws.org/Vol-2547/paper01.pdf (дата звернення: 17.01.2026).
3. Lin, H. Metaverse in Education: Vision, Opportunities, and Challenges / H. Lin, S. Wan, W. Gan, J. Chen, H.-C. Chao. 2022 IEEE International Conference on Big Data. 2022. DOI: 10.1109/BigData55660.2022.10021004.
4. Kebande, V. R. The Impact of Virtual Laboratories on Active Learning and Engagement in

Cybersecurity Distance Education. arXiv preprint arXiv. 2024. DOI: 10.48550/arXiv.2404.04952 .
5. Tymoshchuk D., Yatskiv V. Using hypervisors to create a cyber polygon. Measuring and Computing Devices in Technological Processes. 2024. No. 3. P. 52–56. DOI: 10.31891/2219-9365-2024-79-7.
6. Milan K. Možnosti výuky virtualizačních technologií a jejíautomatizace s využitím technologie vmvmware vsphere. Trends in Education. 2022. Vol. 14, no. 2. P. 5–14. DOI: 10.5507/tvv.2022.001 .
7. Fazuludeen N. Challenges And Issues Of Managing The Virtualization Environment Through VMware vSphere / N. Fazuludeen, S. S. Banu, A. Gupta, S. Swathi. Nanotechnology Perceptions. 2024. Vol. 20, S1. DOI: 10.62441/nano-ntp.v20is1.23.
8. Arun Kumar Akuthota. Role-Based Access Control (RBAC) in Modern Cloud Security Governance: An In-depth Analysis. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2025. Vol. 11, no. 2. P. 3297–3311. DOI: 10.32628/cseit25112793.
9. Broadcom Completes Acquisition of VMware [Електронний ресурс] URL: https://www.broadcom.com/company/news/financial-releases/61541 (дата звернення: 21.01.2026)
10. VMware Cloud Foundation [Електронний ресурс] URL: https://ftpdocs.broadcom.com/cadocs/0/contentimages/VCF_SPD_June2024.pdf (дата звернення: 21.01.2026).
11. VMware vSphere Foundation [Електронний ресурс] URL: https://ftpdocs.broadcom.com/cadocs/0/contentimages/VVF_SPD_May2024.pdf (дата звернення: 21.01.2026).
12. Vmware-vsphere-7-0 [Електронний ресурс] URL: https://techdocs.broadcom.com/content/dam/broadcom/techdocs/us/en/pdf/vmware/vsphere/vsphere/vmware-vsphere-7-0.pdf (дата звернення: 21.01.2026).
13. Product Interoperability Matrix [Електронний ресурс] URL: https://interopmatrix.broadcom.com/Interoperability?isHidePatch=false&isHideLegacyReleases=false&col=1,3495,5558,5890,18609&row=2,3496,5891,18702 (дата звернення: 21.01.2026).
14. Могильний Г. Аналіз програмно-апаратних засобів створення системи з віддаленим доступом до навчальних комп'ютерних лабораторій закладів середньої освіти. Вісник Східноукраїнського національного університету імені Володимира Даля. 2023. № 1(277). С. 5–19. DOI: 10.33216/1998-7927-2019-256-8-5-19.
15. Могильний Г., Донченко В., Донченко С. Огляд та аналіз інструментів створення корпоративного середовища. Інформаційні технології та суспільство. 2024. № 4 (15). С. 99–107. DOI: 10.32689/maup.it.2024.4.16.
16. Кардашук В., Бортник К., Багнюк Н. Проблеми захисту інформації у віртуальних приватних мережах та відбиття атак на Web-додатки. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцк, 2023. № 53. С. 117–124. DOI:10.36910/6775-2524-0560-2023-53-18 .
17. Могильний Г., Семенов М., Кірєєв І. Впровадження системи віддаленого доступу до інформаційних ресурсів комп'ютерних лабораторій. Вісник Східноукраїнського національного університету імені Володимира Даля. 2022. № 2 (272). С. 7–14. DOI: 10.33216/1998-7927-2022-272-2-7-14 .

References

1. Kostenko D. Vprovadzhennia virtualnoho informatsiinoho seredovyshcha u osvitnii protses / D. Kostenko, N. Tokuieva, O. Hrechanovska, M. Veresh, Yu. Klanichka. Naukovi innovatsii ta peredovi tekhnolohii. 2023. № 6(20). DOI: 10.52058/2786-5274-2023-6(20)-462-471.
2. 2. Bondarenko O., Pakhomova O., Lewoniewski W. The didactic potential of virtual information educational environment as a tool of geography students. Training. Augmented Reality in Education : Proceedings of the 2nd International Workshop. Kryvyi Rih, Ukraine, March 22, 2019 (2547). pp. 13-23. URL: http://ceur-ws.org/Vol-2547/paper01.pdf (accessed: 17.01.2026).
3. Lin, H. Metaverse in Education: Vision, Opportunities, and Challenges / H. Lin, S. Wan, W. Gan, J. Chen, H.-C. Chao. 2022 IEEE International Conference on Big Data. 2022. DOI: 10.1109/BigData55660.2022.10021004.
4. Kebande, V. R. The Impact of Virtual Laboratories on Active Learning and Engagement in Cybersecurity Distance Education. arXiv preprint arXiv. 2024. DOI: 10.48550/arXiv.2404.04952 .
5. Tymoshchuk D., Yatskiv V. Using hypervisors to create a cyber polygon. Measuring and Computing Devices in Technological Processes. 2024. No. 3. P. 52–56. DOI: 10.31891/2219-9365-2024-79-7.
6. Milan K. Možnosti výuky virtualizačních technologií a jejíautomatizace s využitím technologie vmvmware vsphere. Trends in Education. 2022. Vol. 14, no. 2. P. 5–14. DOI: 10.5507/tvv.2022.001 .
7. Fazuludeen N. Challenges And Issues Of Managing The Virtualization Environment Through VMware vSphere / N. Fazuludeen, S. S. Banu, A. Gupta, S. Swathi. Nanotechnology Perceptions. 2024. Vol. 20, S1. DOI: 10.62441/nano-ntp.v20is1.23.
8. Arun Kumar Akuthota. Role-Based Access Control (RBAC) in Modern Cloud Security Governance: An In-depth Analysis. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2025. Vol. 11, no. 2. P. 3297–3311. DOI: 10.32628/cseit25112793 .

9. Broadcom Completes Acquisition of VMware URL: https://www.broadcom.com/company/news/financial-releases/61541 (accessed: 21.01.2026)
10. VMware Cloud Foundation URL: https://ftpdocs.broadcom.com/cadocs/0/contentimages/VCF_SPD_June2024.pdf (accessed: 21.01. 2026).
11. VMware vSphere Foundation URL: https://ftpdocs.broadcom.com/cadocs/0/contentimages/VVF_SPD_May2024.pdf (accessed: 21.01. 2026).
12. Vmware-vsphere-7-0 URL: https://techdocs.broadcom.com/content/dam/broadcom/techdocs/us/en/pdf/vmware/vsphere/vsphere/vmware-vsphere-7-0.pdf (accessed: 21.01.2026).
13. Product Interoperability Matrix URL: https://interopmatrix.broadcom.com/Interoperability?isHidePatch=false&isHideLegacyReleases=false&col=1,3495,5558,5890,18609&row=2,3496,5891,18702 (accessed: 21.01.2026).
14. Mohylnyi H. Analiz prohramno-aparatnykh zasobiv stvorennia systemy z viddalenym dostupom do navchalnykh kompiuternykh laboratorii zakladiv serednoi osvity. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia. 2023. № 1(277). S. 5–19. DOI: 10.33216/1998-7927-2019-256-8-5-19.
15. Mohylnyi H., Donchenko V., Donchenko S. Ohliad ta analiz instrumentiv stvorennia korporatyvnoho seredovyshcha. Informatsiini tekhnolohii ta suspilstvo. 2024. № 4 (15). S. 99–107. DOI: 10.32689/maup.it.2024.4.16.
16. Kardashuk V., Bortnyk K., Bahniuk N. Problemy zakhystu informatsii u virtualnykh pryvatnykh merezhakh ta vidbyttia atak na Web-dodatky. Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo. Lutsk, 2023. № 53. S. 117–124. DOI: 10.36910/6775-2524-0560-2023-53-18 .
17. Mohylnyi H., Semenov M., Kirieiev I. Vprovadzhennia systemy viddalenoho dostupu do informatsiinykh resursiv kompiuternykh laboratorii. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia. 2022. № 2 (272). S. 7–14. DOI: 10.33216/1998-7927-2022-272-2-7-14.

Mohylnyi H.A., Pereiaslavska S.O., Donchenko V.U., Shvets I. M., Donchenko S.M., Samotis S.I. Creating a virtual training environment based on Vmware vCenter

The current conditions of the functioning of the higher education system of Ukraine are characterized by the need to ensure continuous blended learning. Therefore, the issue of creating flexible and fault-tolerant learning environments is of critical importance. For IT specialties, the availability of high-performance computer laboratories is a basic requirement for the formation of professional competencies in the field of system administration, cybersecurity and network technologies.

The work, based on a comprehensive analysis of the capabilities of the VMware vCenter software component, examines ways to create a virtual learning environment.

Methodology. The study used a comprehensive systems approach, including a comparative analysis of modern hypervisors and virtualization management platforms. In the implementation process, methods for designing the network topology of virtual machines and configuring access rights based on role models were used.

The work examined the software and hardware requirements for deploying the VMware vSphere environment (including ESXi hypervisors and the vCenter Server management center).

The scientific novelty of the study lies in the development and adaptation of a virtual laboratory model specifically for the needs of higher education institutions. The developed architecture is optimized for conditions of limited hardware resources and specific usage scenarios, unlike standard corporate solutions. A mechanism for integrating virtual infrastructure with existing management systems for providing access to virtual workplaces is proposed. The use of specific role configurations for data storage, virtual resources, and virtual networks is justified to ensure the isolation of students' educational projects from each other while maintaining the overall manageability of the system.

Results. A virtual educational environment based on the use of server virtualization technologies from VMware by Broadcom has been successfully implemented and tested. This is the most effective way to create a "private cloud" of the university, capable of meeting the needs of the educational process regardless of the physical location of teachers and students.

Key words: *VMware by Broadcom, vCenter, ESX, role model, Access Control, virtual resources, learning environment, remote access, router, VPN.*

Могильний Геннадій Анатолійович – к. т. н., доцент, директор Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, g.mogilniy@gmail.com

Переяславська Світлана Олександрівна – к.п.н., доцент кафедри інформаційних технологій та систем Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, pereyaslav9@gmail.com

Донченко Володимир Юрійович – старший викладач кафедри інформаційних технологій та систем Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, ifmit.s.2014@gmail.com

Швець Ірина Михайлівна – асистент кафедри математики та інформатики Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, irinachipenkooo@gmail.com
Донченко Світлана Миколаївна – асистент кафедри інформаційних технологій та систем Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, donchenko.lana77@gmail.com
Самотіс Сергій Іванович – магістрант Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, ssamotss@gmail.com

Стаття подана 12.12.2025.