Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Аналіз та впровадження заходів безпеки в Proxmox VE"

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Стебельський М. В.
підпис (прізвище та ініціали)

Керівник Тимощук Д. І.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д.І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Стебельському Максиму Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз та впровадження заходів безпеки в Proxmox VE

Керівник роботи Тимощук Дмитро Іванович, старший викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «15» 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи 17.06.2024

3. Вихідні дані до роботи Вимоги до заходів безпеки віртуалізованих середовищ та платформ управління віртуалізацією

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати принципи роботи віртуалізації, визначити їх переваги та недоліки.
Дослідити особливості роботи Proxmox VE.
Проаналізувати заходи безпеки Proxmox VE (двофакторну аутентифікацію, контроль доступу та брандмауер).
Здійснити практичну реалізацію налаштування двофакторної аутентифікації, контролю доступу та брандмауера.
Безпека життєдіяльності, основи охорони праці.
Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема. Мета роботи. Актуальність теми дослідження. Об'єкт та предмет дослідження. Аналіз Proxmox VE. Схема організації компонентів Proxmox VE. Заходи безпеки в Proxmox VE. Двофактона автентифікація в Proxmox VE. Контроль доступу користувачів в Proxmox VE. Брандмауер в Proxmox VE. Вхід у веб-інтерфейс та SSH-з'єднання до хосту з комп'ютера Test PC. SSH-з'єднання до ВМ Debian Linux з комп'ютера Test PC. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н, доцент кафедри МТ		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	30.01 – 05.02	Виконано
2.	Підбір джерел для аналізу основних аспектів віртуалізації	08.02 – 15.02	Виконано
3.	Теоретичний аналіз літератури та наукових статей з питань віртуалізації	17.02 – 26.02	Виконано
4.	Проведення аналізу особливостей роботи Proxmox VE	29.02 – 11.03	Виконано
5.	Проведення аналізу засобів безпеки Proxmox VE	13.03 – 18.03	Виконано
6.	Налаштування засобів безпеки Proxmox VE	20.03 – 28.03	Виконано
7.	Оформлення розділу «Основні аспекти віртуалізації»	30.03 – 05.04	Виконано
8.	Оформлення розділу «Аналіз засобів безпеки Proxmox VE»	06.04 – 15.04	Виконано
9.	Оформлення розділу «Практична реалізація заходів захисту в Proxmox VE»	18.04 – 24.04	Виконано
10.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	27.04 – 06.05	Виконано
11.	Оформлення кваліфікаційної роботи	09.05 – 19.05	Виконано
12.	Нормоконтроль	21.05 – 23.05	Виконано
13.	Перевірка на плагіат	03.06 – 05.06	Виконано
14.	Попередній захист кваліфікаційної роботи	18.06.2024	Виконано
15.	Захист кваліфікаційної роботи	27.06.2024	

Студент _____ Стебельський М.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Тимощук Д. І.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз та впровадження заходів безпеки в Proxmox VE // Кваліфікаційна робота ОР «Бакалавр» // Стебельський Максим Віталійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-43 // Тернопіль, 2024 // С. 51 , рис. – 28, табл. – - , кресл. – - , додат. – -.

КЛЮЧОВІ СЛОВА: Proxmox VE, віртуалізація, гіпервізор, двофакторна аутентифікація, контроль доступу, брандмауер.

У кваліфікаційній роботі розглядаються основні аспекти віртуалізації, зокрема її загальні принципи, переваги впровадження, а також недоліки та виклики, що виникають під час використання цих технологій. Основна увага приділяється платформі віртуалізації Proxmox VE та заходам безпеки, що забезпечують її ефективне функціонування.

У першому розділі висвітлюються загальні принципи віртуалізації, її переваги та недоліки. Другий розділ присвячений аналізу заходів безпеки у Proxmox VE, включаючи огляд платформи, двофакторну аутентифікацію, контроль доступу користувачів та використання брандмауера.

Третій розділ містить практичні рекомендації з налаштування заходів захисту в Proxmox VE. У цьому розділі розглядаються конкретні кроки щодо налаштування двофакторної аутентифікації, контролю доступу користувачів та брандмауера.

Четвертий розділ зосереджений на питаннях безпеки життєдіяльності та основах охорони праці. У ньому аналізуються ергономічні проблеми безпеки життєдіяльності та необхідність проведення інструктажів з охорони праці.

Робота спрямована на покращення розуміння технологій віртуалізації та їх безпечного впровадження, зокрема з використанням платформи Proxmox VE, що є актуальним у сучасних умовах розвитку інформаційних технологій.

ABSTRACT

Analysis and Implementation of Security Measures in Proxmox VE // Thesis of educational level "Bachelor"// Stebelskyi Maksym Vitaliyovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБс-43 // Ternopil, 2024 // P. 51 fig. – 28, tab. – -, chair. – -, added. – -.

Keywords: Proxmox VE, virtualization, hypervisor, two-factor authentication, access control, firewall.

The qualification paper examines the main aspects of virtualization, including its general principles, implementation advantages, as well as the disadvantages and challenges that arise when using these technologies. The main focus is on the Proxmox VE virtualization platform and the security measures that ensure its effective operation.

The first section highlights the general principles of virtualization, its advantages and disadvantages. The second section is devoted to the analysis of security measures in Proxmox VE, including an overview of the platform, two-factor authentication, user access control, and firewall usage.

The third section provides practical recommendations for configuring security measures in Proxmox VE. This section covers specific steps for configuring two-factor authentication, user access control, and firewall.

The fourth chapter focuses on life safety and the basics of occupational health and safety. It analyzes the ergonomic issues of life safety and the need for health and safety training.

This work is aimed at improving the understanding of virtualization technologies and their safe implementation, in particular using the Proxmox VE platform, which is relevant in the current conditions of information technology development.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VLAN	—	Virtual Local Area Network
iSCSI	—	Internet Small Computer System Interface
NFS	—	Network File System
LXC	—	Linux Containers
VPS	—	Virtual Private Server
KVM	—	Kernel-based Virtual Machine

ВСТУП

З огляду на швидке зростання кількості кібератак та витоків інформації, питання захисту даних набуває критичної важливості. Віртуалізація дозволяє підвищити ефективність використання апаратних ресурсів, знижуючи витрати на обладнання та обслуговування, а також забезпечує високий рівень безпеки завдяки ізоляції віртуальних машин, що мінімізує ризики несанкціонованого доступу та шкідливого програмного забезпечення. Однак зростання використання технологій віртуалізації також підвищує ризики, пов'язані з інформаційною безпекою. Забезпечення надійного захисту віртуалізованих середовищ є актуальним завданням, особливо для платформ, які широко використовуються в корпоративних мережах, таких як Proxmox VE.

Метою роботи є аналіз та впровадження ефективних заходів захисту для забезпечення безпеки в платформі віртуалізації Proxmox VE. Задачі дослідження включають:

– Провести аналіз загальних принципів віртуалізації та визначити їх переваги та недоліки.

– Дослідити можливості платформи Proxmox VE щодо заходів безпеки.

– Впровадити практичні заходи захисту платформи Proxmox VE для підвищення рівня безпеки.

Об'єктом дослідження є платформа віртуалізації Proxmox VE, яка забезпечує управління віртуальними машинами та контейнерами в корпоративних мережах.

Предметом дослідження є аналіз та впровадження заходів безпеки для забезпечення захисту в платформі віртуалізації Proxmox VE.

Результати дослідження матимуть практичне значення для організацій, які використовують платформу віртуалізації Proxmox VE. Впроваджені заходи безпеки дозволять підвищити рівень захисту віртуалізованої інфраструктури, зменшуючи ризик несанкціонованого доступу та мінімізуючи наслідки потенційних атак.

1 ОСНОВНІ АСПЕКТИ ВІРТУАЛІЗАЦІЇ

Віртуалізація – це технологічний принцип, який полягає у створенні віртуальних екземплярів обчислювального обладнання та операційних систем. Цей процес дозволяє ізолювати ресурси, такі як процесори, пам'ять та сховища даних, щоб їх можна було використовувати незалежно від фізичного обладнання. Технології віртуалізації дозволяють керувати інфраструктурою, забезпечуючи більш ефективне використання ресурсів, скорочення часу на розгортання середовищ та полегшення резервування та відновлення даних. Цей напрям розвивається швидко, і його застосування охоплює такі сфери як хмарні обчислення, віртуалізовані мережі, тестування програмного забезпечення та інші сфери [1].

1.1 Загальні принципи віртуалізації

Основним принципом віртуалізації є ізоляція та віртуалізація фізичних ресурсів з метою їх ефективного використання та управління. Цей процес реалізується шляхом розділення фізичних ресурсів на віртуальні окремі екземпляри, які називаються віртуальними машинами або контейнерами.

Існують різні типи віртуалізації, але прийнято вважати основними типами такі [2]:

– Віртуалізація операційних систем. Цей тип віртуалізації дозволяє запускати кілька ізольованих операційних систем на одному фізичному сервері. Кожна операційна система працює як окремий віртуальний сервер.

– Віртуалізація програмного забезпечення. Тут віртуальне середовище створюється для виконання конкретного програмного забезпечення безпосередньо на операційній системі.

– Віртуалізація інфраструктури. Цей тип віртуалізації включає в себе створення віртуальних версій фізичних об'єктів, таких як обчислювальні ресурси, мережеві з'єднання та сховища даних.

– Віртуалізація віддалених робочих столів. Тут віртуальні робочі столи запускаються на сервері та надаються користувачам через мережу.

– Віртуалізація систем зберігання даних. Цей тип віртуалізації дозволяє об'єднувати фізичні сховища даних в одну віртуальну систему зберігання.

– Віртуалізація мережі. Тут віртуальні мережеві ресурси, такі як маршрутизатори, комутатори та брандмауери, створюються та управляються віртуально.

– Віртуалізація серверів. Цей тип віртуалізації полягає в створенні віртуальних екземплярів серверів на одному фізичному сервері, що дозволяє ефективно використовувати ресурси та забезпечує гнучкість в управлінні серверами.

Робота з віртуалізацією вимагає розуміння основних її елементів та концепцій. Основними складовими віртуалізованих середовищ є гіпервізор та віртуальна машина.

Віртуальна машина (VM) – це ізольоване віртуальне середовище, яке відтворює фізичний комп'ютер. Кожна VM має свою власну операційну систему та ресурси, такі як процесор, пам'ять та диск. VM можуть бути запущені, зупинені, перенесені та копійовані незалежно одна від одної, що забезпечує гнучкість та ефективність управління обчислювальними ресурсами.

Гіпервізор – це програмне забезпечення, яке дозволяє розділити фізичний сервер на декілька віртуальних машин. Існують два основних типи гіпервізорів: Тип 1 (bare-metal) та Тип 2 (hosted). Гіпервізори Типу 1 працюють безпосередньо на апаратному рівні сервера, тоді як гіпервізори Типу 2 встановлюються на операційну систему [3].

1.2 Переваги впровадження технологій віртуалізації

Впровадження технологій віртуалізації має ряд переваг як для звичайних користувачів, так і для бізнесу. Нижче наведено деякі з основних переваг:

– Зручність та спрощення управління. Віртуалізація дозволяє легко управляти великою кількістю віртуальних машин чи контейнерів з централізованого інтерфейсу. Адміністратори можуть швидко розгортати, масштабувати та керувати обчислювальними ресурсами, що спрощує адміністрування та підтримку інфраструктури.

– Масштабованість та гнучкість. Завдяки віртуалізації, компанії можуть легко масштабувати свої обчислювальні потужності відповідно до зростання бізнесу. Створюється можливість швидко реагувати на зміни в навантаженні та вимоги ринку, забезпечуючи необхідні ресурси для виконання завдань.

– Ефективне використання ресурсів. Віртуалізація дозволяє оптимізувати використання фізичних ресурсів серверів. Запуск кількох віртуальних машин на одному фізичному сервері дозволяє знизити кількість потрібних серверів та енергоспоживання, що веде до економії коштів для організації.

– Забезпечення високої доступності та надійності. Віртуалізація дозволяє легко реалізувати механізми резервного копіювання та відновлення даних, а також забезпечує можливість автоматичного перенесення робочих навантажень в разі виникнення неполадок, що забезпечує безперервну роботу системи.

– Підвищення безпеки даних. Віртуалізація дозволяє ізолювати різні середовища та застосунки один від одного, що знижує ризик втрати чи пошкодження даних внаслідок вразливостей одного компоненту системи. Також, завдяки вбудованим механізмам контролю доступу та моніторингу, віртуалізація підвищує рівень безпеки та захисту інформації.

Впровадження технологій віртуалізації приносить значні переваги як для індивідуальних користувачів, так і для бізнесу. Завдяки зручності та спрощенню управління, віртуалізація дозволяє ефективно контролювати велику кількість віртуальних машин або контейнерів через централізований інтерфейс, що полегшує адміністрування та підтримку інфраструктури. Масштабованість та гнучкість технології дозволяють компаніям швидко адаптувати свої обчислювальні потужності до зростання бізнесу та змін ринкових умов.

Ефективне використання фізичних ресурсів серверів сприяє економії коштів завдяки зниженню кількості необхідних серверів та енергоспоживання [4].

Віртуалізація також забезпечує високу доступність та надійність систем, завдяки можливостям резервного копіювання, відновлення даних та автоматичного перенесення робочих навантажень у разі неполадок. Окрім того, ізоляція різних середовищ та додатків підвищує рівень безпеки даних, знижуючи ризик втрати або пошкодження інформації через вразливості окремих компонентів системи. Вбудовані механізми контролю доступу та моніторингу додатково покращують захист інформації.

1.3 Недоліки та виклики, пов'язані з впровадженням віртуалізації

Впровадження віртуалізації в сучасні організації приносить значні переваги, але також стикається з рядом недоліків та викликів. Серед недоліків та викликів можна виділити наступні:

– Збій обладнання може призвести до відмови всіх віртуальних серверів. В разі відмови фізичного сервера, на якому працюють віртуальні машини, всі віртуальні приватні сервери (VPS) можуть бути недоступними. Необхідно реалізувати механізми резервування або забезпечення безперебійної роботи основного хоста, використовуючи технології віртуальної міграції, які дозволяють автоматично переміщувати робочі навантаження з відмовленого сервера на інший та регулярно створювати резервні копії віртуальних машин, щоб забезпечити швидке відновлення при потребі.

– Управління віртуальною інфраструктурою вимагає спеціалізованих знань і навичок, оскільки конфігурація та налаштування віртуальних середовищ може бути складним та технічно вимогливим процесом. Для ефективного управління віртуальними середовищами необхідно мати розуміння принципів віртуалізації, знання про різні типи гіпервізорів та їх особливості, а також розуміння процесів моніторингу та управління ресурсами. Крім того, персонал повинен бути ознайомлений з сучасними технологіями та методиками

управління віртуалізованими інфраструктурами, такими як інструменти автоматизації та оркестрації.

– Деякі рішення віртуалізації можуть вимагати додаткових витрат на придбання ліцензійного програмного забезпечення. Це може стати причиною збільшення загальних витрат на впровадження та експлуатацію віртуальних середовищ. Ліцензійні витрати можуть бути пов'язані з використанням платних гіпервізорів або іншого програмного забезпечення для впровадження віртуалізації. Важливо проаналізувати та обрати оптимальне рішення, яке відповідає потребам організації та бюджетним обмеженням.

Впровадження віртуалізації в сучасні організації приносить значні переваги, проте також супроводжується певними недоліками та викликами. Зокрема, збій обладнання може призвести до відмови всіх віртуальних серверів, що робить необхідним використання механізмів резервування та технологій віртуальної міграції для забезпечення безперебійної роботи.

Управління віртуальною інфраструктурою вимагає висококваліфікованих спеціалістів, здатних налаштовувати та підтримувати складні віртуальні середовища. Це включає глибоке розуміння принципів віртуалізації, різних типів гіпервізорів, процесів моніторингу та управління ресурсами, а також сучасних інструментів автоматизації.

Крім того, деякі рішення віртуалізації можуть вимагати значних фінансових вкладень на придбання ліцензійного програмного забезпечення, що збільшує загальні витрати на впровадження та експлуатацію. Тому важливо ретельно оцінювати та вибирати оптимальні рішення, які відповідають як потребам організації, так і її фінансовим можливостям.

Отже, успішне впровадження віртуалізації потребує ретельного планування, належної підготовки кадрів та фінансових ресурсів для ефективного подолання можливих викликів та забезпечення стабільної і безпечної роботи віртуальних середовищ.

2 АНАЛІЗ ЗАХОДІВ БЕЗПЕКИ PROXMOX VE

2.1 Огляд платформи віртуалізації Proxmox VE

Proxmox VE – це комплексна платформа віртуалізації з відкритим кодом, призначена для керування віртуальними машинами на базі ядра KVM та контейнерами LXC [5]. Proxmox VE відноситься до гіпервізорів Тип-1, а ключова особливість полягає в інтегрованому веб-інтерфейсі, який забезпечує централізоване керування ресурсами, створення та моніторинг віртуальних машин і контейнерів. Завдяки цьому можна швидко впровадити використання Proxmox VE та ефективно керувати віртуалізованими середовищами. Крім того, Proxmox VE підтримує різні типи сховищ та мережевих конфігурацій, що дозволяє легко адаптуватися до вимог різних інфраструктур. Платформа також пропонує можливості для резервного копіювання та відновлення даних, підвищуючи надійність і безпеку системи.

На рисунку 2.1 зображено веб-інтерфейс головної сторінки Proxmox VE.

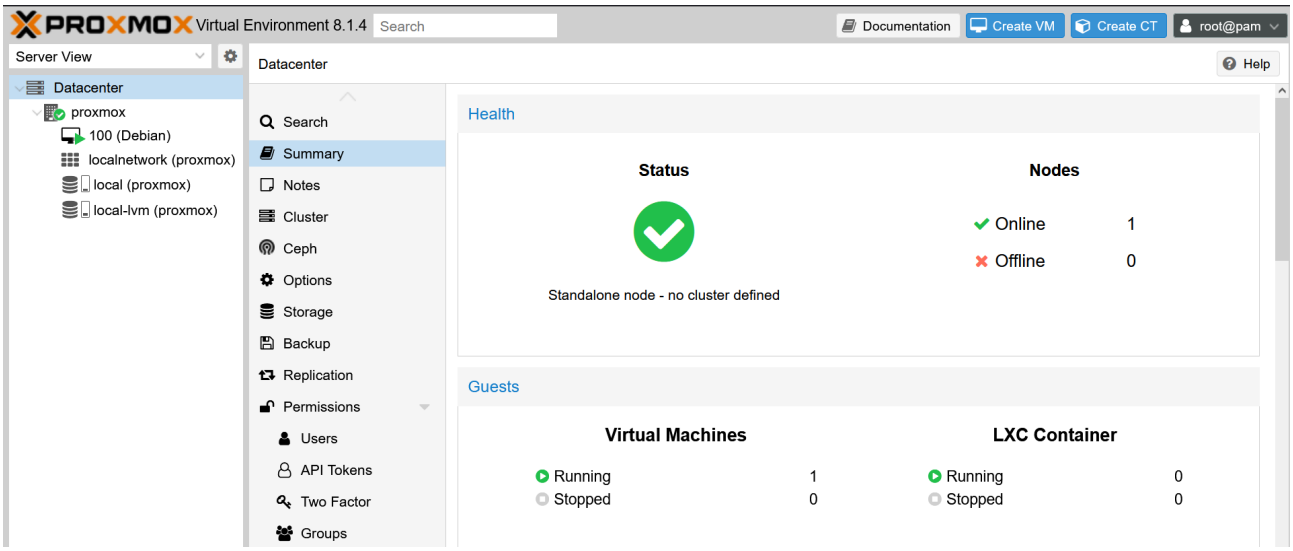

Рисунок 2.1 – Веб-інтерфейс головної сторінки Proxmox VE

До ключових переваг платформи Proxmox VE можна віднести [6]:

– Комплексна віртуалізація. Proxmox VE підтримує як віртуальні машини KVM, так і контейнери LXC, забезпечуючи гнучкість і ефективність

віртуалізації. Віртуалізація на основі KVM дозволяє запускати декілька ізольованих віртуальних машин на одному фізичному сервері з продуктивністю, близькою до нативної, та підтримкою різних операційних систем, включаючи Windows, Linux і BSD. Для полегшеної віртуалізації Proxmox VE використовує контейнери LXC, які поділяють ядро хоста, але забезпечують ізольовані простори користувачів, що робить їх ідеальними для запуску додатків на базі Linux з мінімальними накладними витратами.

– Інтегрований інтерфейс управління. Proxmox VE пропонує веб-інтерфейс, який дозволяє адміністраторам керувати віртуальними машинами, контейнерами, сховищем та мережевими конфігураціями з єдиної, інтуїтивно зрозумілої панелі управління. Цей інтерфейс підтримує різні адміністративні завдання, такі як створення віртуальних машин, планування резервного копіювання та міграція в реальному часі, що спрощує процес управління та підвищує ефективність роботи.

– Висока доступність і кластеризація. Proxmox VE підтримує кластеризацію, що дозволяє керувати кількома серверами Proxmox як єдиним цілим. Завдяки кластеризації забезпечується висока доступність, автоматично перезапускаючи віртуальні машини або контейнери на інших вузлах у разі відмови обладнання. Це гарантує мінімальний час простою та підвищену надійність системи.

– Варіанти зберігання. Proxmox VE пропонує гнучке управління сховищем з підтримкою локального сховища, спільних сховищ (NFS, iSCSI, Ceph) та розподілених систем зберігання даних. Вбудована функція реплікації забезпечує надмірність даних і високу доступність, що підвищує надійність зберігання та захист даних.

– Резервне копіювання та відновлення. Proxmox VE містить вбудовані інструменти для резервного копіювання, які дозволяють здійснювати планове резервне копіювання віртуальних машин і контейнерів. Ці резервні копії можуть зберігатися як на локальних, так і на віддалених сховищах, і можуть бути легко відновлені через управлінський інтерфейс.

– Робота в мережі. Proxmox VE підтримує розширені мережеві можливості, включаючи VLAN, мости та об'єднання інтерфейсів. Це дозволяє створювати складні мережеві топології та оптимально використовувати мережеві ресурси. Платформа також легко інтегрується з SDN (Software-Defined Networking) рішеннями, що покращує управління мережею та забезпечує гнучкість конфігурацій.

Proxmox VE – це потужна платформа віртуалізації з відкритим кодом, яка забезпечує комплексне керування віртуальними машинами на основі KVM та контейнерами LXC. Завдяки інтегрованому веб-інтерфейсу, Proxmox VE спрощує адміністрування віртуалізованих середовищ, дозволяючи централізовано керувати ресурсами, створювати та моніторити віртуальні машини і контейнери.

Ключові переваги Proxmox VE включають комплексну віртуалізацію з підтримкою як KVM, так і LXC, що забезпечує гнучкість і ефективність. Інтегрований веб-інтерфейс дозволяє легко управляти всіма аспектами віртуалізації з однієї панелі управління, що значно підвищує ефективність роботи адміністраторів. Платформа також підтримує кластеризацію для високої доступності, різноманітні варіанти зберігання, а також розширені мережеві можливості, включаючи інтеграцію з SDN. Proxmox VE забезпечує високу надійність і безпеку системи через механізми резервного копіювання та відновлення, а також підтримує міграцію в реальному часі, що дозволяє мінімізувати час простою.

За результатами аналізу документації та можливостей налаштувань Proxmox VE обрані наступні заходи безпеки – налаштування двофакторної аутентифікації, контролю доступу користувачів та брандмауера. Разом ці заходи забезпечують багаторівневий захист, де кожен елемент покриває різні аспекти безпеки: автентифікацію, управління доступом та захист мережі. Всі три заходи інтегруються в загальну політику безпеки Proxmox VE, забезпечуючи надійний та комплексний захист системи [7].

2.2 Двофакторна аутентифікація в Proxmox VE

Двофакторна аутентифікація (2FA) – це метод захисту доступу, що використовує два фактори для підтвердження ідентичності користувача. Двофакторна аутентифікація є ефективним засобом захисту, оскільки вимагається не лише пароль для доступу до облікового запису, але й додаткового підтвердження через інший фактор, такий як одноразовий код або фізичний ключ. Це ускладнює вхід в обліковий запис зловмисникам навіть у випадках, коли пароль став відомий.

Двофакторна аутентифікація дозволяє організаціям знижувати імовірність успішних кібератак, бо навіть у випадку витоку паролів не вистачить для несанкціонованого доступу до системи.

Налаштувати другий фактор аутентифікації можна легко та зручно у веб-панелі керування Proxmox. На рисунку 2.2 зображено меню додавання методів двофакторної аутентифікації у Proxmox VE.

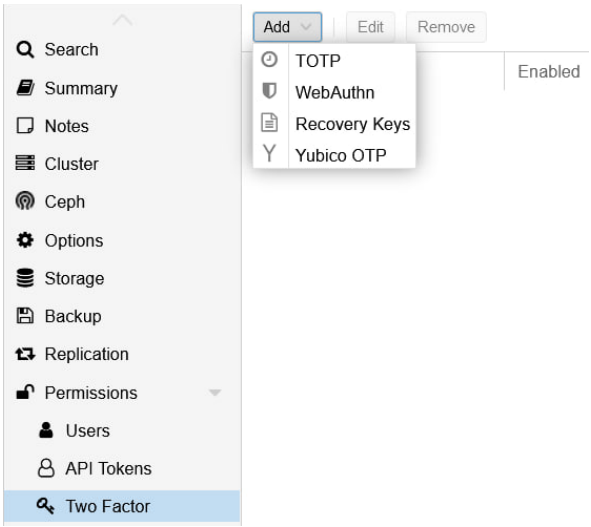

Рисунок 2.2 – Меню додавання методів двофакторної аутентифікації у Proxmox VE

В Proxmox є можливість налаштувати різні види 2FA:

– TOTP (Time-based One-Time Password). Це алгоритм генерації одноразових паролів, які залежать від часу. Він базується на симетричному

ключі, який спільно використовується між аутентифікатором (наприклад, мобільним додатком) і сервером, який перевіряє автентичність [8].

– YubiKey OTP (One-Time Password). Це одноразовий пароль, що генерується апаратним ключем YubiKey. Кожен YubiKey OTP включає унікальний код, який автоматично вводиться під час натискання на фізичну кнопку на пристрої YubiKey. Цей код може бути використаний лише один раз і вимагається для аутентифікації користувача.

– WebAuthn (Web Authentication). Це відкритий стандарт для аутентифікації веб-профілів. Він надає механізм для використання різних пристроїв безпеки, таких як апаратні ключі або TPM (Trusted Platform Modules) на комп'ютерах або смартфонах, для аутентифікації на веб-сайтах.

На рисунку 2.3 зображено вікно налаштування аутентифікації TOTP.

Рисунок 2.3 – Вікно налаштувань методу TOTP

Щоб уникнути ситуацій, коли втрата смартфону чи ключа безпеки заблокує можливість використовувати акаунт, існує можливість налаштувати декілька факторів аутентифікації. Після налаштування другого фактору

надається список ключів відновлення. Їх потрібно зберігати в безпечному місці. Кожен ключ можна використати лише один раз. Це гарантує доступ до акаунту в разі, якщо інші фактори аутентифікації втрачені.

Другий фактор аутентифікації надає більший рівень безпеки, проте також може бути скомпроментований, наприклад методом «грубої сили» (brute force атака), тому користувачі будуть заблоковані після великої кількості невдалих спроб аутентифікації з другим фактором. Для TOTP – 8 невдалих спроб вимикають другі фактори, але їх можна розблокувати, використовуючи ключі відновлення. Якщо TOTP був єдиним доступним фактором, то потрібно втручання адміністратора. Ключі WebAuthn менш чутливі до атак, тому ліміт невдалих спроб для них вищий і становить 100 спроб, проте після перевищення ліміту всі другі фактори блокуються на годину. Адміністратор може розблокувати двофакторну аутентифікацію користувача в будь-який час через список користувачів в інтерфейсі або командний рядок.

Proxmox VE пропонує різні види двофакторної аутентифікації (2FA), забезпечуючи високий рівень безпеки для користувачів. Зокрема, доступні такі методи, як TOTP, YubiKey OTP та WebAuthn, кожен з яких має свої унікальні характеристики та переваги.

2.3 Контроль доступу користувачів в Proxmox VE

Для того, щоб користувач міг виконати певну дію, наприклад, створити, змінити або видалити частину конфігурації віртуальної машини, він повинен мати відповідні дозволи. Користувачі в Proxmox VE можуть мати різні рівні доступу та виконувати різні функції залежно від призначених їм ролей. Гнучка система керування дозволами дозволяє точно налаштовувати доступ для різних користувачів та груп, що підвищує безпеку та ефективність управління ресурсами [9].

Proxmox VE використовує систему управління дозволами, яка базується на ролях і шляхах. У цій системі запис у таблиці дозволів дозволяє користувачеві,

групі або токену взяти на себе певну роль при доступі до об'єкта або шляху. Це означає, що таке правило доступу можна представити у вигляді трійки: (шлях, користувач, роль), (шлях, група, роль) або (шлях, токен, роль). У цій трійці роль містить набір дозволених дій, а шлях представляє ціль цих дій.

Створити нового користувача можна як у веб-інтерфейсі Proxmox VE, так і в терміналі керування гіпервізором. На рисунку 2.4 зображено вікно створення нового користувача у веб-інтерфейсі Proxmox VE.

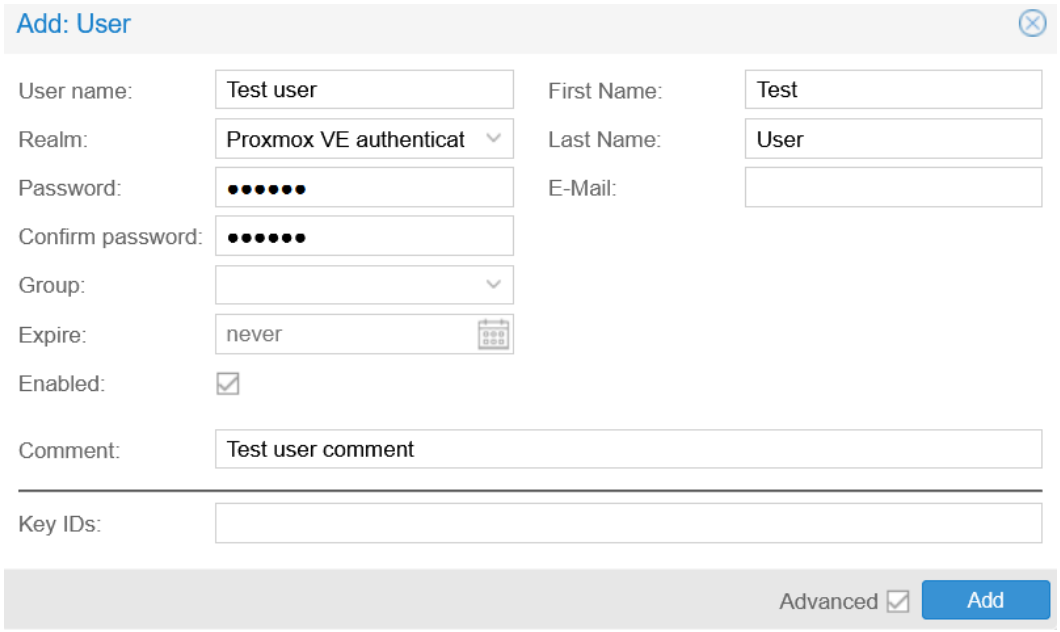

Рисунок 2.4 – Вікно створення нового користувача у веб-інтерфейсі

Таким чином, система управління дозволами Proxmox VE забезпечує гнучке і точне управління доступом до різних об'єктів і конфігурацій віртуальних машин. Кожен користувач, група або токен має суворо визначені права, які дозволяють або забороняють виконання певних дій в межах заданого шляху. Це забезпечує високий рівень безпеки і контроль над доступом до ресурсів, дозволяючи адміністратору точно налаштовувати права доступу відповідно до потреб організації або проекту [10].

Роль – це список привілеїв. Proxmox VE постачається з низкою попередньо визначених ролей, які задовольняють більшість вимог.

На рисунку 2.4 зображено перелік ролей та їх привілеїв в Proxmox VE.

Bui	Name ↓	Privileges
Yes	PVEVMUser	VM.Audit VM.Backup VM.Config.CDROM VM.Config.Cloudinit VM.Console VM.PowerMgmt
Yes	PVEVMAdmin	VM.Allocate VM.Audit VM.Backup VM.Clone VM.Config.CDROM VM.Config.CPU VM.Config.Cloudinit VM.Config.Network VM.Config.Options VM.Console VM.Migrate VM.Monitor VM.PowerMgmt VM.Sna
Yes	PVEUserAdmin	Group.Allocate Realm.AllocateUser User.Modify
Yes	PVETemplateUser	VM.Audit VM.Clone
Yes	PVESysAdmin	Sys.Audit Sys.Console Sys.Syslog
Yes	PVESDNUser	SDN.Audit SDN.Use
Yes	PVESDNAdmin	SDN.Allocate SDN.Audit SDN.Use
Yes	PVEPoolUser	Pool.Audit
Yes	PVEPoolAdmin	Pool.Allocate Pool.Audit
Yes	PVEMappingUser	Mapping.Audit Mapping.Use
Yes	PVEMappingAdmin	Mapping.Audit Mapping.Modify Mapping.Use
Yes	PVEDatastoreUser	Datastore.AllocateSpace Datastore.Audit
Yes	PVEDatastoreAdmin	Datastore.Allocate Datastore.AllocateSpace Datastore.AllocateTemplate Datastore.Audit
Yes	PVEAuditor	Datastore.Audit Mapping.Audit Pool.Audit SDN.Audit Sys.Audit VM.Audit
Yes	PVEAdmin	Datastore.Allocate Datastore.AllocateSpace Datastore.AllocateTemplate Datastore.Audit Group.Alloca Realm.AllocateUser SDN.Allocate SDN.Audit SDN.Use Sys.Audit Sys.Console Sys.Syslog User.Modif VM.Config.CDROM VM.Config.CPU VM.Config.Cloudinit VM.Config.Disk VM.Config.HWType VM.Cor VM.Console VM.Migrate VM.Monitor VM.PowerMgmt VM.Snapshot VM.Snapshot.Rollback
Yes	NoAccess	-

Рисунок 2.4 – Перелік ролей та їх привілеїв

Список попередньо визначених ролей досить великий, але можна виділити наступні:

– NoAccess – не має привілеїв (використовується для заборони доступу).

– PVEAuditor – має доступ лише на читання.

– PVEVMUser – перегляд, резервне копіювання, налаштування CD-ROM, консоль ВМ, керування живленням ВМ.

– PVEUserAdmin – керування користувачами.

– PVEVMAdmin – повне адміністрування віртуальних машин.

– PVEAdmin – може виконувати більшість завдань, але не має прав на зміну системних налаштувань (Sys.PowerMgmt, Sys.Modify, Realm.Allocate) або дозволів (Permissions.Modify).

– Administrator – має повні права.

Додавати нові ролі можна також за допомогою графічного інтерфейсу або за допомогою інструменту командного рядка pveum (скорочення від Proxmox VE User Manager).

Привілеї – це права на виконання певних дій. Для спрощення керування привілеї згруповані у ролі, які потім можна використовувати у таблиці дозволів. Привілеї не можуть бути безпосередньо призначені користувачам або шляхам, якщо вони не є частиною ролі. Такий підхід дозволяє адміністратору створювати ролі, що складаються з одного або декількох привілеїв, і призначати ці ролі користувачам, групам або токенам відповідно до їхніх обов'язків і потреб. Завдяки цьому система управління дозволами стає більш організованою і зручною для використання, оскільки адміністратору не потрібно керувати окремими привілеями для кожного користувача або шляху. Привілеї можна розділити на декілька груп: привілеї, пов’язані з вузлом/системою, привілеї, пов’язані з віртуальними машинами та привілеї, пов’язані зі сховищем.

Основні привілеї, пов’язані з вузлом/системою:

– Group.Allocate – створення/зміна/видалення груп.

– Mapping.Audit – перегляд відображення ресурсів.

– Mapping.Modify – керування відображеннями ресурсів.

– Permissions.Modify – модифікація дозволів на доступ.

– Sys.Audit – перегляд стану/конфігурації вузла, конфігурації кластера.

– Sys.Console – консольний доступ до вузла.

– Sys.Modify – створення/зміна/видалення мережевих параметрів вузла.

– Sys.PowerMgmt – керування живленням вузла (запуск, зупинка, скидання, вимкнення).

– Sys.Syslog – перегляд системного журналу.

– User.Modify – створення/зміна/видалення доступу та даних користувача.

Основні привілеї, пов’язані з віртуальними машинами:

– VM.Allocate – створення/видалення ВМ на сервері.

– VM.Audit – перегляд конфігурації ВМ.

– VM.Backup – резервне копіювання/відновлення ВМ.

– VM.Clone – клонувати/копіювати ВМ.

– VM.Config.CPU – змінити налаштування процесора.

– VM.Config.Memory – зміна параметрів пам'яті.

– VM.Config.Network – додавання/зміна/видалення мережевих пристроїв.

– VM.PowerMgmt – керування живленням (запуск, зупинка, скидання, вимкнення).

– VM.Snapshot – створення/видалення знімків ВМ.

Привілеї, пов’язані із сховищем:

– Datastore.Allocate – створення/зміна/видалення сховища даних і видалення томів.

– Datastore.AllocateSpace – виділення місця у сховищі даних.

– Datastore.AllocateTemplate – виділення/завантаження шаблонів та ISO-образів.

– Datastore.Audit – перегляд/перегляд сховища даних.

Дозволи доступу призначаються об'єктам, таким як віртуальні машини, сховища або пули ресурсів. В Proxmox використовуються шляхи, подібні до файлової системи, щоб звертатися до цих об'єктів. Такі шляхи утворюють природне дерево, і дозволи вищих рівнів (коротші шляхи) можуть поширюватися вниз у цій ієрархії.

2.4 Брандмауер в Proxmox VE

Брандмауер – це мережевий пристрій або програмне забезпечення, яке контролює і фільтрує вхідний та вихідний мережевий трафік на основі встановлених правил безпеки. Це необхідно для захисту комп'ютерних систем від несанкціонованого доступу [11].

Proxmox VE має вбудований брандмауер, який дозволяє користувачам встановлювати правила для контролю мережевого трафіку, що проходить через віртуальні машини і контейнери. Брандмауер Proxmox підтримує як IPv4, так і IPv6 і надає можливості для створення глобальних, кластерних або локальних правил безпеки. Це забезпечує гнучке налаштування політики безпеки на різних рівнях інфраструктури, що допомагає захистити систему від різноманітних загроз.

Вбудований брандмауер також підтримує фільтрацію на основі адрес, портів і протоколів, що дозволяє користувачам точно налаштовувати правила доступу відповідно до їхніх потреб. Інтеграція з іншими функціями Proxmox VE, такими як резервне копіювання та управління ресурсами, робить брандмауер потужним інструментом для забезпечення комплексної безпеки віртуалізованого середовища.

Налаштувати правила можна за допомогою графічного інтерфейсу або шляхом редагування конфігураційних файлів безпосередньо. Правила брандмауера складаються з напрямку (IN або OUT) і дії (ACCEPT, DENY, REJECT). Є можливість використовувати макроси, які містять заздалегідь визначені набори правил і опцій [12].

На рисунку 2.5 зображено вікно створення правил у веб-інтерфейсі Proxmox VE.

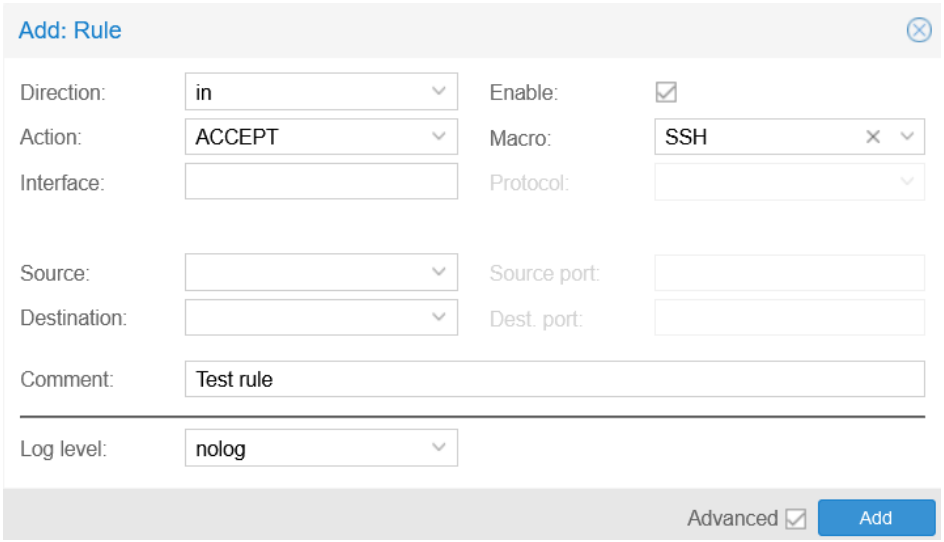

Рисунок 2.5 – Вікно створення правил брандмауера

Браундмауер Proxmox VE групує мережу на логічні зони:

– Зона хоста (вузла/ноди): трафік з/до вузла кластера.

– Зона віртуальної машини: трафік з/до віртуальної машини.

Для кожної зони можна визначити правила брандмауера для вхідного та вихідного трафіку. Також є загальна зона кластера, в якій можна визначити основні правила, групи, списки та використовувати їх в різних хостах та

віртуальних машинах. На рисунку 2.6 наведено схему організації основних компонентів гіпервізора Proxmox VE.

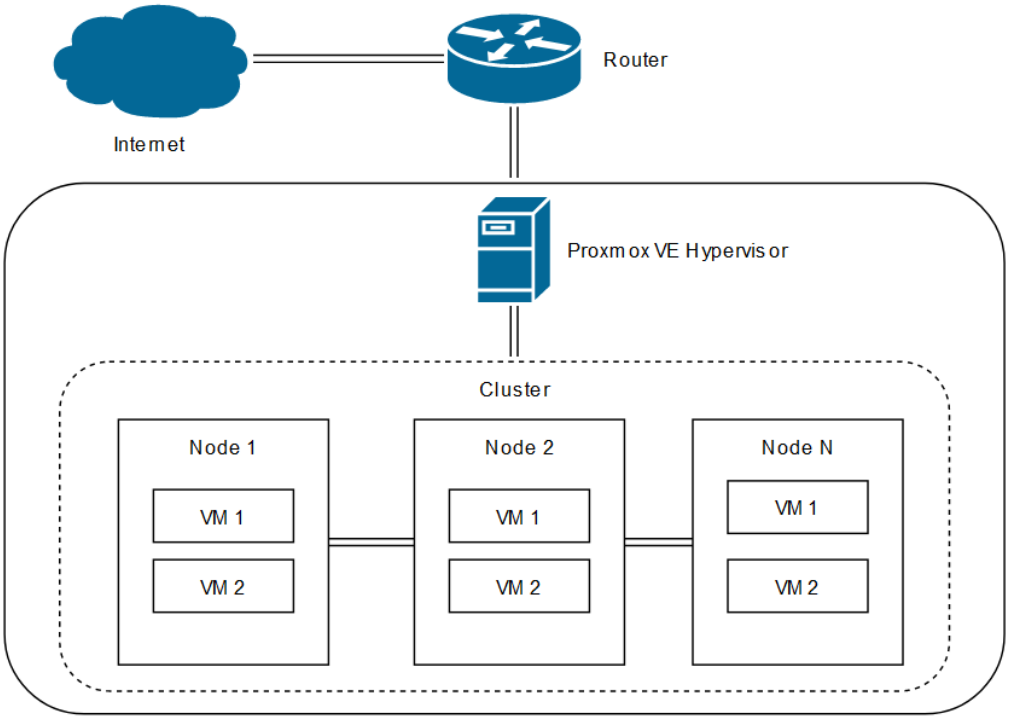

Рисунок 2.6 – Схема організації компонентів Proxmox VE

Схема відображає ієрархічну структуру Proxmox VE, що складається з таких основних компонентів:

– Інтернет: зовнішня мережа, з якої можуть надходити запити та дані до локальної інфраструктури.

– Роутер (Router): мережевий пристрій, який забезпечує з'єднання між Інтернетом та внутрішньою мережею, в якій розташований кластер Proxmox VE.

– Proxmox VE Hypervisor: фізичний сервер, на якому встановлена платформа віртуалізації Proxmox VE. Він керує ресурсами та забезпечує створення та управління віртуальними машинами.

– Кластер (Cluster): група вузлів (нод), об'єднаних для спільного використання ресурсів і забезпечення високої доступності. Кластер дозволяє управляти всіма вузлами як єдиною системою.

– Вузли (Nodes): фізичні сервери всередині кластеру. Кожен вузол виконує роль гіпервізора і може містити кілька віртуальних машин.

– Віртуальні машини (Virtual Machines, VMs): гостьові системи, які працюють на кожному з вузлів. Вони використовують ресурси вузла для виконання своїх задач.

При налаштуванні брандмауера в Proxmox VE важливо враховувати структуру, щоб забезпечити безпечний доступ між Інтернетом та внутрішньою мережею на відповідних рівнях, захищаючи кластери з вузлами та віртуальними машинами від несанкціонованого доступу.

Кожен віртуальний мережевий пристрій має власний прапорець увімкнення брандмауера. Таким чином, можна вибірково увімкнути брандмауер для кожного інтерфейсу. Це потрібно на додаток до загального параметра увімкнення брандмауера. Усі конфігурації брандмауера зберігаються у файловій системі кластера Proxmox VE. Завдяки цьому файли автоматично поширюються на всі вузли кластера, а служба pve-firewall автоматично оновлює основні правила iptables при внесенні змін.

За замовчуванням брандмауер повністю вимкнуто. При увімкненні брандмауера, за замовчуванням увесь трафік до хостів буде заблоковано. Винятками є лише WebGUI (порт 8006) та SSH (порт 22) з локальної мережі. Тому, щоб віддалено адмініструвати хости Proxmox VE, необхідно створити правила, які дозволять трафік з віддалених IP-адрес до веб-інтерфейсу (порт 8006), а також дозволити SSH (порт 22) і, за потреби, SPICE (порт 3128). Щоб полегшити цей процес, можна створити набір IP-адрес з потрібною назвою і додати до нього всі віддалені IP-адреси. Це дозволить автоматично створити всі необхідні правила брандмауера для віддаленого доступу до графічного інтерфейсу [13].

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХОДІВ ЗАХИСТУ В PROXMOX VE

3.1 Налаштування двофакторної аутентифікації

В цьому пункті наведено процес налаштування двофакторної аутентифікації TOTP для root користувача за допомогою інструментів веб-інтерфейсу Proxmox VE. Необхідно увійти до веб-інтерфейсу під іменем користувача root та перейти на вкладку налаштувань двофакторної аутентифікації та обрати пункт «TOTP». На рисунку 3.1 зображено меню налаштування двофакторної аутентифікації з можливістю вибору методу другого фактору.

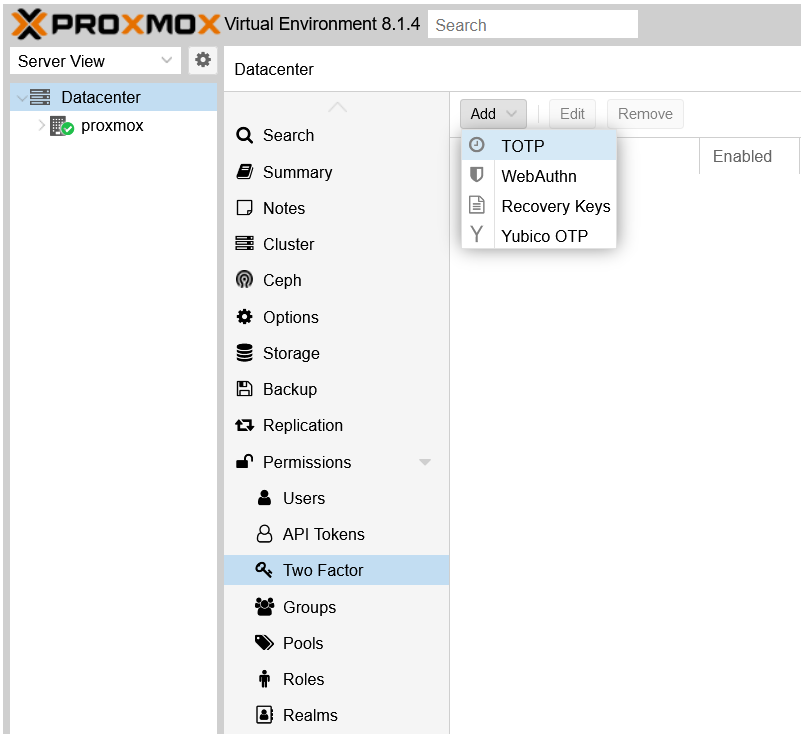

Рисунок 3.1 – Меню налаштування двофакторної аутентифікації у веб-інтерфейсі Proxmox VE

Після вибору методу другого фактору аутентифікації з’являється діалогове вікно налаштувань, в якому можна задати параметри, такі як, вибір користувача, до якого необхідно застосувати другий фактор, опис девайсу аутентифікації, опис власника. Також необхідно завантажити відповідний застосунок для

аутентифікації на пристрій, з якого необхідно буде підтверджувати другий фактор, наприклад, Google Authenticator, FreeOTP та інші. Необхідно відсканувати QR-код, відображений в діалоговому вікні та ввести згенерований тимчасовий код для підтвердження. На рисунку 3.2 зображено діалогове вікно з налаштуванням TOTP для root користувача.

Рисунок 3.2 – Діалогове вікно налаштування другого фактору аутентифікації для root користувача

Після успішного додавання другого фактору при наступній спробі входу у веб-інтерфейс після перевірки введених імені та паролю користувача з’явиться додаткове діалогове вікно для введення тимчасового коду.

На рисунку 3.3 зображено діалогове вікно входу у веб-інтерфейс Proxmox VE.

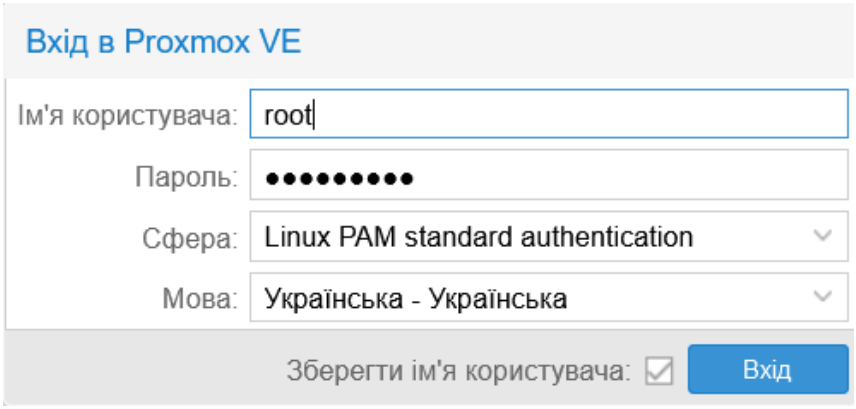

Рисунок 3.3 – Діалогове вікно входу у веб-інтерфейс Proxmox VE

На рисунку 3.4 зображено додаткове діалогове вікно підтвердження другого фактору аутентифікації.

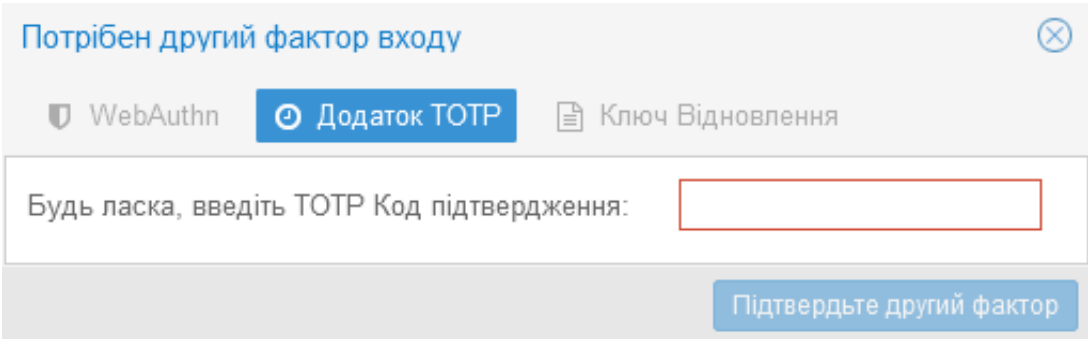

Рисунок 3.4 – Діалогове вікно підтвердження другого фактору аутентифікації

На рисунку 3.5 зображено згенерований тимчасовий код другого фактору для root користувача Proxmox VE з використанням застосунку Google Authenticator.

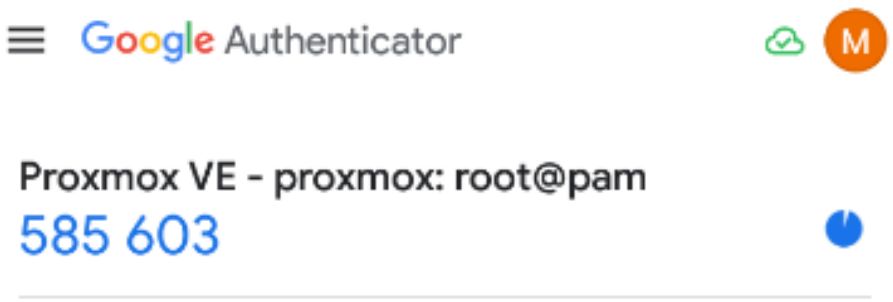

Рисунок 3.5 – Згенерований тимчасовий код у застосунку Google Authenticator

Згенерований у застосунку код необхідно ввести в діалогове вікно підтвердження другого фактору. На рисунку 3.6 зображено введення тимчасового коду в діалогове вікно підтвердження другого фактору аутентифікації.

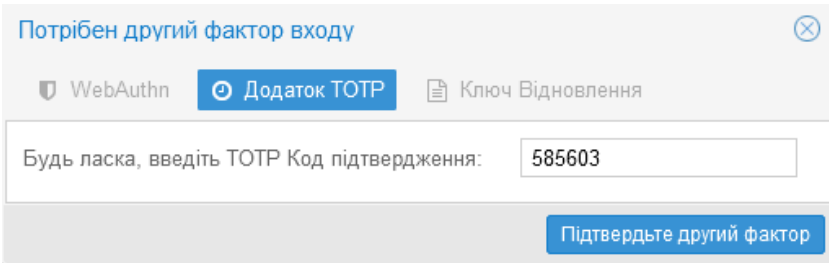

Рисунок 3.6 – Введення тимчасового коду в діалогове вікно підтвердження другого фактору аутентифікації

Для уникнення ситуацій, коли пристрій, за допомогою якого відбувається підтвердження другого фактору буде втрачений, існує можливість згенерувати та зберегти ключі відновлення. Для цього необхідно в меню налаштувань двофакторної аутентифікації обрати пункт «Ключі відновлення».

На рисунку 3.7 зображено меню налаштувань двофакторної аутентифікації з пунктом «Ключі відновлення».

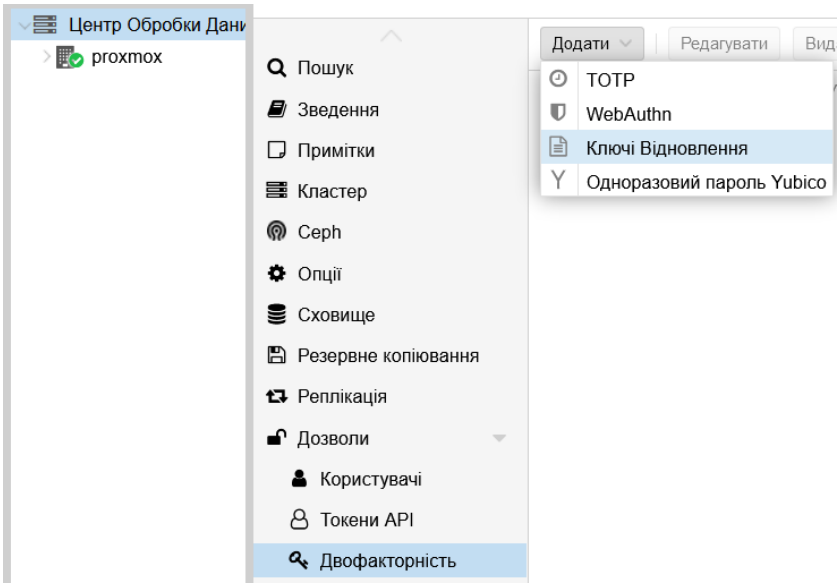

Рисунок 3.7 – Пункт «Ключі відновлення» в меню налаштувань двофакторної аутентифікації

З’являється діалогове вікно, в якому необхідно обрати користувача, для якого необхідно згенерувати ключі, після чого, з’явиться перелік ключів відновлення з можливістю скопіювати або завантажити їх. На рисунку 3.8 зображено діалогове вікно вибору користувача, для якого необхідно згенерувати ключі відновлення.

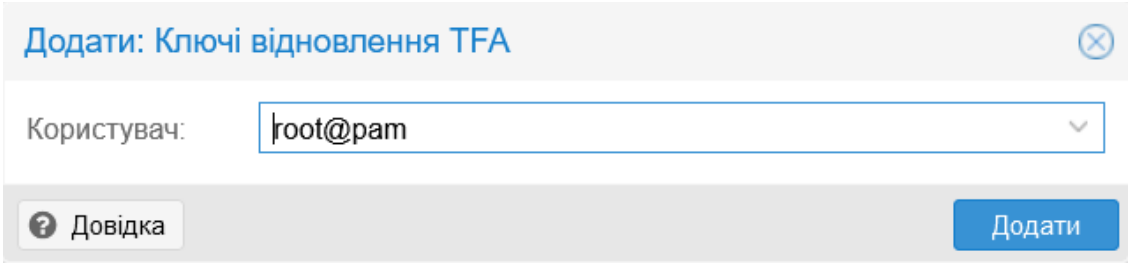

Рисунок 3.8 – Вікно вибору користувача для генерації ключів відновлення

На рисунку 3.9 зображено вікно із згенерованими ключами відновлення для користувача root.

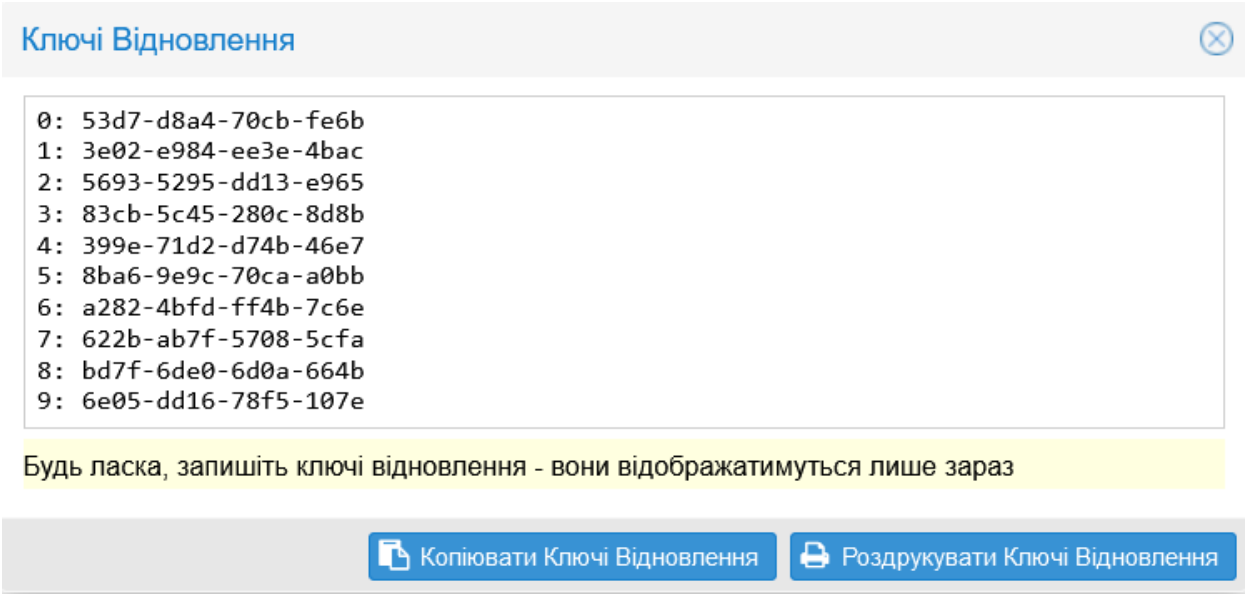

Рисунок 3.9 – Вікно із згенерованими ключами відновлення

Ключі відновлення потрібно зберігати в надійному місці і варто врахувати, що кожен ключ відновлення можна використати лише один раз.

3.2 Налаштування контролю доступу користувачів

Proxmox VE має гнучку систему управління доступом користувачів, що дозволяє детально контролювати, хто має доступ до сервера та які дії може виконувати. Ця система ґрунтується на ролях та привілеях, які визначають рівень доступу користувача до різних функцій та ресурсів сервера [14].

Щоб розмежувати виконання обов'язків, необхідно створити нового користувача та задати йому роль адміністратора. За допомогою наступних команди можна створити нового користувача та задати пароль:

```
$ pveum user add Administrator@pve -comment "Administrator"
$ pveum passwd Administrator@pve
```

Ролі можна задавати одразу для кожного користувача, проте кращим варіантом є створення групи з певними ролями і приєднувати користувачів до потрібної групи. Переглянути доступні ролі та їх привілеї можна за допомогою наступної команди:

```
$ pveum role list
```

На рисунку 3.10 зображено список доступних ролей та їх привілеїв.

Administrator	Datastore.Allocate,Datastore.AllocateSpace,Datastore.AllocateTemplate,Datastore.Audit,
NoAccess	
PVEAdmin	Datastore.Allocate,Datastore.AllocateSpace,Datastore.AllocateTemplate,Datastore.Audit,
PVEAuditor	Datastore.Audit,Mapping.Audit,Pool.Audit,SDN.Audit,Sys.Audit,VM.Audit
PVEDatastoreAdmin	Datastore.Allocate,Datastore.AllocateSpace,Datastore.AllocateTemplate,Datastore.Audit
PVEDatastoreUser	Datastore.AllocateSpace,Datastore.Audit
PVEMappingAdmin	Mapping.Audit,Mapping.Modify,Mapping.Use
PVEMappingUser	Mapping.Audit,Mapping.Use
PVEPoolAdmin	Pool.Allocate,Pool.Audit
PVEPoolUser	Pool.Audit
PVESDNAdmin	SDN.Allocate,SDN.Audit,SDN.Use
PVESDNUser	SDN.Audit,SDN.Use
PVESysAdmin	Sys.Audit,Sys.Console,Sys.Syslog
PVETemplateUser	VM.Audit,VM.Clone
PVEUserAdmin	Group.Allocate,Realm.AllocateUser,User.Modify

Рисунок 3.10 – Список доступних ролей та їх привілеїв

Створити групу та присвоїти їй роль адміністратора можна за допомогою наступних команд:

```
$ pveum group add admin -comment “System Administrators”
$ pveum acl modify / -group admin -role Administrator
```

Перша команда створює групу з назвою «admin» (рис. 3.11), а друга команда модифікує контроль доступу шляхом присвоєння ролі Administrator для групи користувачів «admin», надаючи повний набір дозволів для керування Proxmox VE, включаючи створення віртуальних машин, керування сховищем та налаштування мережі.

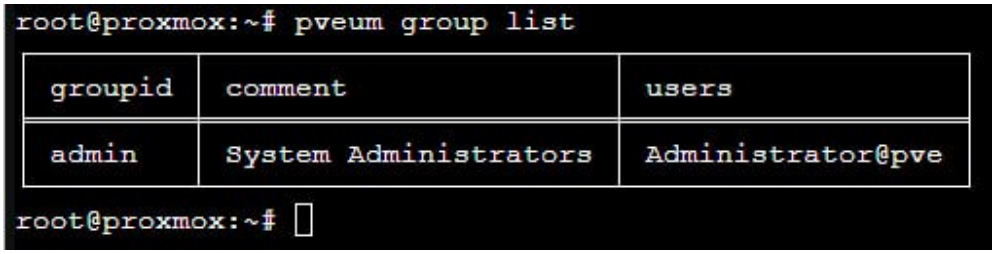

Рисунок 3.11 – Створена група адміністраторів

Щоб додати користувача до створеної групи адміністраторів, необхідно виконати наступну команду:

```
$ pveum user modify Administrator@pve -group admin
```

Якщо немає необхідності створювати групу користувачів, то є можливість одразу присвоїти роль для певного користувача. В лістингу 3.1 наведено команди, за допомогою яких можна створити нового користувача та задати йому роль «PVEUserAdmin».

Лістинг 3.1 – Команди для створення нового користувача та призначення йому ролі «PVEUserAdmin»

```
$ pveum user add userAdministrator@pve -comment "User Administrator"
$ pveum passwd userAdministrator@pve
```

Продовження лістингу 3.1

```
$ pveum acl modify /access -user userAdministrator@pve – role
PVEUserAdmin
```

Ця роль дозволяє додавати та видаляти користувачів, а також змінювати їх атрибути, наприклад пароль. Щоб переконатись в правильному призначенні ролі для користувача, можна скористатись наступною командою перевірки дозволів:

```
$ pveum user permissions userAdministrator@pve
```

На рисунку 3.12 зображено результат виконання перевірки дозволів користувача «userAdministrator».

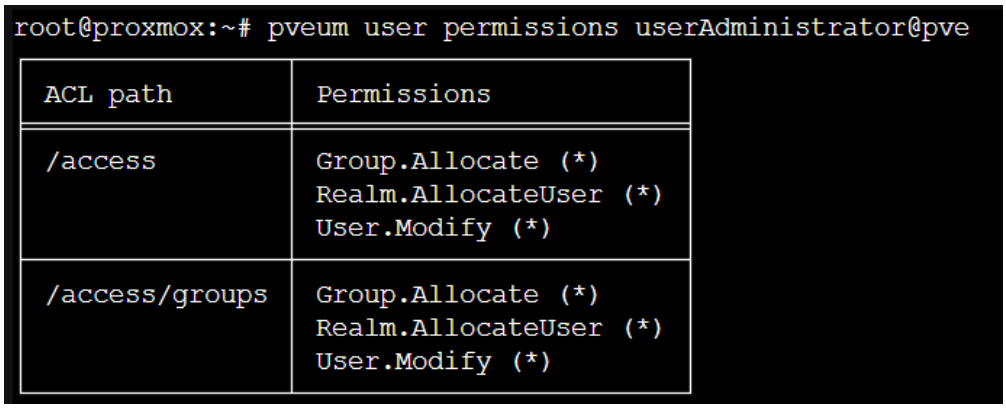

Рисунок 3.12 – Результат виконання команди перевірки дозволів для користувача «userAdministrator»

Налаштовані механізми контролю доступу забезпечують високий рівень безпеки, дозволяють точно контролювати дії користувачів і ефективно керувати правами доступу до ресурсів Proxmox VE.

3.3 Налаштування брандмауера

Proxmox VE забезпечує розширені та гнучкі можливості для налаштування брандмауера на трьох рівнях: кластерному, вузловому та рівні віртуальних машин/контейнерів. Це дозволяє централізовано управляти політиками безпеки

для всіх серверів у кластері, забезпечувати контроль доступу на рівні окремих вузлів, а також детально управляти мережевими правилами для кожної віртуальної машини або контейнера.

IPSet списки – це набори IP-адрес або мереж, які використовуються для швидкого та ефективного застосування правил брандмауера. Списки дозволяють групувати адреси, що пришвидшує налаштування брандмауера, адже зникає потреба вручну налаштовувати адреси при створенні правил, натомість використовувати готові набори.

Налаштування списків IPSet на рівні кластера в Proxmox VE забезпечує ідентичні правила для всіх вузлів одночасно та зменшує потенційні помилки, що можуть виникнути при налаштуванні кожного вузла окремо. Створити IPSet список дозволених IP-адрес можна за допомогою наступної команди:

```
$ pvesh create /cluster/firewall/ipset --name allow_ip --comment
"Allowed IP addresses"
```

Додати одну або простір IP-адрес в створений IPSet список можна за допомогою наступної команди:

```
$ pvesh create /cluster/firewall/ipset/allow_ip – cidr 192.168.28.0
/24 --comment "Local network"
```

Аналогічним методом можна створити список заборонених IP-адрес та додати туди потрібні адреси за допомогою наступних команд:

```
$ pvesh create /cluster/firewall/ipset --name forbidden_ip --comment
"Forbidden IP addresses"
$ pvesh    create    /cluster/firewall/ipset/forbidden_ip    --cidr
192.168.28.244 --comment "Forbidden device IP in local network"
```

Створені списки IPSet можна переглянути за допомогою команди:

```
 $ pvesh get /cluster/firewall/ipset
```

На рисунку 3.13 зображено результат вище наведеної команди, яка виводить таблицю наявних IPSet списків на рівні кластера.

```
root@proxmox:~# pvesh get /cluster/firewall/ipset
```

digest	name	comment
f5e9aaa6e0544f1f893b9aebc4374ffabe9dc9b4	allow_ip	Allowed IP addresses
f5e9aaa6e0544f1f893b9aebc4374ffabe9dc9b4	forbidden_ip	Forbidden IP addresses

Рисунок 3.13 – Таблиця наявних IPSet списків на рівні кластера

Результат виконання команди відображає таблицю, де:

– digest: унікальний ідентифікатор (хеш) для кожного IPSet списку, який використовується для ідентифікації цього списку в системі.

– name: назва IPSet списку, яка вказує на його призначення або дозволену/заборонену групу IP-адрес.

– comment: коментар, що надає додаткову інформацію про цей IPSet список.

Також можна переглянути вміст IPSet списків за допомогою наступної команди:

```
$ pvesh get /cluster/firewall/ipset/<ipsetname>
```

Параметр <ipsetname> необхідно змінити на потрібну назву IPSet списку.

На рисунку 3.14 наведено таблицю вміст IPSet списку дозволених адрес, а на рисунку 3.15 – заборонених адрес.

```
root@proxmox:~# pvesh get /cluster/firewall/ipset/allow_ip
```

cidr	digest	comment	nomatch
192.168.28.0/24	61d90228fd765ba8c34f8fcf95e91f9c873a4cf7	Local network	

Рисунок 3.14 – Таблиця з вмістом IPSet списку дозволених IP-адрес

```
root@proxmox:~# pvesh get /cluster/firewall/ipset/forbidden_ip
```

cidr	digest	comment	nomatch
192.168.28.244	9adef19e635a091d956ddb5e93881a46c91ae11d	Forbidden device IP in local network	

Рисунок 3.15 – Таблиця з вмістом IPSet списку заборонених IP-адрес

В процесі налаштування брандмауера за допомогою команд терміналу, відповідні дії можна виконувати у веб-інтерфейсі Proxmox VE. Виконані налаштування в терміналі одразу відображаються в графічному веб-інтерфейсі, і навпаки – налаштування, що здійснюються в графічному веб-інтерфейсі автоматично генерують відповідні зміни в конфігураційних файлах.

На рисунку 3.16 зображено створені за допомогою команд терміналу IPSet списки у веб-інтерфейсі Proxmox VE.

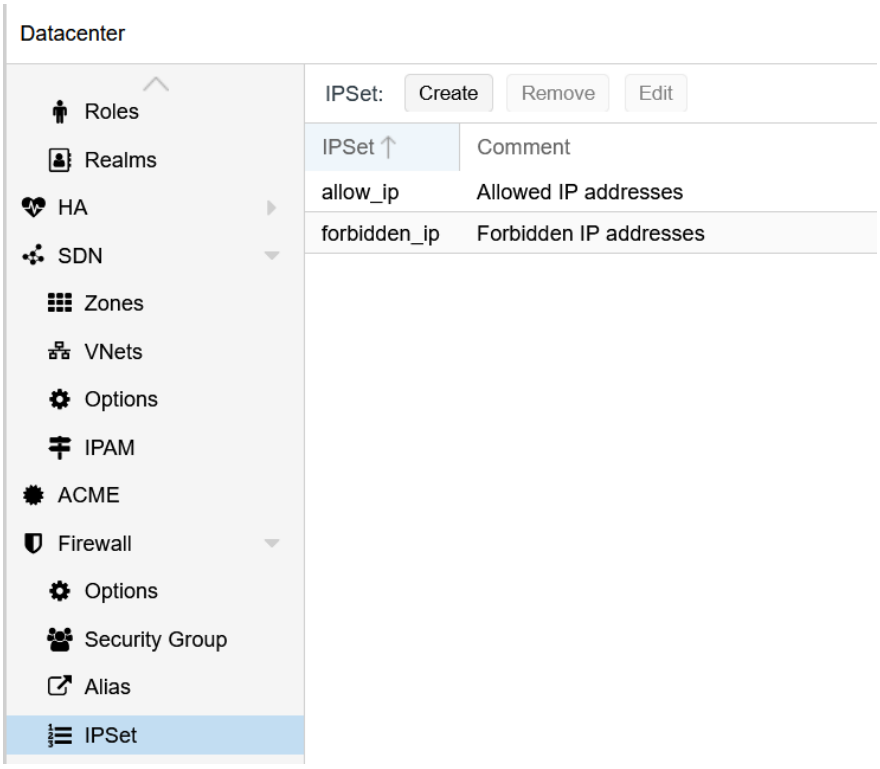

Рисунок 3.16 – IPSet списки у веб-інтерфейсі Proxmox VE

Наступним етапом є створення груп безпеки, які призначені для ефективної організації структури безпеки. Вони дозволяють об’єднувати правила брандмауера в окремі групи, що значно спрощує адміністрування, оскільки замість індивідуального налаштування правил на кожному рівні існує

можливість використовувати групи з попередньо встановленими наборами правил.

Створити групу безпеки для правил Accept, що дозволяють проходити пакетам, які відповідають вказаним параметрам правила, можна, виконавши наступну команду:

```
 $ pvesh create /cluster/firewall/groups --group web_allow --comment
"Allow access to web-interface and SSH"
```

Аналогічно для правил Deny, що забороняють проходити пакетам, які відповідають вказаним параметрам правила, можна створити групу безпеки за допомогою команди:

```
$ pvesh create /cluster/firewall/groups --group web_deny --comment
"Deny access to web interface and SSH"
```

Наступним етапом є створення правил у відповідних групах безпеки. Для того, щоб додати правила, необхідно внести зміни в конфігураційний файл /etc/pve/firewall/cluster.fw. В лістингу 3.2 наведено правила дозволу групи безпеки web_allow.

Лістинг 3.2 – Правила дозволу групи безпеки web_allow

```
IN ACCEPT -source +dc/allow_ip -p tcp -dport 8006 # Allow access to
web-interface from allowed IP
IN SSH(ACCEPT)-source +dc/allow_ip # Allow SSH access from allowed
IP
```

Перше правило дозволяє доступ до веб-інтерфейсу Proxmox VE з внутрішньої мережі (IPSet списку) за протоколом TCP на порту 8006. Таким чином, лише пакети TCP, які приходять з відповідних дозволених IP-адрес, будуть пропущені через брандмауер для доступу до веб-інтерфейсу.

Друге правило дозволяє SSH-з'єднання до сервера Proxmox VE. Правило допускає весь мережевий трафік SSH з вказаного списку IPSet, що забезпечує віддалений доступ через SSH лише з визначених джерел.

Додатково до цих правил, для SSH використовується готовий макрос, який доступний в Proxmox VE, що спрощує конфігурацію, оскільки він автоматично визначає протокол та порт і дозволяє створювати правила швидше та зручніше.

В лістингу 3.3 наведено правила заборони групи безпеки web_deny.

Лістинг 3.3 – Правила заборони групи безпеки web_deny

```
IN DROP -source +dc/forbidden_ip -p tcp -dport 8006 # Deny access to web-interface from forbidden IP
IN SSH(DROP) -source +dc/forbidden_ip # Deny SSH access from forbidden IP
```

Перше правило забороняє доступ до веб-інтерфейсу Proxmox VE з IP-адрес, вказаних у списку forbidden_ip та інших адрес, які є поза списком дозволеної локальної мережі, за протоколом TCP на порту 8006.

Друге правило забороняє SSH-з'єднання до сервера Proxmox VE з IP-адрес, вказаних у списку forbidden_ip. Це правило відхиляє весь мережевий трафік SSH з цих IP-адрес, забезпечуючи, що віддалений доступ через SSH буде заблокований для вказаних джерел.

Щоб додати створені групи безпеки та увімкнути брандмауер, необхідно внести зміни у конфігураційних файлах на потрібних рівнях. Важливо врахувати послідовність використання груп безпеки, адже в Proxmox VE брандмауер отримує доступ до правил послідовно. Для того, щоб увімкнути брандмауер на рівні кластера, необхідно змінити наступний параметр в конфігураційному файлі /etc/pve/firewall/cluster.fw:

```
[OPTIONS]
enable: 1
```

Параметр enable використовується для увімкнення або вимкнення брандмауера відповідно до заданого значення:

– enable: 1 – увімкнення брандмауера.

– enable: 1 – вимкнення брандмауера.

На рисунку 3.17 наведено вміст конфігураційного файлу /etc/pve/firewall/cluster.fw, який містить налаштування брандмауера для всього кластеру Proxmox VE.

```
[OPTIONS]

enable: 1

[IPSET allow_ip] # Allowed IP addresses
192.168.28.0/24 # Local network

[IPSET forbidden_ip] # Forbidden IP addresses
192.168.28.244 # Forbidden device IP in local network

[RULES]

GROUP web_deny
GROUP web_allow

[group web_deny] # Deny access to web-interface and SSH
IN DROP -source +dc/forbidden_ip -p tcp -dport 8006 # Deny access to web-interface from forbidden IP
IN SSH(DROP) -source +dc/forbidden_ip # Deny SSH access from forbidden IP

[group web_allow] # Allow access to web-interface and SSH
IN ACCEPT -source +dc/allow_ip -p tcp -dport 8006 # Allow access to web-interface from allowed IP
IN SSH(ACCEPT) -source +dc/allow_ip # Allow SSH access from allowed IP
```

Рисунок 3.17 – Конфігураційний файл кластера Proxmox VE

Щоб застосувати правила на всіх рівнях, необхідно додати створені групи безпеки в конфігураційні файли кожного рівня та увімкнути брандмауер на кожному рівні. Така система організації рівні доступу надає можливість використовувати різні правила на різних рівнях, а при необхідності, застосувати попередньо створені правила на потрібних рівнях. Щоб додати групи безпеки на рівні хоста та застосувати набір правил цих груп, необхідно змінити конфігураційний файл /etc/pve/nodes/proxmox/host.fw шляхом написання параметрів, наведених в лістингу 3.4.

Лістинг 3.4 – Параметри конфігураційного файлу host.fw

```
[OPTIONS]
enable: 1
[RULES]
GROUP web_deny
GROUP web_allow
```

В блок правил RULES додаються дві групи безпеки, створені в минулих кроках, що відображає мету створення саме груп безпеки, адже після створення груп із правилами на кластерному рівні з’являється можливість використовувати їх на хостовому рівні чи на рівні віртуальних машин.

Щоб перезавантажити службу брандмауера в Proxmox VE, необхідно виконати наступну команду:

```
$ pve-firewall restart
```

Щоб перевірити роботу брандмауера та створених правил доступу чи заборони, можна спробувати здійснити вхід до веб-інтерфейсу Proxmox VE або здійснити спробу SSH-з’єднання до хосту з пристрою, IP-адреса якого визначена в списку заборонених адрес.

На рисунку 3.18 зображено спробу входу у веб-інтерфейс через браузер з IP-адреси, яка внесена в список заборонених адрес.

Рисунок 3.18 – Невдала спроба входу із забороненої IP-адреси

На рисунку 3.19 зображено спробу SSH-з’єднання до хосту із забороненої IP-адреси.

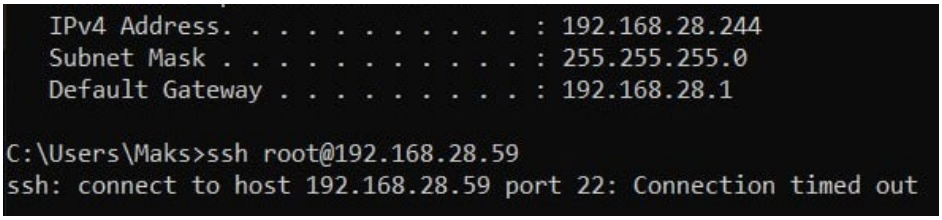

Рисунок 3.19 – Невдала спроба SSH-з’єднання до хосту

Правила успішно працюють на рівні хосту та блокують трафік із забороненої IP-адреси, проте не було використано групи безпеки із правилами на рівні віртуальних машин. На рисунку 3.20 зображено спробу SSH-з'єднання до віртуальної машини хосту із забороненої IP-адреси.

Рисунок 3.20 – Успішне SSH-з'єднання до ВМ хосту

Щоб застосувати правила брандмауера для віртуальної машини, необхідно внести зміни в конфігураційний файл відповідної віртуальної машини. В лістингу 3.5 наведено вміст конфігураційного файлу /etc/pve/firewall/100.fw, де 100 – це ID віртуальної машини.

Лістинг 3.5 – Параметри конфігураційного файлу 100.fw

```
[OPTIONS]
enable: 1
[RULES]
GROUP web_deny
GROUP web_allow
```

Внесені зміни вмикають брандмауер на рівні конкретної віртуальної машини та додають заздалегідь створені групи безпеки із правилами. Після внесення змін необхідно перезавантажити службу брандмауера та перевірити роботу правил.

На рисунку 3.21 зображено спробу SSH-з'єднання до віртуальної машини із забороненої IP-адреси.

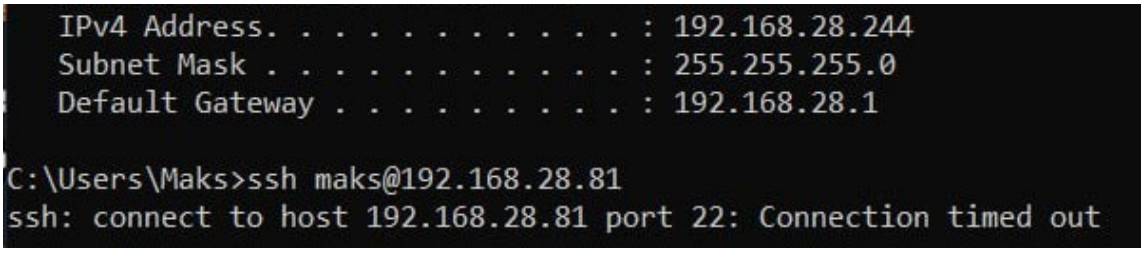

Рисунок 3.21 – Невдала спроба SSH-з’єднання до ВМ хосту

Заборонено доступ до веб-інтерфейсу та SSH-з’єднання користувачам з IP-адресами, внесеними до списку заборонених адрес, а також всім іншим користувачам, які не входять до локальної мережі дозволених адрес. Налаштовані правила та списки можна використовувати для гнучкого та ефективного налаштування брандмауера Proxmox VE на різних рівнях. Наприклад, застосовуючи створені групи правил можна надати певним користувачам доступ до керування хостом Proxmox VE, але заборонити доступ до керування віртуальними машинами за допомогою правил контролю доступу користувачів та правил брандмауера.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Ергономічні проблеми безпеки життєдіяльності

У контексті зростаючої уваги до здоров'я та безпеки на робочому місці, питання ергономічних проблем стають неабиякою проблемою для різних галузей діяльності. Ергономіка, як наука, що досліджує взаємозв'язок між людиною та її робочим оточенням, набуває все більшої важливості в умовах швидкого технологічного прогресу.

Ергономіка спрямована на оптимізацію безпеки, комфорту та продуктивності праці шляхом зменшення фізичного навантаження та стресу на організм. Загальновідомо, що здорове та комфортне робоче середовище має важливе значення для добробуту та продуктивності працівників [15].

В рамках організації робочого середовища, ергономіка відноситься до розробки та адаптації робочих зон, інструментів і устаткування з урахуванням потреб працівників. Використання принципів ергономіки дозволяє роботодавцям створити таке робоче місце, яке сприяє збереженню здоров'я та безпеці працівників, зменшує ризик виникнення травм і захворювань, а також підвищує задоволеність роботою та рівень продуктивності.

Робоче місце – це визначена зона простору, яка облаштована необхідним устаткуванням, де відбувається трудова діяльність працівника або групи працівників [15].

Організація робочого місця включає кілька ключових аспектів:

– оптимальне розташування робочого місця в межах виробничого приміщення для забезпечення ефективного використання простору та зручності працівників;

– раціональне розміщення обладнання та інструментів на робочих місцях, що сприяє зручності доступу та мінімізує зайві рухи;

– забезпечення належного освітлення, яке знижує зорове напруження та підвищує концентрацію, а також контроль за рівнем шуму і вібрацій для запобігання фізичному і психологічному дискомфорту;

– врахування специфіки та особливостей трудової діяльності, зокрема характеру виконуваних завдань, частоти повторюваних операцій та необхідності переміщень, що забезпечує безпеку та ефективність роботи;

– забезпечення правильної робочої пози, яка дозволяє уникнути м'язового напруження та знижує ризик виникнення м'язово-скелетних розладів, що важливо для збереження здоров'я працівників у довгостроковій перспективі.

Ергономічні вимоги до режимів праці та відпочинку мають важливе значення для забезпечення ефективної та безпечної роботи працівників. Вони спрямовані на оптимізацію робочих процесів з метою підвищення продуктивності та зменшення втоми і напруги. Зв'язок між продуктивністю праці та ергономікою є прямим: впровадження ергономічних принципів у робочі режими сприяє підвищенню продуктивності завдяки кращому фізичному та психологічному самопочуттю працівників [15].

Основними аспектами ергономічних вимог до режимів праці та відпочинку є наступні:

– Зменшення втоми та напруги працівників: Виконання роботи в умовах, які мінімізують фізичну та розумову втому, є ключовим для підтримання високого рівня продуктивності. Це досягається за рахунок правильного проектування робочого місця, забезпечення комфортної робочої пози та раціонального розподілу робочого навантаження.

– Розроблення режимів праці відповідно до ергономічних принципів: Режими праці повинні бути розроблені з урахуванням біологічних ритмів людини, що дозволяє оптимізувати час активної роботи та періоди відпочинку.

– Тривалість безперервної праці та відпочинку: Оптимальна тривалість безперервної праці та регулярні перерви є важливими для запобігання накопиченню втоми. Тривалість безперервної праці не повинна перевищувати 4-6 годин. В іншому випадку, працездатність через втому м’язів та зору знижується.

– Сприятливі умови для відпочинку: Робоче середовище має включати зони для відпочинку, де працівники можуть ефективно відновити свої сили.

4.2 Проведення інструктажів з охорони праці

Проведення інструктажів з охорони праці є важливим елементом забезпечення безпеки на робочих місцях. Інструктажі з охорони праці спрямовані на ознайомлення працівників з потенційними небезпеками, методами їх запобігання, а також правилами поведінки в надзвичайних ситуаціях. Регулярне проведення таких заходів сприяє зниженню рівня виробничого травматизму та забезпечує відповідність діяльності підприємства чинному законодавству у сфері охорони праці.

Працівники, включаючи керівний персонал, які не пройшли інструктаж та перевірку знань з охорони праці, не можуть бути допущені до виконання роботи. На підприємстві перевірка знань працівників щодо охорони праці здійснюється спеціальною комісією, склад якої затверджується керівником за допомогою відповідного наказу. Роботодавець несе відповідальність за організацію та проведення інструктажів.

За характером і часом проведення інструктажі з охорони праці поділяються на вступні, первинні, повторні, позапланові та цільові, причому кожен з них проводиться для конкретних категорій працівників і за певних обставин [15].

Вступний інструктаж з охорони праці проводиться спеціалістом або іншим кваліфікованим фахівцем. Працівники проходять цей інструктаж у кабінеті охорони праці або в спеціально обладнаному для цього місці, згідно з програмою та тривалістю, затвердженими роботодавцем. Інструктаж проводиться в перший робочий день працівника або напередодні, якщо існує наказ про його прийняття на роботу [16]. Інформація про проведення вступного інструктажу з питань охорони праці реєструється у відповідному журналі реєстрації. Цей вид інструктажу з охорони праці на підприємстві проводиться:

– працівникам, які приймаються на постійну або тимчасову роботу, незалежно від їх освіти, стажу роботи чи посади;

– працівникам інших організацій, які прибули на підприємство для участі у виробничому процесі або виконання інших робіт для підприємства;

– учням і студентам, які проходитимуть на підприємстві трудове або професійне навчання;

– учасникам екскурсії на підприємство.

Первинний інструктаж проводиться керівником робіт (начальником цеху, майстром) або фізичною особою. Первинний інструктаж проводять з:

– новоприйнятими на постійну або тимчасову роботу працівниками;

– відрядженими працівниками з інших підприємств;

– працівниками, яких перевели з іншого структурного підрозділу підприємства;

– працівниками, які будуть виконувати нову роботу.

Для учнів, студентів, курсантів та слухачів, які проходитимуть трудове або професійне навчання і будуть використовувати різноманітні інструменти, механізми, матеріали також необхідно проводити первинний інструктаж з охорони праці індивідуально або для групи осіб одночасно [16].

Повторний інструктаж є важливим, оскільки дозволяє працівнику відновити знання, отримані під час первинного інструктажу, повторити основні аспекти та уникнути помилок у подальшій роботі. Тому спеціалісти повинні відповідально підходити до розроблення документів з охорони праці, включаючи програми інструктажів, щоб кожен працівник отримав необхідну інформацію та міг своєчасно скористатися набутими знаннями. Терміни проведення повторного інструктажу працівникам:

– які виконують роботи з підвищеною небезпекою –раз на три місяці;

– які виконують інші роботи – раз на пів року.

Позаплановий інструктаж з охорони праці проводять у разі:

– введення в дію нових або зміни наявних нормативних документів з охорони праці;

– модифікації технічного обладнання, технологічного процесу або матеріалів, які змінюють алгоритми виробництва;

– випадків недотримання вимог нормативних документів з охорони праці, що спричинили травми, аварії, пожежі тощо;

– у разі перерви в роботі виконавця робіт з підвищеною небезпекою, яка триває понад 30 календарних днів;

– у разі перерви в роботі виконавця інших робіт, яка триває понад 60 календарних днів.

Цільові інструктажі з охорони праці проводяться у випадку необхідності ліквідації аварії або оформлення наряду-допуску, наказу чи розпорядження та не завжди включаються до журналу реєстрації, якщо вони вже узгоджені в наряді-допуску.

Відповідно до вимог, керівник підприємства, відповідальний спеціаліст або безпосередній керівник відділу, ділянки або цеху повинні своєчасно інформувати співробітників про заходи з безпеки. Розробка інструкцій покладається на роботодавця з урахуванням думки професійних фахівців. Обов'язки інструктора включають навчання персоналу, перевірку засвоєних знань та ведення відповідної документації [16].

ВИСНОВКИ

У кваліфікаційній роботі було проведено дослідження та впровадження заходів безпеки для забезпечення захисту в платформі віртуалізації Proxmox VE.

Проведено дослідження загальних принципів віртуалізації, переваги та недоліки впровадження технологій віртуалізації. Також було проведено аналіз платформи віртуалізації Proxmox VE та доступних заходів захисту, які надає платформа, в результаті якого визначено ефективні заходи, такі як двофакторна аутентифікація, контроль доступу користувачів та брандмауер.

Було проведено практичне впровадження ключових заходів захисту в Proxmox VE, а саме, налаштовано двофакторну аутентифікацію для доступу до веб-інтерфейсу Proxmox VE, що забезпечує додатковий рівень безпеки та знижує ризик несанкціонованого доступу. Налаштовано контроль доступу користувачів шляхом створення нових користувачів та призначення їм відповідних ролей і привілеїв, що дозволяє краще розмежувати обов'язки та доступи між різними користувачами системи. Також налаштовано брандмауер, а саме створено списки IPSet, групи безпеки та правила брандмауера для дозволу чи заборони трафіку з відповідних IP-адрес, що забезпечує ефективне фільтрування мережевого трафіку та захист від можливих зовнішніх атак.

Таким чином, в ході роботи було досягнуто основну мету – проаналізовано та впроваджено комплекс заходів захисту в Proxmox VE, що забезпечило високий рівень безпеки та зменшило ризики несанкціонованого доступу та атак на віртуалізовану інфраструктуру. Результати аналізу підтверджують доцільність та ефективність впроваджених заходів, що є важливим кроком до забезпечення захисту віртуалізованих середовищ.

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. Детально про віртуалізацію: типи, переваги та рішення | Хмара TechExpert. Хмара TechExpert. URL: https://onbiz.biz/about-virtualization/.

3. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146. https://doi.org/10.62731/mcnd-24.05.2024.001

4. Що таке віртуалізація та які переваги вона надає. GigaCloud: Хмарні Технології та Хмарний Сервіс для Бізнесу. URL: https://gigacloud.ua/blog/navchannja/scho-take-virtualizacija-ta-jaki-perevagi-vona-nadae.

5. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170. https://doi.org/10.36074/logos-21.06.2024.034

6. Revniuk O.A., Zagorodna N.V., Kozak R.O., Karpinski M.P., Flud L.O. “The improvement of web-application SDL process to prevent Insecure Design vulnerabilities”. Applied Aspects of Information Technology. 2024; Vol. 7, No. 2: 162–174. DOI:https://doi.org/10.15276/aait.07.2024.12.

7. Proxmox VE | OSISM – Sovereign Cloud Infrastructure. OSISM – Sovereign Cloud Infrastructure. URL: https://osism.tech/docs/guides/concept-guide/components/proxmox/.

8. Stadnyk, M., Fryz, M., Zagorodna, N., Muzh, V., Kochan, R., Nikodem, J., & Hamera, L. (2022). Steady state visual evoked potential classification by modified KNN method. Procedia Computer Science, 207, 71-79.

9. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). СИСТЕМА ЗМЕНШЕННЯ ВПЛИВУ DOS-АТАК НА ОСНОВІ MIKROTIK. Матеріали конференцій МЦНД, (17.05. 2024; Ужгород, Україна), 198-200. https://doi.org/10.62731/mcnd-17.05.2024.008

10. Proxmox VE Administration Guide. Proxmox VE. URL: https://pve.proxmox.com/pve-docs/pve-admin-guide.html.

11. Tymoshchuk, V., Dolinskyi, A., & Tymoshchuk, D. (2024). MESSENGER BOTS IN SMART HOMES: COGNITIVE AGENTS AT THE FOREFRONT OF THE INTEGRATION OF CYBER-PHYSICAL SYSTEMS AND THE INTERNET OF THINGS. Матеріали конференцій МЦНД, (07.06. 2024; Луцьк, Україна), 266-267. https://doi.org/10.62731/mcnd-07.06.2024.004

12. Nataliya Zagorodna, Iryna Kramar (2020). Economics, Business and Security: Review of Relations. Business Risk in Changing Dynamics of Global Village BRCDGV-2020: Monograph / Edited by Pradeep Kumar, Mahammad Sharif. India, Patna: Novelty & Co., Ashok Rajpath,. 446 p., pp.25-39.

13. Lechachenko, T., Kozak, R., Skorenkyy, Y., Kramar, O., & Karelina, O. (2023). Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model. In ITTAP (pp. 416-424).

14. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ВИКОРИСТАННЯ ТЕХНІКИ ДИНАМІЧНОГО ВІДКРИВАННЯ МЕРЕЖЕВИХ ПОРТІВ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ СЕРВЕРІВ. Collection of scientific papers «ΛΌГОΣ», (May 24, 2024; Zurich, Switzerland), 233-234. https://doi.org/10.36074/logos-24.05.2024.051

15. Види інструктажів з охорони праці – Охорона праці і пожежна безпека. Охорона праці і пожежна безпека. URL: https://oppb.com.ua/articles/vydy-instruktazhiv-z-ohorony-pratsi.

16. Profiteh. Інструктажі з охорони праці в Україні – види й порядок проведення | Профітех. ПРОФІТЕХ. URL: https://profiteh.ua/instruktazhi-z-okhorony-pratsi-v-ukraini/.