Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Оцінювання ризиків інформаційної безпеки віртуальної інфраструктури
(тема)

Виконав:
студент 2 курсу, групи АМСЗІм-21-2
Шульга М.Д.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського
Добринін І.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2023р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації

(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2023р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Шульзі Микиті Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Оцінювання ризиків інформаційної безпеки віртуальної інфраструктури
затверджена наказом по університету від «23» березня 2023р. №292 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 15.05.2023р.
3. Вихідні дані до роботи: віртуальна інфраструктура, модель об’єктів захисту віртуальної інфраструктури, дані про методи оцінювання ризиків інформаційної безпеки, статистика вразливостей та загроз віртуального середовища.
4. Перелік питань, що потрібно опрацювати в роботі:
1) Ідентифікація інформаційних ризиків при роботі з віртуальною інфраструктуро
2) Аналіз активів віртуального середовища
3) Оцінювання ризиків інформаційної безпеки віртуальної інфраструктури

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Добринін Ігор Станіславович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	15.02.2023	Виконано
2	Збір матеріалів для дослідження	28.02.2023	Виконано
3	Розробка 1 розділу	19.03.2023	Виконано
4	Розробка 2 розділу	06.04.2023	Виконано
5	Розробка 3 розділу	01.05.2023	Виконано
6	Оформлення кваліфікаційної роботи	05.05.2023	Виконано

Дата видачі завдання 15 лютого 2023 року

Студент _____ Шульга М.Д.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Добринін І.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 86 с., 11 рис., 14 табл., 1 додаток, 20 джерел.

ВІРТУАЛІЗАЦІЯ, ВІРТУАЛЬНА МАШИНА, ГІПЕРВІЗОР, ІНФОРМАЦІЙНІ РИЗИКИ, ОПЕРАЦІЙНА СИСТЕМА, СЕРВЕР, ВІРТУАЛЬНЕ СХОВИЩЕ.

Об'єкт дослідження – процес виявлення й оцінювання інформаційних ризиків при роботі з віртуальною інфраструктурою.

Предмет дослідження – методи оцінювання інформаційних ризиків віртуальної інфраструктури.

Мета роботи – оцінювання ризиків інформаційної безпеки віртуальної інфраструктури

Методи досліджень – аналіз теоретичних джерел, емпіричний аналіз, формалізація, моделювання загроз, аналіз загроз, аналіз методів оцінювання ризиків, оцінювання ризиків.

Багато компаній в даний час застосовують віртуальну інфраструктуру як необхідне програмне забезпечення для перевірки рішень, тому забезпечення безпеки віртуальної інфраструктури стає незамінною складовою інформаційної безпеки підприємства.

В даній роботі проаналізовані важливі активи віртуального середовища, наявні методи оцінювання ризиків, застосована діаграма Fishbone для визначення характеристики безпеки віртуальної інфраструктури за допомогою структурованого підходу. Запропоновано контрзаходи для забезпечення інформаційної безпеки, які могли б запобігти подальшим порушення конфіденційності, цілісності та доступності. Проведено оцінювання ризиків відповідно до розробленої моделі об’єктів захисту віртуального середовища.

ABSTRACT

The report contains: 86 p., 11 fig., 14 tables, 1 application, 20 sources.

VIRTUALIZATION, VIRTUAL MACHINE, HYPERVISOR, INFORMATION RISKS, OPERATING SYSTEM, SERVER, VIRTUAL STORAGE.

The object of research is the process of identifying and assessing information risks when working with virtual infrastructure.

The subject of the study is methods of assessing information risks of virtual infrastructure.

The purpose of the work is to assess the information security risks of the virtual infrastructure

Research methods – analysis of theoretical sources, empirical analysis, formalization, threat modeling, threat analysis, analysis of risk assessment methods, risk assessment.

Many companies currently use virtual infrastructure as a necessary software for verifying solutions, therefore ensuring the security of virtual infrastructure becomes an indispensable component of the information security of the enterprise.

This paper analyzes the important assets of the virtual environment, the existing risk assessment methods, and applies the Fishbone diagram to determine the security characteristics of the virtual infrastructure using a structured approach. Countermeasures are proposed to ensure information security that could prevent further breaches of confidentiality, integrity, and availability. A risk assessment was carried out in accordance with the developed model of virtual environment protection objects.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ВМ – віртуальна машина
ІС – інформаційні системи
ОС – операційна система
ЦП – центральний процесор
CRAMM – CCTA Risk Analysis and Management Method
CSRF – Cross-Site Request Forgery
CVE – Common Vulnerabilities and Exposures
FAIR – Factor Analysis of Information Risk
ISAMM – Information Security Assessment and Monitoring Method
IPS – Intrusion Prevention System
NAS – Network Attached Storage
OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation
PRNG – Pseudorandom Number Generator
RBAC – Role Based Access Control
SAN – Storage Area Network
SCSI – Small Computer System Interface
UEFI – Unified Extensible Firmware Interface
VMM – Virtual Machine Manager

ВСТУП

Метою управління ризиками IT-проектів є оперативне виявлення факторів, пов’язаних з виконанням інформаційної системи або системи автоматизації, які можуть негативно вплинути на реалізацію проекту, та оптимальне планування дій для мінімізації цих факторів.

Сьогодні багато організацій покладаються на віртуальне середовище як на критичне програмне забезпечення для тестування рішень. Забезпечення захисту даних віртуального середовища є важливим компонентом корпоративної інформаційної безпеки протягом багатьох років розгортання віртуальної інфраструктури. Робота з віртуальними машинами пов'язана з різними ризиками [1].

Оскільки віртуалізовані середовища формують основу для розподілених інфраструктур, таких як хмара, вони широко застосовуються та стають об’єктами кібератак. Розробляються більш складні та спеціалізовані атаки для використання вразливостей або слабких місць на рівні віртуалізації.

Основна увага при гарантуванні інформаційної безпеки віртуального середовища полягає в мінімізації шкоди в результаті загроз безпеці, спрямованих на цілісність і доступність програмного комплексу в інформаційній системі. Таким чином, проведення оцінювання ризиків інформаційної безпеки, що стосуються віртуального середовища, відіграє вирішальну роль у розробці планів захисту даних.

Метою роботи є оцінювання ризиків інформаційної безпеки віртуальної інфраструктури.

Для вирішення поставленої задачі, в першому розділі кваліфікаційної роботи проведено аналіз підходів до віртуалізації, проаналізовано можливі вразливості та загрози безпеки віртуалізації. У другому розділі проведено класифікацію важливих активів та аспектів віртуального середовища, методів оцінювання ризиків інформаційної безпеки, у третьому розділі проведено оцінювання ризиків інформаційної безпеки віртуальної інфраструктури за допомогою матричного методу.

Оцінювання інформаційних ризиків під час роботи з віртуальним середовищем має вирішальне значення для підтримки безпеки та цілісності даних та IT-ресурсів [2].

1 ІДЕНТИФІКАЦІЯ ІНФОРМАЦІЙНИХ РИЗИКІВ ПРИ РОБОТІ З ВІРТУАЛЬНОЮ ІНФРАСТРУКТУРОЮ

1. Аналіз підходів до віртуалізації

Технології віртуалізації можна спочатку класифікувати на основі їхнього рівня емуляції апаратного забезпечення, розрізняючи повну емуляцію апаратного забезпечення та віртуалізацію апаратного забезпечення (також відому як віртуалізація операційних систем (ОС) або часткова емуляція апаратного забезпечення). Повна апаратна емуляція дозволяє виконувати немодифіковану систему (гостьову ОС) на іншій архітектурі хосту, емулюючи всі функції програмної системи або пристрою на апаратній платформі з іншим набором інструкцій.

Апаратна віртуалізація передбачає виконання програмної системи або пристрою на апаратній платформі з тим самим набором інструкцій. Різниця між апаратною віртуалізацією та емуляцією не завжди чітка, оскільки апаратні емулятори іноді можна використовувати для віртуалізації пристрою [3].

Повна віртуалізація імітує базове апаратне забезпечення в програмному забезпеченні для кожної віртуальної машини, повністю відокремлюючи гостьову ОС від основного апаратного забезпечення. Цей підхід забезпечує найвищу ізоляцію та безпеку, але знижує продуктивність і додає додаткові витрати. Приклади включають VirtualBox, Virtual PC, VMware, Win4Lin, User Mode Linux.

Паравіртуалізація – це легка техніка, за якої гіпервізор відкриває hypercalls, які можуть бути викликані безпосередньо модифікованою гостьовою ОС для імітації привілейованих інструкцій, які важко віртуалізувати. Цей метод забезпечує кращу продуктивність і менші накладні витрати, ніж повна віртуалізація, але вимагає змін гостьової операційної системи. Приклади включають Xen і KVM/QEMU.

Віртуалізація з підтримкою апаратного забезпечення залежить від постачальників апаратного забезпечення, які надають нові функції для підтримки методів віртуалізації, таких як Intel Virtualization Technology і AMD AMD-V. Цей метод пропонує кращу продуктивність і зменшує зміни, необхідні для паравіртуалізації. Приклади включають VMware Workstation, VirtualBox, Xen, KVM/QEMU, Parallels і Microsoft Hyper-V [4]. Окрім рівня апаратної емуляції, технології віртуалізації можна класифікувати за рівнем віртуалізації.

Віртуалізація на рівні операційної системи використовує операційну систему, яка підтримує кілька екземплярів ізольованого простору користувача, які називаються контейнерами. Цей підхід забезпечує високу продуктивність, низькі накладні витрати та дозволяє виконувати ту саму ОС, що й головна машина. Приклади включають контейнери Docker, Virtuozzo, OpenVZ і Solaris. Віртуалізація на рівні програми покращує перенесення програм між різними програмно-апаратними архітектурами. Приклади рішень, що підтримують віртуалізацію на рівні програми, включають Java VM, Microsoft .NET, Perl, Python і Ruby.

Технології віртуалізації також можна класифікувати на основі типу хостингу, який надає гіпервізор, із двома можливими типами хостингу: власний (віртуалізація на голому металі або гіпервізор типу I) і нерідний (віртуалізація на хості або гіпервізор типу II).

Віртуалізація «голого металу» включає в себе рівень віртуалізації, встановлений безпосередньо на апаратному забезпеченні хоста, який виконує запити від віртуальних машин. Гіпервізор працює безпосередньо на апаратному забезпеченні хоста та спілкується з фізичними пристроями. У цьому випадку головна операційна система та гіпервізор об’єднані в один рівень у гіпервізори. Навпаки, розміщена віртуалізація має багатошарову структуру, що включає апаратне забезпечення хосту, операційну систему хост-машини, гіпервізор та гостьову операційну систему, встановлену на віртуальній машині. Гіпервізор встановлюється поверх головної операційної системи та співіснує з програмами, вже встановленими в головній операційній системі [5].

Технології віртуалізації повинні адаптуватися до навколишнього апаратного та програмного середовища, взаємодіючі з ними, щоб створити безпечну, надійну та ефективну віртуалізовану систему. Безпека віртуалізованої системи залежить від безпеки гостьових операційних систем, включаючи захист від атак, спрямованих на загальні ОС, встановлені на певному фізичному обладнанні.

Розглянемо поширений сценарій застосування віртуалізації, де вона відіграє значну роль, приносячи як переваги, так і обмеження – це повна віртуалізація. Гіпервізор забезпечує повне середовище віртуалізації, укомплектоване власним віртуалізованим процесором, пам’яттю, накопичувачем і пристроями введення/виведення. Це дозволяє віртуальним машинам працювати так, ніби вони знаходяться на власному виділеному фізичному обладнанні, можливість швидко відновити сервер після збою апаратного забезпечення та можливість комбінувати різні апаратні платформи та операційні системи, усуваючи залежності між

апаратними та програмними компонентами. Однак це може негативно вплинути на безпеку даних, автентифікацію сервера та ефективність. Можна виділити такі основні переваги повної віртуалізації.

1) Сумісність. Віртуальні машини сумісні зі стандартними комп'ютерами. Подібно до фізичних комп'ютерів, віртуальні машини мають власну гостьову операційну систему та можуть запускати програми. Вони включають усі стандартні компоненти фізичного комп'ютера, такі як материнська плата, графічна карта та мережевий контролер. Ця сумісність дозволяє віртуальним машинам бездоганно працювати зі стандартними операційними системами на базі x86, програмами та драйверами пристроїв. По суті, будь-яке програмне забезпечення, придатне для фізичного комп'ютера, можна запускати на віртуальній машині.

2) Ізоляція. Віртуальні машини повністю ізольовані одна від одної, подібно до фізичних комп'ютерів. Хоча кілька віртуальних машин можуть спільно використовувати фізичні ресурси одного комп'ютера, вони залишаються ізольованими одна від одної як окремі сутності. Це означає, що якщо одна віртуальна машина виходить з ладу, це не впливає на доступність інших віртуальних машин, що працюють на тому самому фізичному сервері. Ця ізоляція забезпечує вищу доступність і безпеку для програм, що працюють у віртуальному середовищі, порівняно зі стандартною невіртуалізованою системою.

3) Інкапсуляція. Віртуальні машини інкапсулюють все обчислювальне середовище в програмний контейнер. Віртуальна машина містить повний набір віртуальних апаратних ресурсів, а також операційну систему та всі її програми. Ця інкапсуляція робить віртуальні машини дуже портативними та простими в управлінні. Їх можна переміщувати або копіювати з одного місця в інше, як і будь-який інший програмний файл. Крім того, віртуальні машини можна зберігати на різних носіях інформації.

4) Незалежність від обладнання. Віртуальні машини працюють незалежно від основного обладнання. Вони не прив'язані до конкретного фізичного обладнання, на якому працюють. Наприклад, віртуальна машина може мати віртуальні компоненти (такі як центральний процесор, мережева карта та контролер Small Computer System Interface (SCSI)) із налаштуваннями, які відрізняються від фізичних характеристик основного обладнання. Віртуальні машини навіть мають гнучкість для запуску різних операційних систем (наприклад, Windows, Linux) на одному фізичному

сервері. У поєднанні з інкапсуляцією та сумісністю незалежність від апаратного забезпечення дозволяє вільно переміщати віртуальні машини між комп'ютерами без необхідності змінювати драйвери пристроїв, операційні системи чи програми. Це також дозволяє запускати абсолютно різні операційні системи та програми на одному фізичному комп'ютері.

Віртуальні машини можна легко копіювати між комп'ютерами, передавати через мережі, миттєво створювати резервні копії та відновлювати в режимі реального часу. Образ віртуальної машини представлений у вигляді файлу, і операційна система може бути швидко завантажена за допомогою віртуальної машини.

Віртуальні машини пропонують можливість виділяти більше фізичної пам'яті, ніж те, що фактично підтримує базове обладнання, і можуть імітувати функціональність 64-розрядного процесора на 32-розрядній архітектурі. Деякі серверні операційні системи працюють у стеку віртуальних машин, що полегшує зручне оновлення обладнання, зниження версії або перенесення на зовсім інші комп'ютерні конфігурації.

Запуск кількох серверних операційних систем у віртуальному середовищі на одному сервері дозволяє ефективно використовувати незадіяні ресурси, що призводить до зниження витрат для кінцевих користувачів. Ця технологія часто використовується для впровадження віртуальних виділених серверів, забезпечуючи комплексне керування сервером, включаючи доступ до Unified Extensible Firmware Interface (UEFI), консольний завантажувач, адміністрування та віддалене керування без необхідності додаткових інвестицій [6].

Крім того, з точки зору безпеки, важливо налаштувати два фізичні сервери, на кожному з яких працюють віртуальні сервери, одночасно створюючи резервні копії образів віртуальних серверів на сервері, розташованому віддалено. У разі збою одного сервера резервна копія віртуального сервера, що працює на ньому, може бути швидко запущена у віртуальному середовищі робочого сервера.

Віртуальні машини служать невід'ємними компонентами віртуальної інфраструктури, яка охоплює об'єднані апаратні ресурси цілої інформаційної інфраструктури, включаючи комп'ютери, мережеві пристрої та спільне сховище.

2. Слабкі місця безпеки віртуального середовища

Віртуалізація має кілька спільних проблем безпеки з традиційними обчислювальними середовищами, наприклад тих, що впливають на операційні системи, протоколи зв'язку та програми. У деяких випадках ці проблеми

посилюються наявністю віртуалізованих компонентів, які вимагають додаткової уваги. Наприклад, традиційні проблеми безпеки операційної системи, такі як підвищення привілеїв, можуть мати більш значний вплив, якщо метою є ОС фізичної машини, на якій розміщено віртуалізовану систему та її користувачів. Віртуалізація також представляє унікальні проблеми безпеки, які вимагають спеціальних рішень, таких як:

- multi-tenancy (режим колективної оренди), що дозволяє міжплатформний потік інформації між клієнтами, які використовують один фізичний хост;
- зловмисники, які виконують довільний код поза гостьовою системою без належних прав доступу;
- спеціальні вимоги безпеки для віртуалізованого сховища для забезпечення безпеки даних під час хмарних подій, таких як міграція.

У віртуальних налаштуваннях, де кілька користувачів спільно використовують фізичні ресурси, певні дії можуть призвести до розкриття конфіденційних даних. Наприклад, вплив через залишкові дані у віртуальних середовищах може бути більш критичним, ніж у фізичних. Крім того, загрози перехоплення можуть бути більш значущими у віртуальних середовищах, оскільки вони дозволяють перехресну перевірку даних кількох користувачів і можуть використовуватися для планування атак на відмову в обслуговуванні. Протидія загрозам вторгнення може бути складною у віртуалізованих налаштуваннях, оскільки зловмисники можуть отримати привілеї з різних ресурсів, включно з тими, що знаходяться за межами видимості віртуального середовища. Конфіденційні дані також можуть бути отримані шляхом використання привілейованих процесів під час інтроспекції віртуалізації, проблема, яка посилюється сценаріями додатків віртуалізації, які підтримують міграцію та об’єднання віртуальних машин.

Обман передбачає навмисне введення в оману інших сторін, коли неавторизовані організації отримують доступ або завдають шкоди, видаючи себе за авторизованих. Цього можна досягти шляхом шахрайства з особистими даними, фальсифікації даних, відмови від відповідальності за дії або маніпулювання користувачами, щоб вони завдали шкоди системі. Обман поширений як у фізичному, так і у віртуальному середовищах; однак керування ідентифікацією може бути більш складним у віртуальних налаштуваннях через складне адміністрування привілеїв.

Збій призводить до погіршення роботи системи, що негативно впливає на послуги, які вони пропонують. Загрози збою можуть вивести з ладу компоненти, пошкодити функції системи або перешкодити наданню послуг. Віртуальні середовища можуть успадковувати збої від фізичних систем, наприклад неконтрольований розподіл ресурсів, тоді як спільні ресурси можуть підвищити ризик перешкод. Перевантаження ресурсів у фізичних системах може спричинити погіршення продуктивності віртуальної мережі та порушення зв'язку як ненавмисно, так і в рамках скоординованих атак.

Неавторизований контроль систем або ресурсів – ця загроза полягає в тому, що неавторизований суб'єкт захоплює контроль над системою або ресурсом, використовуючи вразливі місця, виконуючи неавторизовані дії або отримуючи неавторизовані привілеї. Це може призвести до злому системи, витоку даних або несанкціонованого використання ресурсів.

У віртуальних середовищах неавторизований контроль може бути складніше виявити та пом'якшити через динамічний характер ресурсів і складність керування привілеями. Зловмисники можуть використовувати вразливості на рівнях віртуалізації, використовувати спільні ресурси або використовувати вразливості в процесі міграції, щоб отримати контроль над ресурсами. Крім того, зловмисники можуть використовувати неправильні конфігурації або слабкі місця у віртуалізованих середовищах, щоб збільшити привілеї та отримати несанкціонований доступ до конфіденційних даних або систем. Проаналізувавши вразливості та загрози віртуалізації можна побудувати перелік слабких місць віртуального середовища.

1) Недостатня перевірка контрольованого користувачем введення даних може призвести до ненавмисного виконання команд або неавторизованого доступу до даних. Ці проблеми зберігаються у віртуалізованих середовищах, зокрема в компонентах віртуалізації, які взаємодіють із певними елементами, такими як гіпервізор і Virtual Machine Manager (VMM). На жаль, ці проблеми часто ігноруються, оскільки залучені користувачі часто мають права адміністратора.

2) Помилка автентифікації: це відноситься до вразливостей, що виникають через погано розроблені або реалізовані механізми автентифікації, що впливає на специфікацію та застосування політик контролю доступу. Він охоплює питання, пов'язані з автентифікацією, авторизацією, керуванням користувачами та зв'язком із кінцевою точкою. У віртуалізованих середовищах автентифікація застосовується як до кінцевих

користувачів, так і до компонентів системи. Приклади таких недоліків включають використання невідповідних облікових даних або методів перевірки, наприклад використання автентифікації на основі пароля замість сертифікатів, або використання слабких механізмів реєстрації та помилок у процесах автентифікації.

3) Керування обліковими даними: слабкі сторони в цій області включають керування паролями, надійність пароля або слабкі методи шифрування, застарілі паролі та недостатні механізми відновлення паролів для забутих паролів. У віртуалізованих середовищах ці недоліки посилюються через спільне використання незахищених транспортних каналів, що збільшує кількість потенційних користувачів, які можуть отримати доступ до облікових даних.

4) Керування дозволами та привілеями: це стосується проблем, пов'язаних із відсутністю необхідних привілеїв або неправильним призначенням привілеїв, а також помилками під час видалення, пониженням або збережених успадкованих дозволів. У віртуалізованих середовищах ця слабкість посилюється складним характером привілеїв і кількома адміністративними рівнями, особливо враховуючи динамічний характер віртуалізованих середовищ і сценарії, що включають міграцію та злиття.

5) Криптографія охоплює публічне зберігання або передачу конфіденційної інформації, помилки в управлінні ключами, як-от обмін ключами без належної автентифікації, відсутність або слабку перевірку ключа. Це також відноситься до вразливостей у криптографічних протоколах і відсутності або слабкості шифрування для захисту конфіденційних даних під час зберігання або передачі. Віртуалізовані середовища загострюють проблеми з криптографією через спільні канали або ресурси, причому атаки типу «людина посередині» стають особливо критичними, коли повідомлення від різних користувачів спільно використовують той самий канал або інфраструктуру.

6) Недоліки в обробці даних: ця категорія охоплює слабкі місця у функціях обробки даних. Ця широка категорія включає помилки рядків і типів, загальні помилки представлення, наприклад, неправильна обробка синтаксично недійсної структури, і числові помилки (наприклад, помилка обертання або неправильне перетворення між числовими типами) [7]. У віртуалізованих середовищах це також включає проблеми збереження

даних, властиві віртуалізації та ще більше посилені спільним сховищем або ресурсами пам’яті.

7) Помилки в управлінні інформацією: це стосується недоліків, пов’язаних із неправильним поводженням з конфіденційною інформацією, наприклад, розголошення інформації або ненавмисне надання інформації неавторизованим особам. У віртуалізованих середовищах це має більше значення, ніж фізичні середовища. Наприклад, атаки по побічних каналах були продемонстровані у віртуалізованих середовищах, де зловмисник може отримати конфіденційну інформацію, спостерігаючи за поведінкою віртуальної машини, розташованої на тій же фізичній машині. Крім того, механізми розповсюдження та реплікації, властиві віртуалізованим середовищам, полегшують атаки видобутку даних. Приховані канали, що використовують фізичну архітектуру центрального процесора (ЦП), стають більш критичними через спільне використання ЦП і пам’яті, що дозволяє отримувати інформацію про процеси або мережевий трафік, що належать іншим користувачам [8].

8) Неправильна перевірка даних: система не перевіряє або неправильно перевіряє введені користувачем дані. Наприклад, неправильне розв’язання посилання перед доступом до файлу. Також відноситься до вразливостей буфера пам’яті, наприклад, переповнення буфера та проблеми з читанням або записом поза межами. У віртуалізованих середовищах багаторівнева взаємодія між компонентами програмного забезпечення посилює вплив цієї слабкості, а перевірка стає складною через складність взаємодії на рівні компонентів.

9) Недостатня перевірка автентичності даних: це стосується неправильної перевірки введених даних, тобто система не перевіряє або неправильно перевіряє введені дані. Він охоплює слабкі сторони, такі як неправильний вибір механізмів автентифікації даних, неправильна перевірка криптографічних підписів, відсутність перевірки цілісності та вразливості, такі як підробка міжсайтових запитів. Cross-Site Request Forgery (CSRF) використовує слабкість, коли програма не може належним чином перевірити, що надісланий користувачем запит є дійсним і послідовним. У віртуалізованих середовищах ця слабкість посилюється, оскільки багато компонентів піддають інтерфейси таким атакам, як CSRF, користуючись цією вразливістю [9]. Зокрема, віртуалізація підтримує такі технології, як Intel-VT, захищені криптопроцесори та Trust Computing, які

надають фундаментальні функції віртуалізації, але також відкривають ряд недоліків, характерних для технології віртуалізації (наприклад, руткіт у вкладеній віртуалізації або неправильна поведінка під час перевірки автентичності під час завантаження).

10) Неналежна перевірка сертифіката: це стосується нездатності перевірити або неправильно перевірити сертифікати, що потенційно може спровокувати атаки «людина посередині». Він охоплює вразливості, пов'язані з невідповідною перевіркою хоста, закінченням терміну дії сертифіката або повною відсутністю перевірки. Він також містить недоліки в перевірці довіри сертифіката. У віртуалізованих середовищах ця слабкість посилюється тим фактом, що конфіденційність і цілісність (як внутрішнього, так і зовнішнього) зв'язку між компонентами віртуалізації залежать від сертифікатів. Однак захист сертифікатів знаходиться під загрозою через спільну та багатокористувацьку природу інфраструктури віртуалізації.

11) Використання недостатньо випадкових значень: це пов'язано з недостатньою ентропією в Pseudorandom Number Generator (PRNG), проблемами передбачуваності та використанням криптографічно слабких PRNG. Ця слабкість посилюється віртуалізацією апаратних пристроїв. Наприклад, досягти достатньої ентропії ще складніше, оскільки віртуалізоване середовище знижує якість джерела ентропії, де зазвичай використовують псевдовипадкові числа [10].

12) Недоліки в управлінні ресурсами: це стосується вразливостей, пов'язаних із неправильним керуванням системними ресурсами, що призводить до виснаження ресурсів. Це охоплює недоліки, викликані неправильним вимкненням або звільненням ресурсів, що призводять до неочікуваних змін пам'яті, та іншими проблемами керування пам'яттю, наприклад «витоками пам'яті» або проблемами збереження даних. У віртуалізованих середовищах це стає критичним, оскільки багато атак покладаються на виснаження системних ресурсів для досягнення відмови в обслуговуванні або маніпулювання системою в стан, який сприяє іншим атакам. Проблеми споживання ресурсів мають широкий вплив на численні компоненти, від гіпервізорів, які намагаються забезпечити збалансовану обчислювальну потужність, до віртуалізованих мереж, які стикаються з серйозними вузькими місцями через виснаження ресурсів.

13) Міжсайтовий сценарій: в першу чергу це стосується традиційних сценаріїв веб-перегляду. У віртуалізованих середовищах клієнти використовують інформаційні панелі для оцінювання функцій віртуалізації або перевірки ресурсів. Ці інтерактивні веб-панелі вимагають захисту від вразливостей міжсайтових сценаріїв.

14) Послідовності коду, які можуть виконуватися одночасно, вимагаючи тимчасового ексклюзивного доступу до спільних ресурсів. Існують часові вікна, у яких спільні ресурси можна змінювати шляхом одночасного виконання послідовностей коду. У віртуалізованих середовищах наявність численних незалежно керованих асинхронних компонентів вимагає ретельного проектування та впровадження механізмів для керування такими ситуаціями.

15) Вразливості апаратного забезпечення: у віртуалізованих середовищах кілька програмних компонентів співпрацюють, щоб надати кінцевим користувачам можливості віртуалізації. Ця екосистема містить програмне забезпечення від різних постачальників, що використовує різноманітні технології та розроблене та підтримується відповідно до різних методологій. Це підкреслює проблеми, пов’язані із співіснуванням і взаємодією програмних компонентів у системах віртуалізації.

16) Вразливості конфігурації: віртуалізовані системи покладаються на набір програмних компонентів, які працюють разом і вимагають динамічної конфігурації для забезпечення віртуалізації в різних прикладних сценаріях. Слабкі місця на рівні конфігурації стають більш критичними, коли на поведінку віртуалізації впливають залежності між різними компонентами. Крім того, ці компоненти побудовані на основі складних конфігурацій, які можуть розвиватися протягом життєвого циклу віртуалізованого середовища через їхній інтерактивний характер. Як наслідок, вразливості в групі конфігурації мають ще більше значення у віртуалізованих середовищах порівняно з традиційними системами.

Інтегруючи знання про вразливості з вищезазначеними заходами безпеки, організації можуть ще більше посилити захист своїх віртуальних середовищ від різних загроз. Цей комплексний підхід до кібербезпеки допомагає захистити конфіденційні дані, підтримувати доступність системи та пом’якшити потенційні негативні наслідки інцидентів безпеки. Зрештою, надійні методи безпеки дозволяють організаціям використовувати переваги віртуалізації, одночасно ефективно керуючи пов’язаними ризиками.

2 АНАЛІЗ АКТИВІВ ВІРТУАЛЬНОГО СЕРЕДОВИЩА

2.1. Аналіз активів та аспектів віртуального середовища

Активи віртуалізації стосуються компонентів і ресурсів, залучених до створення віртуальних середовищ і керування ними. Нижче наведено аналіз активів віртуалізації:

- віртуальні машини – це емуляція програмного забезпечення для його нормального функціонування у апаратному середовищі. У віртуальній машині підлягає емуляції все, починаючи від ядра операційної системи і драйверів для роботи з апаратним забезпеченням, закінчуючи додатками користувача;
- гіпервізор – це програма, яка створює з одного фізичного комп'ютера кілька копій, клонів апаратних ресурсів, і кожен клон видно з боку користувача як окремий пристрій. На кожну віртуальну машину можна встановити гостьову операційну систему користувача, яка не прив'язана до «заліза» хоста;
- компоненти віртуальної мережі які включають віртуальні комутатори, маршрутизатори та брандмауери, які забезпечують підключення до мережі та зв’язок між віртуальними машинами та зовнішньою мережею;
- віртуальне сховище охоплює рішення для зберігання, спеціально розроблені для віртуальних середовищ, таких як віртуальні диски, Storage Area Network (SAN) і Network Attached Storage (NAS);
- інструменти управління дозволяють надавати, конфігурувати, контролювати та керувати віртуальними середовищами. Вони надають адміністраторам централізовану платформу для контролю та автоматизації завдань віртуалізації, підвищуючи ефективність і знижуючи ризик людської помилки;
- інструменти безпеки та елементи керування: спеціальні рішення безпеки для віртуалізації, такі як системи виявлення вторгнень, системи запобігання вторгненням і віртуалізовані брандмауери, захищають віртуальні активи та підтримують конфіденційність, цілісність і доступність даних і систем.

Аналізуючи активи віртуалізації зі сторін функціональності, виявлення потенційних вразливостей і розуміння взаємодії між ними необхідно також враховувати такі аспекти:

- посилення конфігурації та безпеки: забезпечення належної конфігурації віртуальних активів і застосування найкращих практик безпеки для мінімізації поверхні атаки;
- розподіл ресурсів і продуктивність для підтримки ефективних і стабільних віртуальних середовищ;
- забезпечення безперебійної інтеграції та сумісності між активами віртуалізації для забезпечення безперебійної роботи та мінімізації потенційних конфліктів або проблем;
- відповідність і забезпечення виконання політики: впровадження та моніторинг відповідності політикам організації, галузевим стандартам і нормативним вимогам;
- реагування на інциденти: розробка процесів та інструментів для реагування на інциденти безпеки, розслідування можливих порушень та аналіз доказів у віртуальних середовищах.

Ретельно проаналізувавши активи та вищезазначені аспекти, пропонується побудувати надійну основу для захисту віртуальних середовищ, зменшення ризиків та максимізації переваг віртуалізації, звертаючи увагу на наступні аспекти, такі як:

- стратегії резервного копіювання та відновлення: впровадження надійних стратегій резервного копіювання та відновлення для захисту даних і забезпечення безперервності бізнесу в разі збою обладнання, втрати даних або інших інцидентів. Це включає регулярне тестування процесів резервного копіювання та відновлення для підтвердження їхньої ефективності;
- моніторинг і сповіщення: розгортання інструментів моніторингу для відстеження стану та ефективності віртуальних активів у режимі реального часу, що дозволяє проактивно виявляти та вирішувати потенційні проблеми. Крім того, впровадження механізмів сповіщення для сповіщення адміністраторів про будь-які незвичайні дії або зниження продуктивності може допомогти запобігти порушенням безпеки та підтримувати стабільність системи;

- керування виправленнями: створення узгодженого процесу керування виправленнями, щоб підтримувати віртуальні активи в актуальному стані за допомогою останніх оновлень безпеки, виправлень помилок і покращень;
- контроль доступу та керування ідентифікацією: впровадження надійних механізмів контролю доступу, таких як контроль доступу на основі ролей Role Based Access Control (RBAC), щоб гарантувати, що користувачі та адміністратори мають відповідні дозволи на доступ до віртуальних активів і керування ними. Інтеграція рішень для керування ідентифікацією може допомогти оптимізувати автентифікацію та авторизацію користувачів, ще більше посилюючи безпеку [11];
- навчання та підвищення обізнаності: навчання співробітників і IT-персоналу унікальним проблемам безпеки, пов'язаним із віртуальними середовищами, включаючи найкращі методи захисту віртуальних активів, розпізнавання потенційних загроз і реагування на інциденти;
- співпраця та обмін інформацією: участь у галузевих групах, форумах або професійних мережах, зосереджених на безпеці віртуалізації, для обміну досвідом, отриманими знаннями та найкращими практиками. Співпраця та обмін інформацією можуть допомогти організаціям бути в курсі нових загроз та ефективних заходів протидії, тим самим покращуючи загальну безпеку.

2.2. Аналіз методів і засобів оцінювання ризиків в контексті забезпечення інформаційної безпеки віртуального середовища

Оцінювання ризику включає ймовірність і потенційний збиток від виявлених загроз, заходи індивідуального рівня ризику кожного інформаційного активу і як вони ставляться до конфіденційності, цілісності та доступності. Потім вимірюється ефективність наявних заходів. Результати допомагають організації визначити, які активи є найбільш критичними, служать основою для визначення пріоритетів і рекомендують курс дій для захисту активів. Існує безліч способів оцінювання інформаційного ризику.

Оцінювання ризику – це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику. Він включає у себе:

- оцінювання ймовірності загроз й вразливостей, які можливі;
- розрахунок впливу, який може мати загроза на кожен актив;
- визначення кількісної або якісної вартості ризику [12].

Треба взяти до уваги те, що ці три змінні майже завжди залежать одна від одної.

На рис. 2.1 представлені методи оцінювання інформаційних ризиків.

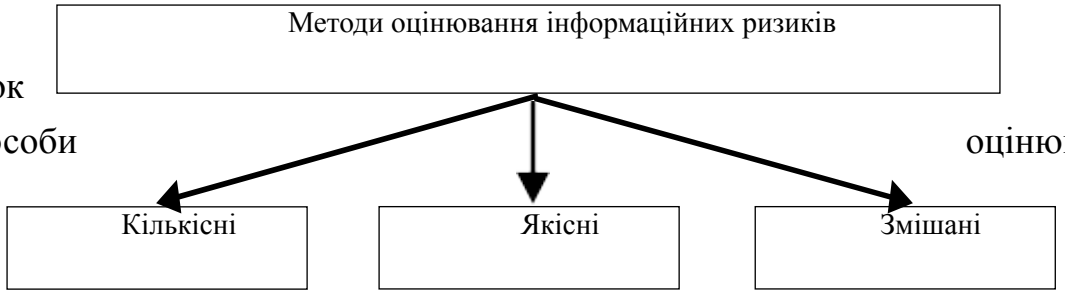

Рисунок 2.1 – Способи оцінювання інформаційних ризиків

Розглянемо більш детально способи оцінювання інформаційних ризиків.

Всі методи оцінювання ризику можна поділити на кількісні, якісні або комбінацію кількісних методів з якісними (змішані).

Кількісні методи використовують вимірні та об'єктивні дані для визначення вартості активів, ймовірності збитків і пов'язаних ризиків. Основною метою є обчислення числових значень для кожного компонента, отриманих під час оцінювання ризиків та аналізу витрат і вигоди.

З іншого боку, якісні методи використовують порівняльний показник для визначення ризику або вартості активу, спираючись на рейтинги або класифікації, такі як «низький, середній, високий», «неважливий, важливий, дуже важливий» або «за шкалою від 1 до 9». Якісна модель швидко та економічно ефективно оцінює дії та ймовірності виявлених ризиків. Набори ризиків реєструються та аналізуються в якісній оцінці ризику, яка потім може служити основою для цільової кількісної оцінювання.

Розглянемо найбільш відомі методики управління ризиками інформаційної безпеки такі як: Information Security Assessment and Monitoring Method (ISAMM), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), CCTA Risk Analysis and Management Method (CRAMM), Microsoft, Factor Analysis of Information Risk (FAIR), матрична методологія, для того щоб визначити найбільш прийнятну методику для оцінювання ризиків віртуальної інфраструктури.

ISAMM – кількісний метод, який був розроблений на основі Telindus. Це кількісний тип методології управління ризиками, де оцінюються ризики, які виражаються через їхні щорічні очікувані збитки у грошових одиницях.

ISAMM дозволяє показувати й моделювати зниження ризику для кожного поліпшеного контролю і порівнювати з його вартістю реалізації. Ефективність методу дозволяє виконувати оцінювання ризику в рамках з мінімальними витратами часу і зусиль. Останньою еволюцією в методології ISAMM є надання активів. Це означає, що він може бути використаний для запуску оцінювання ризиків щодо активів або згрупувати набір активів. Цей метод оцінювання ризиків

складається з трьох основних частин: огляд; оцінка; результат розрахунків та звітність, має хорошу керівну документацію. На рис. 2.2 представлений SWOT-аналіз використання методу ISAMM.

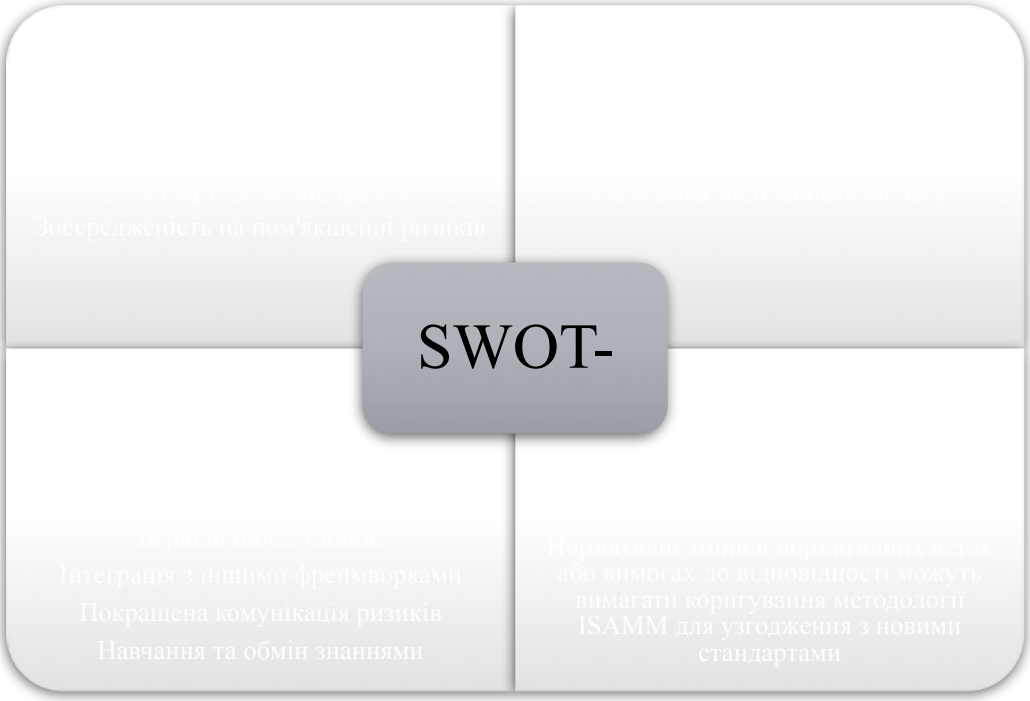

Рисунок 2.2 – SWOT-аналіз використання методу ISAMM

OCTAVE – якісний метод, який є самостійним підходом і вказує на те, що персонал несе відповідальність за встановлення стратегії безпеки організації. На рис. 2.3 представлено метод OCTAVE.

Рисунок 2.3 – Метод OCTAVE

OCTAVE потребує аналізу, який враховує взаємодію між критично важливими активами, загрозами для цих активів і вразливими місцями, охоплюючи як організаційні, так і технологічні аспекти. Він визначає пов’язані з інформацією активи, які мають значення для організації, і зосереджує зусилля на

цих активах через їхню першорядну важливість. На рис. 2.4 представлено SWOT-аналіз використання методу OCTAVE.

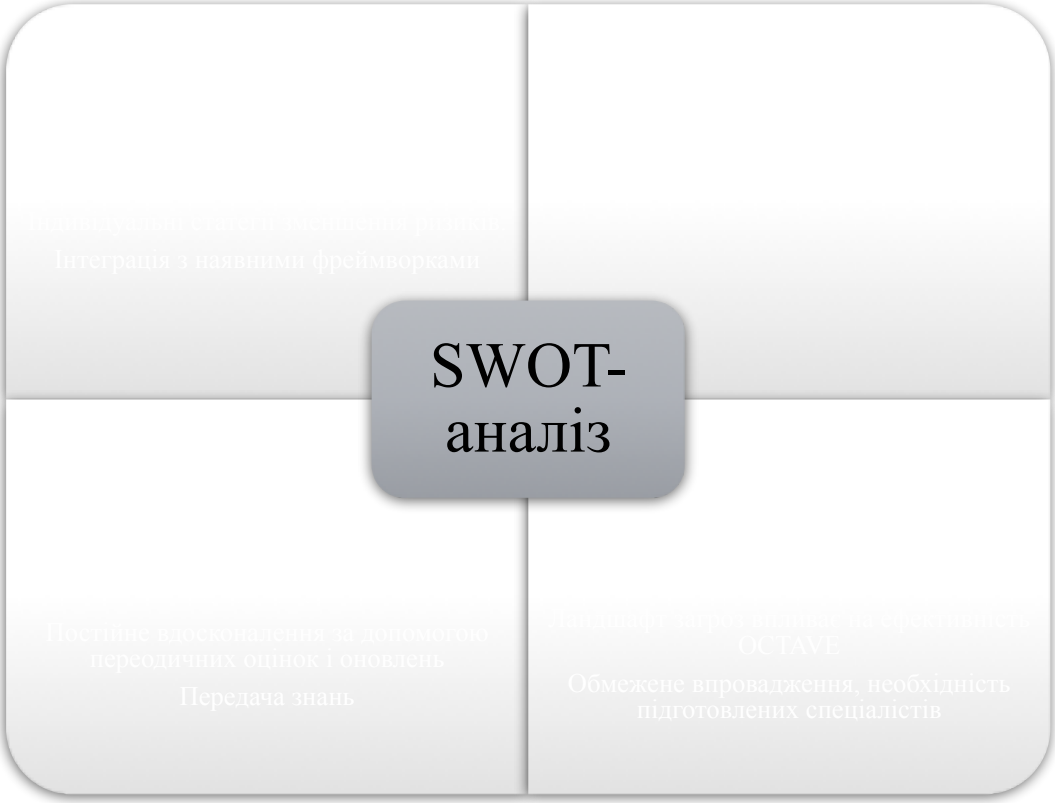

Рисунок 2.4 – SWOT-аналіз використання методу OCTAVE

CRAMM, гібридний метод, може бути складним для використання без спеціального інструменту CRAMM. Підхід CRAMM передбачає комплексний підхід до оцінювання ризиків, який поєднує як кількісні, так і якісні методи аналізу. Це універсальний метод, який підходить для організацій будь-якого розміру, будь то державні чи комерційні. Вміле використання методу CRAMM дає якісні результати, зокрема дозволяє економічно обґрунтувати витрати організації на інформаційну безпеку та безперервність бізнесу. Економічно обґрунтована стратегія управління ризиками зрештою призводить до економії коштів завдяки уникненню непотрібних витрат. Допоміжні програмні засоби також доступні для CRAMM. [13]. На рис. 2.5 представлений SWOT-аналіз використання методу CRAMM.

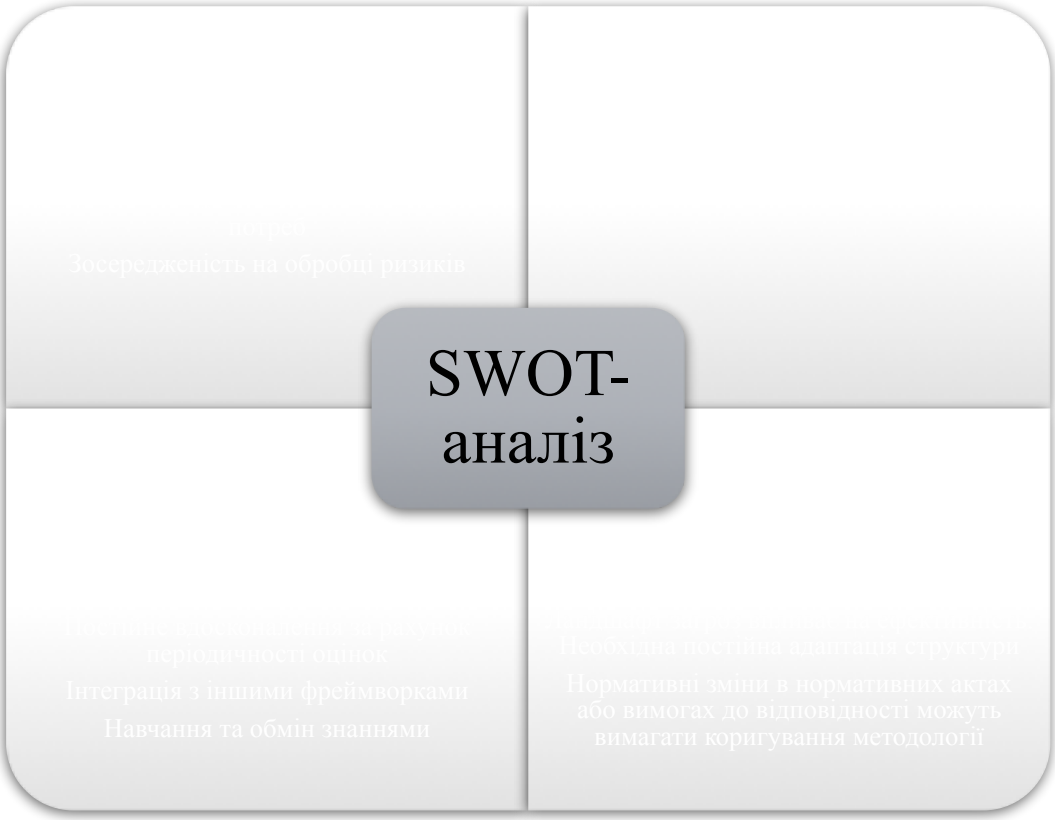

Рисунок 2.5 – SWOT-аналіз використання методу CRAMM

Методологія управління ризиками інформаційної безпеки, запропонована корпорацією Microsoft, яка представлена на рис. 2.6, містить детальний опис інструкцій по реалізації кожного з перерахованих етапів управління ризиками, огляд ключових факторів успіху, а також типові переліки IT-активів, загроз, вразливостей і шаблони документів, необхідних для реалізації процесу управління ризиками інформаційної безпеки.

Рисунок 2.6 – Методологія Microsoft

На рис. 2.7 зображено SWOT-аналіз використання методу Microsoft.

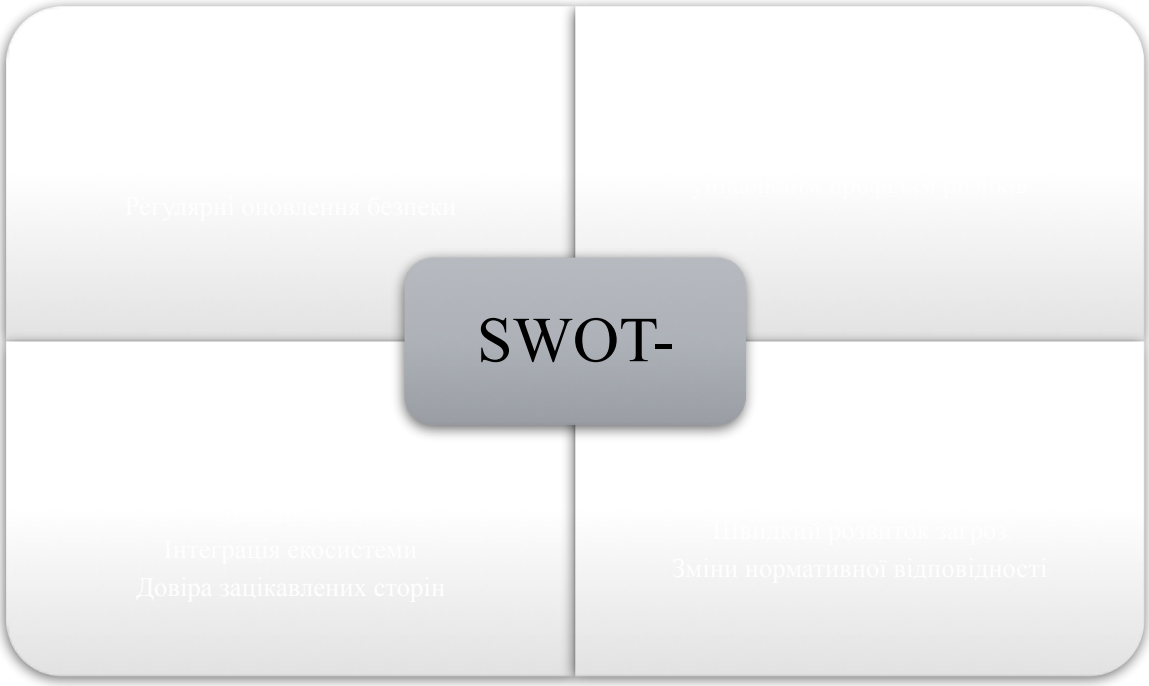

Рисунок 2.7 – SWOT-аналіз використання методу Microsoft

FAIR – це міжнародний кількісний метод оцінювання інформаційного ризику. Методика факторного аналізу інформаційних ризиків FAIR передбачає найбільш повне урахування факторів виникнення інформаційних ризиків.

FAIR дозволяє отримати опис достатньої кількості факторів, що впливають на оцінку ризику та конкретні значення ризику, яким би могли оперувати керівники підприємств. Основою методики FAIR є аналіз факторів, що впливають безпосередньо на ризик. Аналізуються фактори, що мають вплив на компоненти, які є складовими ризику. Відповідно до зазначеної методики, головними складовими ризику є частота появи інциденту та величина збитків від настання зазначеного інциденту. Кожна із цих складових поділяється на інші фактори: частота появи загрози, вразливість, первинні та вторинні збитки. Відповідно до методики FAIR, основним принципом ефективного керування кіберризиками є кількісний аналіз ризиків [14]. На рис. 2.8 зображено SWOT-аналіз використання методу FAIR.

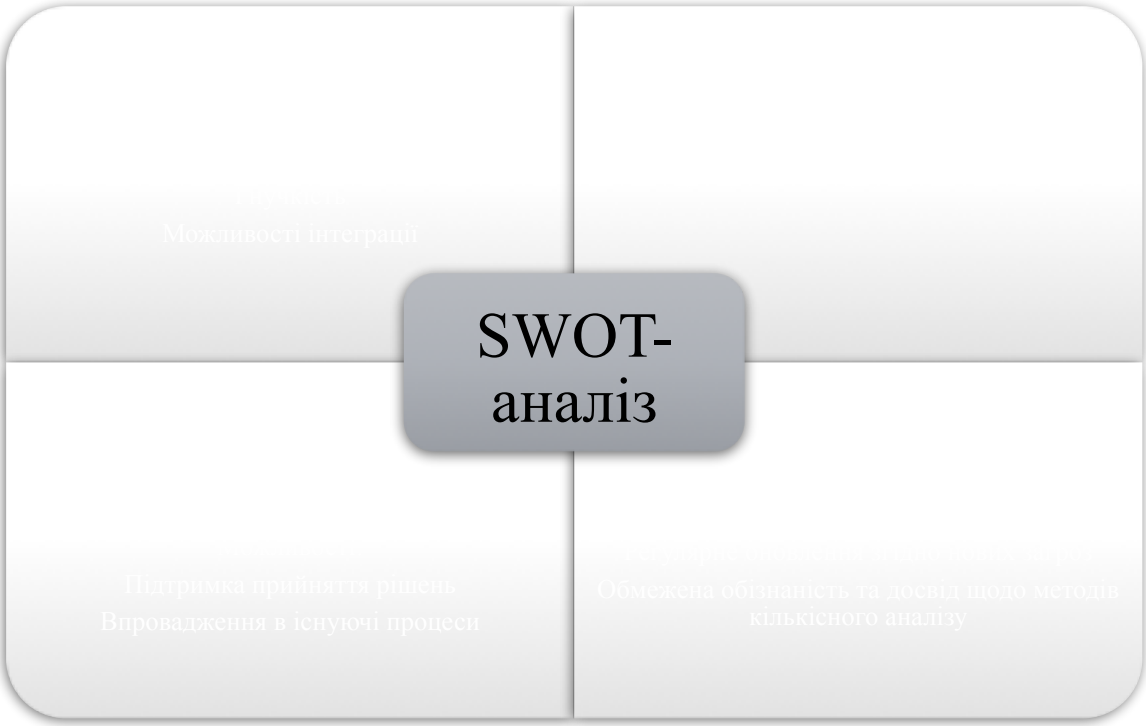

Рисунок 2.8 – SWOT-аналіз використання методу FAIR

Матрична методологія – використовує три окремі матриці, а саме: матрицю вразливостей, матрицю загроз та матрицю контролю для збору даних, необхідних для аналізу ризиків [15]. Матриця вразливостей містить зв'язки між активами та вразливими місцями в організації, приклад матриці вразливостей представлено в таблиці 2.1.

Таблиця 2.1 – Приклад матриці вразливостей активів

	Активи								
	Комерційна таємниця	Репутація	Витрати	Інформація	Апаратне забезпечення	Програми	Послуги	Комунікація	Сукупний вплив
Відносна вартість активів C_i	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	
Вразливості									
Вебсервери	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	V_1
Обчислювальні сервери	a_{21}	a_{22}	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}	a_{28}	V_2
Маршрутизатори	a_{31}	a_{32}	a_{33}	a_{34}	a_{35}	a_{36}	a_{37}	a_{38}	V_3

Сукупний вплив вразливостей V_j на активи організації розраховується за формулою:

$$V_j = \sum_{i=1}^{n} (a_{ij} \bullet C_i), \quad (2.1)$$

де j – номер вразливості;

і – номер критичного активу;

C_i – відносна вартість активу;

a_{ij}– приведене в таблиці число, що характеризує ступінь впливу j – тої вразливості на і – критичний актив.

В таблиці 2.2 за такою ж методикою враховуємо можливості реалізації окремих типів загроз через вразливості елементів захисту

Таблиця 2.2 – Приклад матриці загроз

	Вразливості							
	Вебсервер	Маршрутизатор	Клієнт	Базиданих	Брандмауери	Програмне	Передача	Сукупназначущість загро
Відносний вплив вразливостей V_j	V_1	V_2	V_3	V_4	V_5	V_6	V_7	
Загрози								
Атаки на відмову в обслуговуванні	d_{11}	d_{12}	d_{13}	d_{14}	d_{15}	d_{16}	d_{17}	T_1
Маскування	d_{21}	d_{22}	d_{23}	d_{24}	d_{25}	d_{26}	d_{27}	T_2
Шкідливий код(віруси тощо)	d_{31}	d_{32}	d_{33}	d_{34}	d_{35}	d_{36}	d_{37}	T_3
Людські помилки	d_{41}	d_{42}	d_{43}	d_{44}	d_{45}	d_{46}	d_{47}	T_4
Інсайдерські атаки	d_{51}	d_{52}	d_{53}	d_{54}	d_{55}	d_{56}	d_{57}	T_5
Вторгнення	d_{61}	d_{62}	d_{63}	d_{64}	d_{65}	d_{66}	d_{67}	T_6

Сукупна значущість загрози T_k розраховується за формулою:

$$T_k = \sum_{j=1}^{m} (d_{jk} \bullet V_j), \quad (2.2)$$

де k – номер загрози;

d_{jk} – ступінь можливості реалізації k – тої загрози через j – ту вразливість елементу системи захисту.

В третій матриці враховуємо протидію окремих елементів захисту до загроз, приклад матриці контролю продемонстровано в таблиці 2.3.

Таблиця 2.3 – Приклад матриці контролю

	Загрози						
	Відмова	Спуфінг	Шкідливий код	Людські помилки	Інсайдерські атаки	Розсилка спаму	Сукупна ефективність контрзаходів
Відносна значущість загроз T_k	T_1	T_2	T_3	T_4	T_5	T_6	
Засоби протидії та контролю							
Конфігурація архітектури	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}	A_1
Брандмауери	e_{21}	e_{22}	e_{23}	e_{24}	e_{25}	e_{26}	A_2
Intrusion Detection System	e_{31}	e_{32}	e_{33}	e_{34}	e_{35}	e_{36}	A_3
Єдиний вхід	e_{41}	e_{42}	e_{43}	e_{44}	e_{45}	e_{46}	A_4
Демілітаризована зона	e_{51}	e_{52}	e_{53}	e_{54}	e_{55}	e_{56}	A_5
Політика безпеки	e_{61}	e_{62}	e_{63}	e_{64}	e_{65}	e_{66}	A_6
Навчання співробітників	e_{71}	e_{72}	e_{73}	e_{74}	e_{75}	e_{76}	A_7

Сукупна ефективність контрзаходів A_l розраховується за формулою:

$$A_l = \sum_{l=1}^{q} (e_{kl} \bullet T_k), \tag{2.3}$$

де l – номер контрзаходу;

e_{kl} – вплив l – того контрзаходу на k-ту загрозу.

Кожна частина матриці містить значення зв'язку між елементом рядка і стовпця таблиці (наприклад, активом і вразливістю).

На початковому етапі аналізу ризиків створюються списки активів, вразливостей, загроз і засобів контролю, які додаються до відповідних таблиць. Потім матриці заповнюються шляхом додавання даних, які співвідносять рядок матриці зі стовпчиком матриці. дані з матриці вразливостей агрегуються за допомогою формули (2.1), а потім каскадуються в таблицю 2.2. Аналогічно, дані з матриці загроз агрегуються за допомогою формули (2.2) і каскадуються в таблицю 2.3. Дані з матриці засобів контролю потім агрегуються для отримання відносної важливості різних засобів контролю [15].

Матрична методологію аналізу ризиків інформаційної безпеки можна легко адаптувати. Методологія містить прості у використанні шаблони, які можна поступово вдосконалювати в міру надходження додаткової інформації [16]. На рис. 2.9 зображено SWOT-аналіз використання методу матричного методу.

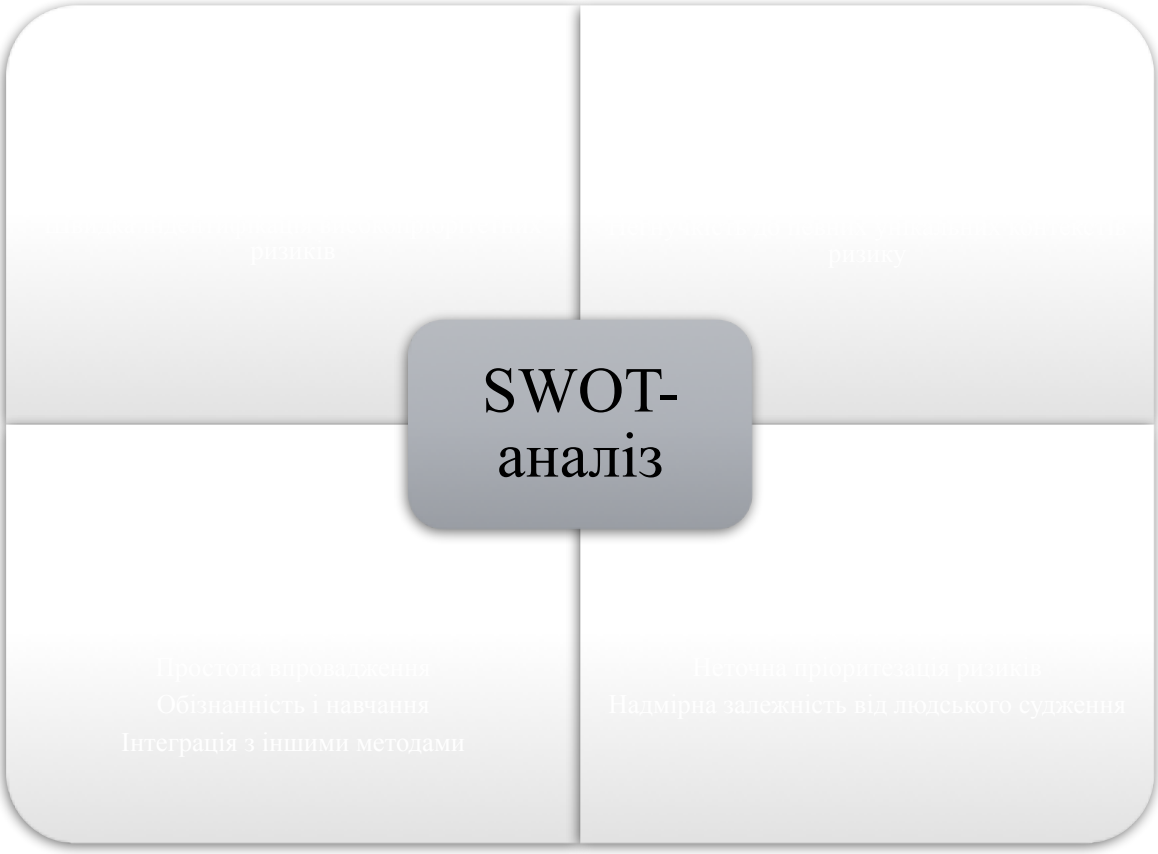

Рисунок 2.9 – SWOT-аналіз використання матричного методу

Методи управління ризиками інформаційної безпеки, такі як ISAMM, OCTAVE, CRAMM, Microsoft, FAIR і матрична методологія оцінювання ризиків, забезпечують різні підходи до оцінювання та управління ризиками в різних

середовищах. Хоча кожен метод має свої сильні сторони та обмеження, матрична методологія оцінювання ризиків особливо підходить для оцінювання ризиків віртуальної інфраструктури. Розглянемо основні переваги матричної методології:

- комплексна оцінка: матрична методологія оцінювання ризику пропонує комплексний підхід до оцінювання ризику, враховуючи різні параметри, такі як вартість активів, ймовірність загрози, вразливість і вплив. Це дозволяє проводити оцінювання ризиків у віртуальній інфраструктурі з урахуванням багатьох факторів, які можуть вплинути на стан безпеки;
- ясність і простота: матрична методологія використовує матричний формат для відображення та оцінювання ризиків. Це візуальне представлення спрощує розуміння рівнів ризику, забезпечуючи ясність і легкість інтерпретації. Це дозволяє легко ідентифікувати зони високого ризику у віртуальній інфраструктурі, полегшуючи ефективні стратегії зменшення ризиків;
- аналіз взаємозалежності: віртуальна інфраструктура часто передбачає взаємозалежність між активами та вразливими місцями. Матрична методологія оцінювання ризиків враховує цей аспект, враховуючи взаємозалежність активів та їхній зв’язок з вразливими місцями та загрозами. Це допомагає зрозуміти, як ризики можуть поширюватися у віртуальному середовищі, і відповідно розставляти пріоритети заходів із пом’якшення;
- гнучкість і налаштування: матричну методологію оцінювання ризиків можна налаштувати відповідно до конкретних потреб і характеристик віртуальної інфраструктури. Організації можуть визначати власні критерії для оцінювання активів, ймовірності загрози та впливу, адаптуючи матрицю відповідно до свого унікального середовища. Ця гнучкість дозволяє точніше та відповідніше оцінювати ризики, характерні для віртуальної інфраструктури;
- пріоритезація ризиків: матрична методологія оцінювання ризиків забезпечує систематичний підхід до визначення пріоритетів ризиків на основі їхньої серйозності, беручи до уваги як ймовірність виникнення, так і потенційний вплив. Це дозволяє організаціям зосередити свої ресурси та зусилля на усуненні найбільш критичних ризиків у віртуальній інфраструктурі, максимізуючи ефективність зменшення ризиків;

- підтримка прийняття рішень: матрична методологія є інструментом підтримки прийняття рішень, що дозволяє організаціям робити обґрунтований вибір щодо варіантів зменшення ризиків.

Загалом матрична методологія добре підходить для оцінювання ризиків віртуальної інфраструктури завдяки комплексному підходу до оцінювання, чіткості, урахуванню взаємозалежностей, гнучкості, можливостям визначення пріоритетів ризиків і функціям підтримки прийняття рішень. Її здатність забезпечувати структурованість, що адаптується, робить його ефективним методом оцінювання та управління ризиками у віртуальних середовищах. Інші методи, такі як ISAMM, OCTAVE, CRAMM, Microsoft і FAIR теж підходять для оцінювання ризиків віртуальної інфраструктури але мають свої обмеження: складність, ресурсовитратність, обмеження масштабованості і застосовності по часу, необхідності точності вихідних даних.

3 ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІРТУАЛЬНОЇ ІНФРАСТРУКТУРИ

3.1. Побудова моделі об’єктів захисту віртуального середовища

При складанні шкали активів для віртуального середовища важливо враховувати різні компоненти та елементи, які сприяють функціонуванню віртуальної інфраструктури. Нижче наведено основні активи, які зазвичай зустрічаються у віртуальному середовищі:

- віртуальні машини – це основні одиниці віртуальної інфраструктури, що представляють окремі операційні системи та програми, що працюють на віртуалізованому обладнанні;
- хости віртуалізації – фізичні сервери, на яких розміщені віртуальні машини, що забезпечують обчислювальні ресурси та можливості віртуалізації;
- гіпервізор – програмне забезпечення або вбудоване програмне забезпечення, яке забезпечує віртуалізацію шляхом керування розподілом і використанням фізичних ресурсів між кількома віртуальними машинами;
- консолі керування: інструменти або інтерфейси, що використовуються для керування та моніторингу віртуального середовища, включаючи такі функції, як надання, розподіл ресурсів і моніторинг продуктивності;
- віртуальні мережі – віртуалізована мережева інфраструктура, яка з’єднує віртуальні машини та полегшує зв’язок між ними та із зовнішніми мережами;
- інфраструктура зберігання – системи зберігання, які використовуються для зберігання образів дисків віртуальної машини, знімків та інших даних, пов’язаних із віртуальним середовищем;
- системи резервного копіювання – рішення або процеси для резервного копіювання та відновлення даних віртуальної машини для забезпечення цілісності та доступності даних;
- інфраструктура безпеки – інструменти та механізми безпеки, реалізовані для захисту віртуального середовища, включаючи брандмауери, системи виявлення вторгнень і засоби контролю доступу;

- системи керування конфігурацією – інструменти та процеси, що використовуються для керування та підтримки конфігурації віртуальних машин і пов’язаних із ними ресурсів;
- системи моніторингу та звітності – рішення для моніторингу продуктивності та працездатності віртуального середовища, створення звітів і виявлення аномалій або проблем;
- аварійне відновлення та безперервність бізнесу – стратегії та механізми для забезпечення доступності та відновлення віртуального середовища у разі збоїв або катастроф;
- ліцензування та відповідність – процеси та механізми для керування ліцензіями на програмне забезпечення та забезпечення дотримання відповідних нормативних актів та ліцензійних угод.

Захист інформації в будь-якій інформаційній системі, у тому числі побудованій на основі використання технології віртуалізації – це діяльність, яка полягає у створенні бар'єрів, призначення яких забезпечуватиме захист даних від доступу неавторизованого суб'єкта. Оскільки бар'єри покликані забезпечувати безпеку на шляхах поширення потенційно можливих загроз, для визначення місць розміщення засобів захисту в інформаційних системах (ІС) підприємства, що функціонує з використанням технології віртуалізації, має бути побудована деталізована модель об’єктів захисту безпеки віртуального середовища.

Базуючись на основних активах, які зустрічаються у віртуальному середовищі побудуємо діаграму, що ілюструє взаємозалежності активів віртуальної інфраструктури, яка базується на продукті VMWare, який заснований на віртуалізації серверних ОС. Ця діаграма представлена на рис. 3.1. за допомогою вузлів з’єднаних лініями, кожен вузол представляє актив, а лінії зображують зв’язки або залежності між ними.

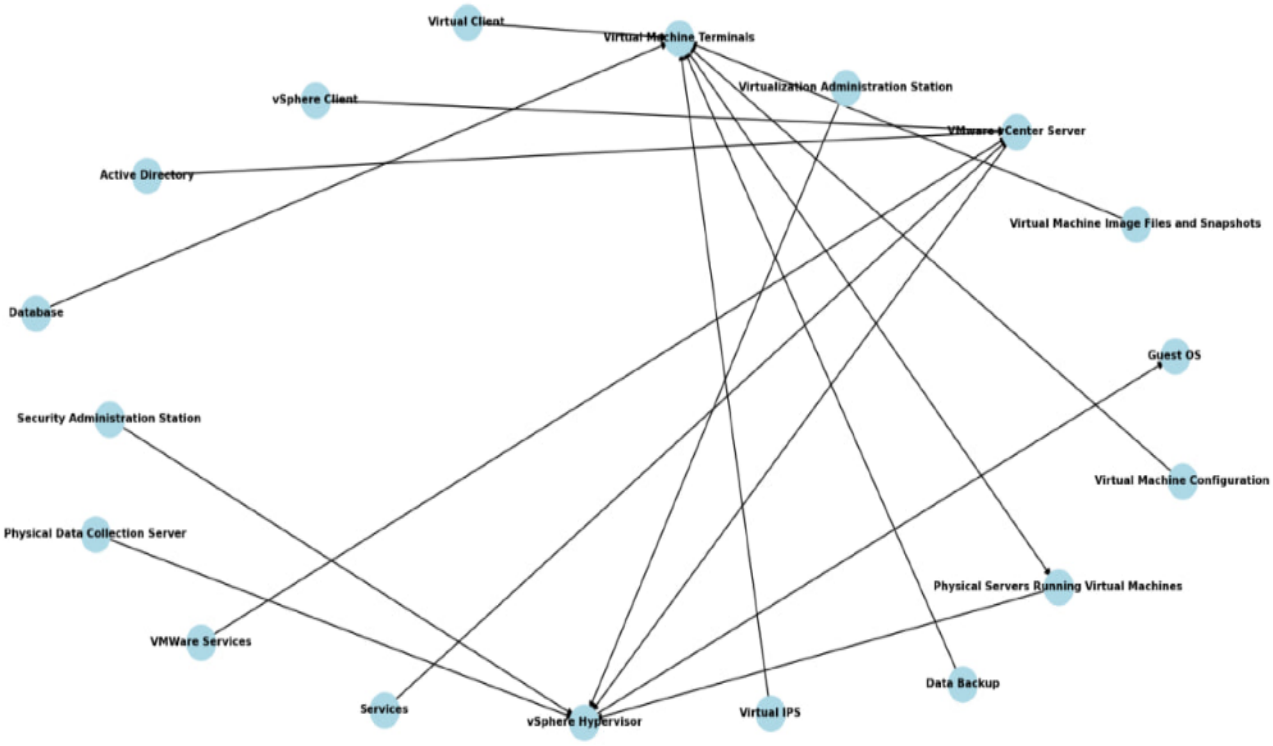

Рисунок 3.1 – Діаграма взаємозалежності активів віртуальної інфраструктури

Розглянемо кожну взаємозалежність, згадану на рис. 3.1:

- термінали віртуальної машини підключені до станції адміністрування віртуалізації, станції адміністрування безпеки та фізичних серверів, на яких запущені віртуальні машини. Це означає, що термінали покладаються на ці компоненти для своєї роботи та функціональності. Термінали можуть спілкуватися зі станціями адміністрування з метою керування та отримувати доступ до ресурсів на фізичних серверах, на яких працюють віртуальні машини;
- станція адміністрування віртуалізації служить центральною точкою керування для віртуальної інфраструктури. Вона підключена до терміналів віртуальної машини, станції адміністрування безпеки, фізичних серверів, на яких запущено віртуальні машини, та інших відповідних активів. Це підключення означає, що станція адміністрування взаємодіє з цими компонентами та контролює їх, керуючи віртуальними машинами, налаштуваннями безпеки та іншими пов’язаними операціями;
- станція адміністрування безпеки відповідає за керування та забезпечення безпеки віртуальної інфраструктури. Вона підключена до терміналів віртуальної машини та станції адміністрування віртуалізації, що вказує на її роль у моніторингу та налаштуванні параметрів безпеки для цих компонентів;
- фізичні сервери, на яких запущені віртуальні машини, розміщують фактичні екземпляри віртуальної машини. Вони підключені до терміналів віртуальної машини, станції адміністрування віртуалізації, станції адміністрування безпеки та інших відповідних активів. Це підключення означає, що сервери взаємодіють із цими компонентами, щоб надавати ресурси та послуги віртуальним машинам;
- сервер збору фізичних даних підключено до фізичних серверів, на яких запущені віртуальні машини та потенційно інші відповідні активи. Це підключення означає, що сервер збору даних покладається на фізичні сервери для збору та обробки даних з віртуальних машин;
- гіпервізор vSphere – це базовий рівень програмного забезпечення, який забезпечує віртуалізацію на фізичних серверах. Він підключений до терміналів віртуальних машин, фізичних серверів, на яких запущені віртуальні машини, та інших відповідних активів, що вказує на його роль в управлінні та полегшенні процесів віртуалізації;

- гостьова ОС відноситься до операційної системи, встановленої на кожній віртуальній машині;
- client vSphere: використовується для керування інфраструктурою vSphere та доступу до неї. Він підключений до терміналів віртуальної машини, станції адміністрування віртуалізації та інших відповідних активів, що вказує на його роль у наданні можливостей віддаленого керування та контролю;
- сервер VMware vCenter: централізована платформа керування для середовищ VMware. Він підключений до терміналів віртуальної машини, станції адміністрування віртуалізації та інших відповідних активів, що означає його роль в управлінні та контролі компонентів віртуальної інфраструктури;
- Active Directory: служба каталогів, яка використовується для централізованого керування мережевими ресурсами. Вона підключена до терміналів віртуальних машин, фізичних серверів, на яких запущені віртуальні машини, та інших відповідних активів, що вказує на її інтеграцію у віртуальну інфраструктуру для автентифікації користувачів і контролю доступу до ресурсів;
- сервіси VMware: спеціальні служби та компоненти, які надаються VMware для керування віртуалізацією. Вони підключені до терміналів віртуальної машини, станції адміністрування віртуалізації та інших відповідних активів, що представляє їхній зв’язок із віртуальною інфраструктурою;
- virtual Intrusion Prevention System (IPS): компонент безпеки, розгорнутий у віртуальній інфраструктурі для виявлення та запобігання мережевим вторгненням. Він підключений до терміналів віртуальної машини, станції адміністрування безпеки та інших відповідних активів, що вказує на його роль у захисті віртуального середовища;
- база даних являє собою репозиторій для зберігання та керування даними у віртуальній інфраструктурі. Він підключений до терміналів віртуальних машин, фізичних серверів, на яких запущені віртуальні машини, та інших відповідних активів, що підкреслює його інтеграцію з цими компонентами для зберігання та пошуку даних;
- файли іміджів віртуальної машини та снепшотів підключені до терміналів віртуальних машин, фізичних серверів, на яких запущені віртуальні машини, та інших відповідних активів, що представляє їхній

зв’язок із цими компонентами для надання та керування віртуальною машиною;

- резервне копіювання даних підключене до терміналів віртуальних машин, фізичних серверів, на яких працюють віртуальні машини, та інших відповідних активів, що вказує на його роль у захисті та відновленні даних;
- конфігурація віртуальної машини підключена до терміналів віртуальної машини, станції адміністрування віртуалізації та інших відповідних активів, представляючи його зв’язок із цими компонентами для керування та налаштування віртуальної машини.

Ці взаємозалежності підкреслюють зв’язок і відносини між різними активами у середовищі віртуальної інфраструктури. Розуміння цих зв’язків має вирішальне значення для оцінювання ризиків, впровадження заходів безпеки та забезпечення безперебійної роботи та захисту віртуального середовища.

На основі представлених взаємозалежностей побудуємо моделі об’єктів захисту. В таблиці 3.1 представлена модель об’єкту захисту обчислювальної техніки віртуального середовища. В таблиці 3.2 продемонстрована модель об’єкту захисту інформаційних технології віртуального середовища Для кожного елементу ресурсу прописані відомі вразливості, опис відомих вразливостей та дефектів безпеки для віртуального середовища можна побачити в таблиці А.1 [17]. В таблиці 3.3 представлена модель об’єкту захисту інформаційних ресурсів віртуального середовища.

Таблиця 3.1 – Модель об’єкту захисту обчислювальної техніки віртуального середовища

Найменування елементу ресурсу	Рівень фізичного доступу	Вбудовані сервіси безпеки	Розташування елемента ресурсу
Термінали користувачів віртуальних машин (ВМ)	Співробітники відділу підприємства	Антивірус	Відповідні відділи підприємства
Робоча станція адміністратор віртуалізації	Адміністратор віртуалізації	Active Directory, Антивірус	Адміністративний сегмент
Робоча станція адміністратора безпеки	Адміністратор безпеки	Active Directory, Антивірус	Адміністративний сегмент
Фізичні сервери з запущеними віртуальними машинами	Адміністратор безпеки, адміністратор віртуалізації	Active Directory, Антивірус, ACL	Серверна кластеру віртуалізації
Фізичний сервер зберігання даних	Адміністратор безпеки, адміністратор віртуалізації	Active Directory, Антивірус, ACL	Серверна кластеру віртуалізації

Таблиця 3.2 – Модель об’єкту захисту інформаційних технологій віртуального середовища

№	Найменування елементу ресурсу	Common Vulnerabilities and Exposures (CVE)	Суб’єкт доступу	Розташування елементу
1	2	3	4	5
1	Гіпервізор типу vSphere	CVE-2013-1405, CVE-2012-5703, CVE-2012-1666, CVE-2016-5331	Адміністратор віртуалізації	Сервер VMWare
2	Гостьова ОС		Адміністратор віртуалізації	Сервер VMWare
3	vSphere Client	CVE-2014-1210, CVE-2014-1209, CVE-2013-1405, CVE-2013-5971, CVE-2012-1512.	Адміністратор віртуалізації	Робоча станція адміністратора віртуалізації, термінали клієнтів
4	VMware vCenter Server	CVE-2014-3790, CVE-2013-5973, CVE-2013-1212, CVE-2013-3107	Адміністратор віртуалізації	ПК адміністратора віртуалізації
5	ВМ vSphere	CVE-2014-3790, CVE-2014-1210, CVE-2014-1209, CVE-2013-5556	Адміністратор віртуалізації, клієнт ВМ	Сервер VMWare
6	Active Directory	CVE-2014-8764, CVE-2014-0602	Адміністратор безпеки	VMWareESX
7	Служби, сервіси VMWare	CVE-2014-3608, CVE-2014-6278, CVE-2014-7187, CVE-2014-7169	Адміністратор віртуалізації, клієнт ВМ	Сегмент віртуалізації

Продовження таблиці 3.2

1	2	3	4	5
8	Віртуальний міжмережевий екран	CVE-2013-6398, CVE-2007-4967, CVE-2006-7160	Адміністратор віртуалізації	Периметр віртуальної інфраструктури
9	Virtual IPS	CVE-2010-0827	Адміністратор віртуалізації	Периметр віртуальної інфраструктури

Таблиця 3.3 – Модель об’єкту захисту інформаційних ресурсів віртуального середовища

№ елементу	Найменування елементу ресурсу	Суб’єкт доступу	Місцезнаходження елемента ресурсу
1	Бази даних	Користувачі віртуальних машин	Сховище даних
2	Файли іміджів та снепшотів віртуальних машин	Користувачі віртуальних машин, адміністратор віртуалізації	Сховище даних
3	Службова інформація	Адміністратор віртуалізації, адміністратор безпеки	Робоча станція адміністратора безпеки/ віртуалізації
4	Бекапи даних	Адміністратор віртуалізації	Сховище даних
5	Конфігурація віртуальних машин	Користувачі віртуальних машин	Робоча станція користувачів

Численні технологічні рішення віртуалізації містять функції безпеки на платформі, що дозволяє експертам із безпеки застосовувати протоколи безпеки для програм. Зазначені атаки можуть бути здійснені, якщо зловмисник отримає доступ до інструментів адміністрування.

Правильна конфігурація інструментів керування як фізичною, так і віртуальною інфраструктурою, а також використання інструментів віртуальної безпеки, які відстежують трафік на сервері віртуалізації, є важливими. Процедура

централізованого керування віртуальною машиною має відповідати інструкціям щодо безпеки організації.

Дослідження безпеки технологій віртуалізації зосереджені в основному на використанні конкретних вразливостей. Отже, у службах хмарних обчислень часто приділяється надмірна увага зусиллям щодо вразливостей або підходу, орієнтованого на вразливості, тоді як для виявлення загальних кореневих проблем безпеки докладається мало зусиль. вразливостям системи та інцидентам приділяється увага на мікрорівні, а не розгляду більш масштабних сценаріїв і моделей загроз і подальшої розробки стратегій зменшення ризиків.

Таким чином, застосуємо діаграму Fishbone або Ishikawa для визначення характеристики безпеки за допомогою структурованого підходу. Його головна перевага – окреслити основні причини проблеми, у нашому випадку питання безпеки.

Діаграма Fishbone спочатку використовувалася для виявлення та групування причин проблем із якістю на виробничій лінії. Згодом він отримав широке застосування в управлінні якістю. Ця методологія була названа на честь Каору Ісікава, японського статистика з контролю якості, людини, яка піонером використовувала цю діаграму в 1960-х роках. Діаграма «Риб’яча кістка» – це інструмент аналізу, який забезпечує систематичний спосіб розгляду наслідків і причин, які створюють або сприяють цим наслідкам. Через функцію діаграми «Риб’яча кістка» її можна назвати діаграмою причинно-наслідкових зв’язків.

Застосуємо діаграму Ісікави для аналізу ризиків безпеки гіпервізора . Ця методологія окреслює у схемній формі причини, які можуть спричинити певний результат. Наприклад, скомпрометований гіпервізор, кожній головній причині відповідали загрози: підробка, фальсифікація, відмова, розкриття інформації, відмова в обслуговуванні та підвищення привілеїв. Діаграма визначає проблеми безпеки гіпервізора як ті невизначені події, які можуть призвести до виникнення впливу. На рис. 3.2 представлено аналіз безпеки гіпервізора.

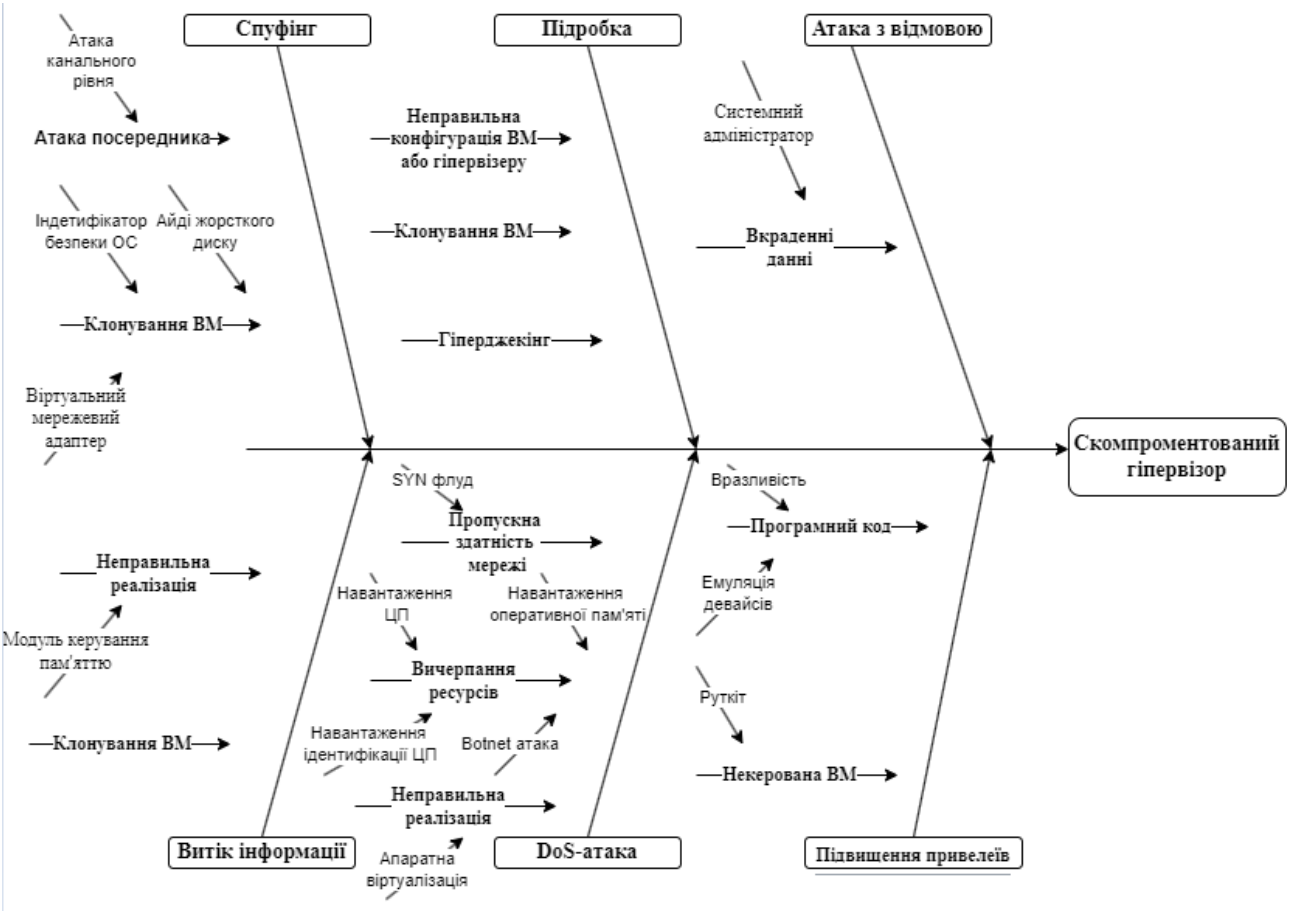

Рисунок 3.2 – Діаграма Fishbone

З діаграми бачимо, що більшість випадків походять від вразливого програмного коду та архітектури продукту. Таким чином, превентивні контрзаходи безпеки повинні бути розглянуті на ранніх етапах перед початком роботи.

Окремі результати дослідження вразливостей гіпервізора були представлені в документі NISTIR 8221 [18]. A methodology for Enabling Forensic Analysis Using Hypervisor Vulnerabilities Data. В цій методології проведено дослідження вразливостей та атак гіпервізорів. На ринку гіпервізорів є чотири провідні продукти: Microsoft Hyper-V, VMware VSphere/ESX, Citrix XenServer/Xen та KVM. Перші два Microsoft Hyper-V та VMware VSphere/ESX – є комерційними продуктами, тоді як останні два є продуктами з відкритим вихідним кодом. Ці продукти з відкритим вихідним кодом (тобто Xen і KVM) були обрані як платформи для класифікації атак на гіпервізор. В даному документі представлений відносний розподіл вразливостей для такої функціональності гіпервізора:

- vCPU;
- VSMP;
- Soft MMU;
- I/O and Networking;
- Interrupt/Timer;
- Hypercalls;
- VMExit;
- VM Management;
- Remote Management Software;
- Hypervisor Add-ons.

Класифікації вразливостей засновані на функціональних можливостях гіпервізора, наведено в таблиці 3.4.

Таблиця 3.4 – Вразливості гіпервізорів Xen та KVM класифіковані за функціоналом гіпервізора

Функціональність гіпервізора	Гіпервізор Xen	Гіпервізор KVM
vCPU	6 (7 %)	4 (20 %)
VSMP	0 (0 %)	0 (0 %)
Soft MMU	34 (40 %)	5 (25 %)

Продовження таблиці 3.4

I/O and Networking	24 (29 %)	4 (20 %)
Interrupt/Timer	7 (8 %)	3 (15 %)
Hypercalls	3 (4 %)	1 (5 %)
VMExit	1 (1 %)	2 (10 %)
VM Management	7 (8 %)	0 (0 %)
Remote Management Software	1 (0 %)	0 (0 %)
Hypervisor Add-ons	0 (0 %)	1 (5 %)

За винятком функціональності віртуальної симетричної багатопроцесорної обробки, всі функціональні можливості були визнані вразливими. Наведено кількість вразливостей та їхнє відсоткове співвідношення для кожного гіпервізора. З таблиці 3.5 видно, що вразливостей в Xen більше, ніж в KVM. Однією з причин цього може бути ширша база користувачів Xen. Крім того, приблизно 69 % вразливостей в Xen та 45 % вразливостей в KVM сконцентровано в двох функціональних можливостях програмному модулі Soft MMU та I/O and Networking.

Вразливості, що базуються на функціоналі вводу/виводу та мереж, також були пов'язані з кожним з чотирьох типів віртуалізації вводу/виводу: повністю віртуалізовані пристрої, паравіртуалізовані пристрої, пристрої з прямим доступом та само-віртуалізовані пристрої. Таблиця 3.5 показує, що більшість вразливостей вводу/виводу та мережевих вразливостей в Xen походять з паравіртуалізованих пристроїв, в той час як всі вразливості вводу/виводу та мережеві вразливості в KVM походять з повністю віртуалізованих пристроїв. Це пов'язано з тим, що в більшості Xen функціональність вводу/виводу та мережі налаштовується за допомогою паравіртуалізованого пристрою, в той час як в KVM ця функціональність налаштовується за допомогою повністю віртуалізованого пристрою.

В таблиці 3.5 представлені вразливості Xen та KVM класифіковані за функціоналом гіпервізора, а в таблиці 3.6 представлені джерела атак та кількість експлойтів на гіпервізори.

Таблиця 3.5 – Вразливості Xen та KVM класифіковані за функціоналом гіпервізора

Тип атаки	Гіпервізор Xen	Гіпервізор KVM
Відмова в обслуговуванні	48 (44 %)	17 (63 %)
Ескалація привілеїв	33 (30 %)	3 (11 %)
Витік інформації	15 (14 %)	5 (19 %)
Довільне виконання коду	8 (7 %)	2 (7 %)
Читання/зміна/видалення файлу	3 (3 %)	0 (0 %)
Компроментація хоста, сканування операцій інших адміністраторів і пошкодження даних	3 (3 %)	0 (0 %)

Таблиця 3.6 – Джерела атак та кількість експлойтів на гіпервізори

Джерело атаки	Гіпервізор Xen	Гіпервізор KVM
Адміністратор	2 (2 %)	0 (0 %)
Адміністратор гостьової ОС	17 (20 %)	1 (5 %)
Гостьовий користувач ОС	63 (76 %)	17 (85 %)
Віддалений зловмисник	1 (1 %)	1 (5 %)
Користувач хост-системи	0 (0 %)	1 (5 %)

Таблиця 3.6 показує, що найпоширенішим типом атаки був DoS (44 % для Xen та 63 % для KVM), що свідчить про те, що атаки на доступність хмарних сервісів можуть бути серйозною проблемою безпеки хмарних технологій. Іншими найбільш поширеними атаками були підвищення привілеїв (30 % для Xen і 11 % для KVM), витік інформації (14 % для Xen і 19 % для KVM) та довільне виконання коду (7 % для Xen і 7 % для KVM). Хоча кожна з цих трьох атак трапляється рідше, ніж DoS-атака, всі вони несуть потенційний ризик витоку конфіденційної інформації користувачів або компрометації хостів чи гостьових віртуальних машин. Таблиця 3.7 показує, що найбільшим джерелом усіх атак були

користувачі гостьових ОС (76 % для Xen і 85 % для KVM). Це свідчить про те, що хмарні провайдери повинні уважно стежити за діями гостьових користувачів, щоб зменшити ризики атак [17].

На жаль, окремі результати дослідження вразливостей для віртуальних інфраструктур які базуються на продукті VMware не є доступними, тому що це комерційний продукт, доступність статистики вразливостей і даних про загрози може залежати від різних факторів, наприклад, відсутність статистики вразливостей для продуктів VMware може бути пов’язано з практикою звітування про вразливості дослідниками безпеки та організаціями. Про вразливості, виявлені в продуктах VMware, зазвичай повідомляють через відповідальні канали розкриття інформації, такі як VMware Security Response Center або CVE. Тому конкретні статистичні дані, можуть бути недоступними. VMware регулярно випускає поради щодо безпеки та виправлення для виявлених вразливостей у своїх продуктах. Однак серйозність і вплив цих вразливостей можуть відрізнятися. Деякі вразливості можуть бути більш критичними та широко відомими, і вони будуть опубліковані у публічних звітах і статистичних даних, тоді як інші можуть бути менш серйозними або специфічними для певних середовищ, що призводить до меншої видимості.

Хоча конкретна статистика вразливостей і дані про загрози для продуктів VMware на даний момент є недоступними, важливо зазначити, що VMware активно вирішує питання безпеки, випускає рекомендації щодо безпеки та співпрацює зі спільнотою безпеки для підтримки безпеки та цілісності своїх продуктів. Рекомендуємо стежити за останніми порадами щодо безпеки та дотримуватися рекомендованих практик безпеки, наданих VMware, щоб підвищити безпеку вашої віртуальної інфраструктури.

3.2. Оцінювання потенційних вразливостей моделі віртуальної інфраструктури

Оцінювання ризиків у віртуальному середовищі проводитиметься за такими кроками:

- оцінювання активів – включає визначення та класифікацію ресурсів, які потребують захисту;
- аналіз джерел проблем – це включає побудову моделі злочинця, створення моделі загрози та визначення вразливості;
- оцінювання ризику. Тут упорядковуються та класифікуються результати попереднього етапу;

- прийняття рішень – це робиться на основі висновків звіту про аналіз ризиків.

Щоб зібрати дані для аналізу ризиків, будемо використовувати три окремі матриці: матрицю вразливостей, матрицю загроз і матрицю контролю. Матриця вразливостей відображає кореляцію між ресурсами та вразливістю у віртуальному середовищі, матриця загроз вказує на кореляцію між вразливістю та загрозами, а матриця контролю відображає кореляцію між загрозами та заходами контролю.

Під час початкового аналізу ризиків створимо списки активів, вразливостей, загроз та інструментів керування віртуальним середовищем. Заповнимо матриці, додавши дані про зв’язок між елементом стовпця матриці та елементом рядка. Дані з матриці вразливостей будуть реструктуровані та введені в матрицю загроз. Подібним чином дані з матриці загроз будуть передані в матрицю контролю, яка містить відносну значимість заходів контролю.

Початковим кроком в оцінювання ризику з використанням матричного методу є створення каталогу активів, вразливостей і загроз.

Для оцінювання взаємозалежності активів (загроз) і вразливостей будемо використовувати таку шкалу балів: 0 – немає впливу; від 1 до 2 – слабкий вплив; від 3 до 6 – помірний вплив; від 7 до 9 – сильний вплив.

Проведемо оцінювання ризиків моделі віртуальної інфраструктури на базі продукту VMware за допомогою матричного підходу на базі моделей які були представлені в таблицях 3.1, 3.2, 3.3. Вразливостями будемо вважати об’єкти віртуальної інфраструктури.

Матрицю вразливостей віртуальної інфраструктури надано в таблиці 3.7.

Таблиця 3.7 – Матриця вразливостей віртуальної інфраструктури

	Активи				Сукупний вплив
	Публічна інформація	Конфіденційна інформація	Фінансова інформація	Програмне забезпечення	
Вразливості/пріоритет	2	4	3	3	
Термінали користувачів ВМ	6	7	5	6	73
Робоча станція адміністратора віртуалізації	7	8	6	7	85
Робоча станція адміністратора безпеки	7	8	6	7	85
Фізичні сервери з запущеними віртуальними машинами	5	6	4	5	61
Фізичний сервер зберігання даних	3	5	2	4	44
Гіпервізор типу vSphere	5	6	4	6	64
Гостьова ОС	5	6	4	6	64
vSphere Client	5	6	4	6	64
VMware vCenter Server	6	7	5	7	76
Active Directory	6	7	5	7	76
Служби, сервіси VMWare	5	6	4	6	64
Віртуальний міжмережевий екран	5	6	4	6	64
Virtual IPS	5	6	4	6	64
Бази даних	6	7	5	7	76
Файли іміджів та снепшотів віртуальних машин	4	5	3	5	52
Бєкапи даних	4	5	3	5	52
Конфігурація віртуальних машин	4	5	3	5	52

Значення які виставляються експертним шляхом в рядку помножуються на ваговий коефіцієнт пріоритету для стовпчика. Наприклад, для робочої станції адміністратора віртуалізації маємо для конфіденційної інформації оцінку 7 балів, а пріоритет 4 бали. Отже загальна оцінка дорівнює 28 балів. Аналогічним чином отримуємо оцінку для інших стовпчиків і в кінці сумуємо для отримання оцінки кумулятивного впливу вразливостей на активи.

Нижче наведено пояснення балів, призначених кожному активу, і їхньої взаємозалежності для кожної категорії вразливості:

Термінали віртуальної машини:

- вразливість має оцінку 6 балів для загальнодоступної інформації, тому що якщо її зламати, вона потенційно може оприлюднити конфіденційну інформацію;
- оцінка 7 балів для конфіденційної інформації вказує на те, що якщо ці термінали зламано, до конфіденційних даних можуть отримати доступ неавторизовані особи;
- оцінка 5 балів для фінансової інформації свідчить про те, що якщо зловмисники отримають контроль над цими терміналами, вони потенційно можуть отримати доступ або маніпулювати фінансовими даними;
- оцінка 6 балів для безпеки програмного забезпечення означає, що компрометація терміналів віртуальних машин може призвести до порушень безпеки та потенційного використання вразливостей програмного забезпечення.

Станція адміністрування віртуалізації:

- при оцінці загальнодоступної інформації 7 балів компрометація адміністративної станції може призвести до несанкціонованого доступу або розкриття загальнодоступних систем або інформації;
- оцінка 8 балів для конфіденційної інформації вказує на те, що компрометація цього ресурсу може призвести до несанкціонованого доступу до конфіденційних і конфіденційних даних у віртуалізованому середовищі;
- оцінка 6 балів для фінансової інформації свідчить про те, що компрометація адміністративної станції може призвести до несанкціонованого доступу або маніпулювання фінансовими даними;
- оцінка 7 балів для безпеки програмного забезпечення означає, що атака на станцію адміністрування може призвести до використання вразливостей програмного забезпечення в інфраструктурі віртуалізації.

Станція адміністрування безпеки:

- при оцінці загальнодоступної інформації 7 балів компрометація станції адміністрування безпеки може призвести до несанкціонованого доступу або розкриття публічних систем або інформації;
- оцінка 8 балів для конфіденційної інформації вказує на те, що компрометація цього ресурсу може призвести до несанкціонованого доступу до чутливих і конфіденційних даних, пов'язаних із безпекою;
- оцінка 6 балів для фінансової інформації свідчить про те, що компрометація станції адміністрування безпеки може призвести до несанкціонованого доступу або маніпулювання фінансовими даними, пов'язаними з системами безпеки;
- оцінка 7 балів для безпеки програмного забезпечення означає, що атака на станцію адміністрування безпеки може призвести до використання вразливостей програмного забезпечення в системах безпеки.

Фізичні сервери з віртуальними машинами:

- оцінка 5 балів для публічної інформації вказує на те, що компрометація цих серверів потенційно може вплинути на загальнодоступні системи або інформацію, що на них розміщена;
- оцінкою 6 балів за конфіденційну інформацію компрометація цих фізичних серверів може призвести до несанкціонованого доступу до конфіденційних даних у віртуальних машинах, які на них працюють;
- оцінка 4 бали для фінансової інформації свідчить про те, що компрометація цих серверів потенційно може вплинути на фінансові дані, що зберігаються у віртуальних машинах;
- оцінка 5 балів для безпеки програмного забезпечення означає, що компрометація цих серверів може призвести до використання вразливостей програмного забезпечення у віртуальних машинах або інфраструктурі віртуалізації.

Сервер збору фізичних даних:

- оцінкою 3 бали за публічну інформацію компрометація цього сервера може мати слабкий вплив на загальнодоступні системи чи інформацію;
- оцінка 5 балів для конфіденційної інформації вказує на те, що якщо цей сервер зламано, можливий несанкціонований доступ до конфіденційних даних;
- оцінка 2 бали для фінансової інформації означає, що компрометація цього сервера може мати обмежений вплив на фінансові дані;

- оцінка 4 бали для безпеки програмного забезпечення означає, що компрометація цього сервера може призвести до потенційної вразливості безпеки програмного забезпечення в системі збору даних.

Гіпервізор vSphere:

- оцінка 5 балів для загальнодоступної інформації свідчить про те, що компрометація vSphere Hypervisor може потенційно вплинути на загальнодоступні системи або інформацію, розміщену на гіпервізорі;
- оцінкою 6 балів за конфіденційну інформацію компрометація гіпервізора може призвести до несанкціонованого доступу до конфіденційних даних у віртуалізованому середовищі;
- оцінка 4 бали для фінансової інформації вказує на те, що компрометація гіпервізора може мати обмежений вплив на фінансові дані;
- оцінка 6 балів для безпеки програмного забезпечення означає, що компрометація гіпервізора може призвести до використання вразливостей програмного забезпечення в інфраструктурі віртуалізації.

Гостьова ОС:

- оцінка 5 балів для публічної інформації свідчить про те, що компрометація гостьової ОС може потенційно вплинути на загальнодоступні системи або інформацію, розміщену на гостьових машинах;
- оцінкою 6 балів за конфіденційну інформацію компрометація гостьової ОС може призвести до несанкціонованого доступу до конфіденційних даних на гостьових машинах;
- оцінка 4 бали для фінансової інформації вказує на те, що компрометація гостьової ОС може мати обмежений вплив на фінансові дані;
- оцінка 6 балів для безпеки програмного забезпечення означає, що компрометація гостьової ОС може призвести до використання вразливостей програмного забезпечення на гостьових машинах.

Клієнт vSphere:

- оцінка 5 балів для публічної інформації свідчить про те, що компрометація клієнта vSphere може потенційно вплинути на загальнодоступні системи або інформацію, доступ до якої здійснюється через клієнт;
- оцінкою 6 балів за конфіденційну інформацію компрометація клієнта vSphere може призвести до несанкціонованого доступу до конфіденційних даних у віртуалізованому середовищі;

- оцінка 4 бали для фінансової інформації вказує на те, що компрометація клієнта vSphere може мати обмежений вплив на фінансові дані;
- оцінка 6 балів для безпеки програмного забезпечення означає, що компрометація клієнта vSphere може призвести до використання вразливостей програмного забезпечення в інфраструктурі віртуалізації.

Сервер VMware vCenter:

- оцінка 6 балів для загальнодоступної інформації свідчить про те, що компрометація сервера VMware vCenter може потенційно вплинути на загальнодоступні системи або інформацію, доступ до якої здійснюється через сервер;
- оцінкою 7 балів за конфіденційну інформацію компрометація сервера vCenter може призвести до несанкціонованого доступу до конфіденційних даних у віртуалізованому середовищі;
- оцінка 5 балів для фінансової інформації вказує на те, що компрометація сервера vCenter може мати помірний вплив на фінансові дані;
- оцінка 7 балів для безпеки програмного забезпечення означає, що компрометація сервера vCenter може призвести до використання вразливостей програмного забезпечення в інфраструктурі віртуалізації.

Active Directory:

- оцінка 6 балів для публічної інформації свідчить про те, що компрометація Active Directory може потенційно вплинути на загальнодоступні системи або інформацію, пов’язану з автентифікацією користувачів і контролем доступу;
- оцінкою 7 балів за конфіденційну інформацію компрометація Active Directory може призвести до несанкціонованого доступу до чутливих і конфіденційних даних користувача;
- оцінка 5 балів для фінансової інформації вказує на те, що компрометація Active Directory може мати помірний вплив на фінансові дані, пов’язані з обліковими записами та дозволами користувачів;
- оцінка 7 балів для безпеки програмного забезпечення означає, що компрометація Active Directory може призвести до використання вразливостей програмного забезпечення в службі каталогів.

Служби VMWare:

- оцінка 5 балів для публічної інформації свідчить про те, що компрометація служб VMWare може потенційно вплинути на загальнодоступні системи або інформацію, доступ до якої здійснюється через ці служби;
- оцінкою 6 балів за конфіденційну інформацію компрометація служб VMWare може призвести до несанкціонованого доступу до конфіденційних і конфіденційних даних у віртуалізованому середовищі;
- оцінка 4 бали для фінансової інформації вказує на те, що компрометація служб VMWare може мати обмежений вплив на фінансові дані;
- оцінка 6 балів для безпеки програмного забезпечення означає, що компрометація служб VMWare може призвести до використання вразливостей програмного забезпечення в інфраструктурі віртуалізації.

Віртуальний IPS:

- оцінка 5 балів для загальнодоступної інформації свідчить про те, що компрометація Virtual IPS може потенційно вплинути на загальнодоступні системи або інформацію, захищену IPS;
- оцінкою 6 балів за конфіденційну інформацію компрометація Virtual IPS може призвести до несанкціонованого доступу до чутливих і конфіденційних даних у віртуалізованому середовищі;
- оцінка 4 бали для фінансової інформації вказує на те, що компрометація Virtual IPS може мати обмежений вплив на фінансові дані;
- оцінка 6 балів для безпеки програмного забезпечення означає, що компрометація Virtual IPS може призвести до використання вразливостей програмного забезпечення в системі IPS.

База даних:

- оцінка 6 балів для публічної інформації свідчить про те, що компрометація бази даних може потенційно вплинути на публічні системи або інформацію, що зберігається в базі даних;
- оцінкою 7 балів за конфіденційну інформацію компрометація бази даних може призвести до несанкціонованого доступу до конфіденційних та конфіденційних даних, що зберігаються в базі даних;
- оцінка 5 балів для фінансової інформації вказує на те, що компрометація бази даних може мати помірний вплив на фінансові дані, які зберігаються в ній;

- оцінка 7 балів для безпеки програмного забезпечення означає, що компрометація бази даних може призвести до використання вразливостей програмного забезпечення в системі бази даних.

Файли зображень віртуальної машини та знімки:

- оцінка 4 бали для публічної інформації свідчить про те, що компрометація файлів зображень і знімків віртуальної машини може мати слабкий вплив на загальнодоступні системи або інформацію;
- оцінкою 5 балів за конфіденційну інформацію компрометація цих файлів і знімків може призвести до несанкціонованого доступу до конфіденційних і конфіденційних даних у віртуальних машинах;
- оцінка 3 бали для фінансової інформації вказує на те, що компрометація цих файлів і знімків може мати обмежений вплив на фінансові дані;
- оцінка 5 балів для безпеки програмного забезпечення означає, що компрометація цих файлів і знімків може призвести до використання вразливостей програмного забезпечення у віртуальних машинах.

Резервне копіювання даних:

- оцінка 4 бали для публічної інформації свідчить про те, що порушення резервного копіювання даних може мати слабкий вплив на загальнодоступні системи або інформацію, пов’язану з резервним копіюванням і відновленням даних;
- оцінкою 5 балів для конфіденційної інформації компрометація резервної копії даних може призвести до несанкціонованого доступу до конфіденційних і конфіденційних даних резервної копії;
- оцінка 3 бали для фінансової інформації вказує на те, що порушення резервного копіювання даних може мати обмежений вплив на фінансові дані, пов’язані з системами резервного копіювання;
- оцінка 5 балів для безпеки програмного забезпечення означає, що порушення резервного копіювання даних може призвести до використання вразливостей програмного забезпечення в системах резервного копіювання.

Конфігурація віртуальної машини:

- оцінка 4 бали для загальнодоступної інформації свідчить про те, що порушення конфігурації віртуальної машини може мати слабкий вплив на загальнодоступні системи або інформацію, пов’язану з параметрами конфігурації віртуальних машин;
- оцінкою 5 балів за конфіденційну інформацію компрометація конфігурації віртуальної машини може призвести до несанкціонованого доступу до конфіденційних і конфіденційних даних конфігурації;
- оцінка 3 бали для фінансової інформації вказує на те, що порушення конфігурації віртуальної машини може мати обмежений вплив на фінансові дані, пов’язані з налаштуваннями віртуальної машини;
- оцінка 5 балів для безпеки програмного забезпечення означає, що компрометація конфігурації віртуальної машини може призвести до використання вразливостей програмного забезпечення у віртуальних машинах.

Ці бали та взаємозалежності суб’єктивні та можуть змінюватися залежно від конкретного контексту та оцінювання ризиків віртуальної інфраструктури. Важливо налаштувати ці показники на основі унікальних потреб організації, середовища та потенційного впливу вразливостей на активи.

Призначені бали взаємозалежності базувалися на припущенні, що певні вразливості можуть мати більший вплив на певні активи.

Крім того, присвоєні бали також враховують характер активів і вразливості в середовищі віртуальної інфраструктури:

- публічна інформація – категорія активів представляє інформацію, яка призначена для загального доступу. Таким чином, вразливості, що впливають на загальнодоступні інформаційні активи, отримали відносно високі бали, щоб підкреслити потенційний вплив на репутацію організації, дотримання вимог;
- конфіденційна інформація – ця категорія активів містить конфіденційні дані, які потребують захисту. Вразливості, пов’язані з розголошенням, несанкціонованим доступом або компрометацією конфіденційних інформаційних активів, отримали високі бали, щоб підкреслити потенційні правові, фінансові та репутаційні наслідки, пов’язані з такими інцидентами;
- фінансова інформація має вирішальне значення для діяльності організації, вразливості, що впливають на фінансові інформаційні активи,

отримали значні бали, щоб відобразити потенційний вплив на фінансову стабільність;

- безпека програмного забезпечення – враховуючи все більшу залежність від програмних систем і програм у віртуальній інфраструктурі, вразливості, пов’язані з безпекою програмного забезпечення, можуть наражати віртуальне середовище на такі ризики, як несанкціонований доступ, витік даних або збоїв в системі. Таким чином, їм присвоєно відповідні бали, щоб вказати на їхню важливість у підтримці загального стану безпеки віртуальної інфраструктури.

Проаналізувавши матрицю вразливостей можна зробити висновок, що найбільший вплив на віртуальну інфраструктуру має робоча станція адміністратора віртуалізації, робоча станція адміністратора безпеки, VMware vCenter Server і бази даних, тому важливо враховувати при аналізі загроз їхній вплив на віртуальну інфраструктуру.

Для побудови матриці загроз розглянемо статистику тенденцій вразливостей та загроз за роками для продукту VMware [19], яка представлена в таблиці 3.8.

Таблиця 3.8 – Статистика тенденцій вразливостей та загроз за роками для продукту VMware

Рік	DoS	Code Execution	Memory Corruption	Directory Traversal	Bypass something	Gain Information	Gain Privileges
1	2	3	4	5	6	7	8
2000	1						
2001							
2002		1					
2003							2
2004		1					
2005	1	3					2
2006	1	1					2
2007	11	5				2	5
2008	6	4	2	2	1	2	9
2009	11	5	2	2	1	1	5
2010	5	4				4	5
2011	6	2		2	1	3	2

2012	10	7	1	3		4	9

Продовження таблиці 3.8

1	2	3	4	5	6	7	8
2013	7	6	2	1	1		5
2014	8	1		1		3	2
2015	8	4			1	1	2
2016	3	1	1	2		1	3
2017	11	24			3	4	1
2018	3	14		3	7	4	
2019	3	6		1		4	
2020	7	16		4	3	4	
2021	5	13		4	5	1	2
2022	3	18	1	1	8	2	2
2023	2	8		2	5	1	1
Total	112	144	9	28	36	41	59

Проаналізувавши таблицю 3.8, можна зробити висновки, що з кожним роком збільшувалось кількість вразливостей та атак, таких як відмова в обслуговуванні та виконання довільного коду, тому при побудові матриці загроз та матриці контролю слід враховувати ці тенденції.

Для побудови матриці загроз візьмемо наявні вразливості та загрози з таблиці 3.8. Матрицю загроз віртуального середовища надано в таблиці 3.9.

Таблиця 3.9 – Матриця загроз віртуальної інфраструктури

	Загрози							Сукупна значущість загроз
	DoS	Довільне виконання	Пошкодження пам’яті	Обхід каталогу	Обхід елементів безпе	Отримання інформації	Отримання привілеїв	
	1	2	3	4	5	6	7	8
Вразливості/	4	4	1	2	3	3	3	
Термінали користувачів	3	7	5	4	4	4	6	95
Робоча станція адміністратор	6	8	7	5	6	6	8	133
Робоча станція адміністратор	6	9	8	7	8	7	9	154
Фізичні сервери з запущеними віртуальними	5	8	7	6	7	6	8	134
Фізичний сервер	4	7	6	5	6	5	7	114

Продовження таблиці 3.9

1	2	3	4	5	6	7	8	9
Гіпервізор типу	4	8	7	6	7	6	8	130
Гостьова ОС	4	9	8	6	8	7	9	144
vSphere	3	7	6	4	5	4	7	102
VMware vCenter	4	9	8	7	8	7	9	149
Active	3	8	7	6	7	6	8	126
Служби, сервіси	3	7	6	5	6	5	7	110
Віртуальний міжмережевий екран	2	6	5	4	5	4	6	90
Virtual IPS	4	8	7	6	7	6	8	130
Бази даних	7	9	8	6	7	8	9	156
Файли іміджів та снепшотів	2	7	6	3	4	6	7	99
Бєкапи	2	6	5	3	4	6	7	94
Конфігурація	3	6	5	4	5	5	7	100

Показники вразливості ранжуються на основі пріоритету загроз. Оцінки вказують на значимість і центральність загроз. Розглянемо більш детально оцінки наведені в таблиці 3.9:

Термінали віртуальних машин:

- оцінка 3 бали: успішна атака типу «відмова в обслуговуванні» (DoS) може тимчасово зробити термінали віртуальної машини недоступними, це вплине на продуктивність користувача, але вона має обмежений вплив на інші активи у віртуальній інфраструктурі;
- оцінка 7 балів виконання довільного коду: можливий запуск довільного коду у терміналах віртуальної машини, що призведе до неавторизованого доступу або компрометації віртуальних машин. Можливий значний вплив на безпеку та цілісність всієї віртуальної інфраструктури;
- оцінка 5 балів пошкодження пам'яті: можуть призвести до збоїв, нестабільності або неочікуваної поведінки терміналів віртуальної машини, впливаючи на їхню продуктивність і надійність. Основний вплив на порушення роботи терміналів і впливу на стабільність віртуальної інфраструктури;
- оцінка 4 бали обхід каталогу: може дозволити зловмиснику вийти за межі передбаченої структури каталогів і отримати доступ до несанкціонованих файлів або каталогів у віртуальній інфраструктурі. Це ставить під загрозу безпеку віртуальної інфраструктури;
- оцінка 4 бали обхід елементів безпеки: може дозволити зловмиснику обійти елементи керування безпекою або механізми автентифікації, потенційно отримуючи неавторизований доступ до віртуальних машин або конфіденційних даних. Ця атака може послабити загальну безпеку віртуальної інфраструктури та збільшити ризик несанкціонованого доступу;
- оцінка 4 бали отримання інформації: можливе розкриття конфіденційної інформації про віртуальну інфраструктуру, таку як деталі конфігурації або облікові дані користувача, що може допомогти зловмисникам у подальшій експлуатації системи;
- оцінка 6 балів отримання привілеїв: можуть дозволити зловмиснику підвищити свої привілеї у віртуальному середовищі, надавши йому доступ до конфіденційних ресурсів або порушивши цілісність віртуальних машин. Це може призвести до значного компрометування та несанкціонованого контролю над віртуальною інфраструктурою.

Робоча станція адміністратора віртуалізації:

- оцінка 6 балів: DoS атака, націлена на станцію адміністрування віртуалізації, може порушити доступність адміністративних функцій, потенційно вплинувши на управління та контроль віртуальної інфраструктури. Основний вплив на загальне управління та адміністрування віртуальної інфраструктури, впливаючи на інші активи та функції;
- оцінка 8 балів виконання довільного коду: виконання довільного коду може призвести до несанкціонованого доступу, контролю або маніпулювання віртуальною інфраструктурою;
- оцінка 7 балів пошкодження пам'яті: може призвести до збоїв, нестабільності або неочікуваної поведінки в адміністративних функціях, впливаючи на контроль і керування віртуальною інфраструктурою. Основний вплив на адміністративні можливості, що може поставити під загрозу стабільність віртуальної інфраструктури;
- оцінка 5 балів обхід каталогу: можливе отримання несанкціонованого доступу до конфіденційних файлів або каталогів у віртуальній інфраструктурі, що потенційно може призвести до витоку даних або несанкціонованих змін. Це ставить під загрозу конфіденційність і цілісність адміністративних ресурсів і потенційно вплинути на безпеку віртуальної інфраструктури;
- оцінка 6 балів обхід елементів безпеки: може дозволити зловмисникам обійти елементи керування безпекою або механізми автентифікації, надавши їм несанкціонований доступ до адміністративних функцій і поставивши під загрозу керування віртуальною інфраструктурою. Це вплине на безпеку адміністративних функцій і відкриє шляхи для несанкціонованого доступу або маніпуляцій;
- оцінка 6 балів отримання інформації: розкриття конфіденційної інформації про адміністрування віртуальної інфраструктури, таку як облікові дані або деталі конфігурації, дозволяючи зловмисникам збирати знання для подальшого використання;
- оцінка 8 балів отримання привілеїв: надає несанкціонований контроль над адміністративними функціями та можливість скомпрометувати віртуальну інфраструктуру.

Робоча станція адміністратора віртуалізації:

- оцінка 6 балів: DoS атака може порушити доступність пов’язаних із безпекою функцій, потенційно вплинувши на можливості моніторингу;

- оцінка 9 балів виконання довільного коду: може дозволити зловмисникам виконувати довільний код із привілеями адміністрування безпеки, що потенційно ставить під загрозу цілісність і ефективність наявних елементів керування безпекою. Це може призвести до несанкціонованого доступу, маніпуляцій або обходу механізмів безпеки, суттєво впливаючи на стан безпеки віртуальної інфраструктури;
- оцінка 8 балів пошкодження пам'яті: призводить до збоїв, нестабільності або неочікуваної поведінки у функціях адміністрування безпеки, ставлячи під загрозу надійність і ефективність елементів керування безпекою;
- оцінка 7 балів обхід каталогу: отримання несанкціонованого доступу до конфіденційних файлів або каталогів, пов’язаних із безпекою, що потенційно може призвести до розкриття інформації або несанкціонованих змін конфігурацій безпеки;
- оцінка 8 балів обхід елементів безпеки: дозволить зловмисникам обійти елементи керування безпекою, механізми автентифікації або системи моніторингу, потенційно отримуючи несанкціонований доступ до функцій адміністрування безпеки та скомпрометувавши безпеку віртуальної інфраструктури;
- оцінка 7 балів отримання інформації: розкриття конфіденційної інформації, пов’язаної з безпекою, наприклад, конфігурація безпеки, дані моніторингу або облікові дані користувача, дозволяючи зловмисникам збирати знання для подальшого використання або ухилення від заходів безпеки;
- оцінка 9 балів отримання привілеїв: підвищення привілеїв в межах функцій адміністрування безпеки, надасть несанкціонований контроль над конфігураціями безпеки, доступ до систем моніторингу або контроль доступу.

Фізичні сервери з запущеними віртуальними машинами:

- оцінка 5 балів: DoS атака на фізичні сервери, на яких запущені віртуальні машини, може зробити віртуальні машини недоступними, що вплине на доступність і продуктивність віртуальної інфраструктури;
- оцінка 8 балів виконання довільного коду: може дозволити зловмисникам виконувати довільний код у віртуальних машинах, потенційно призводячи до несанкціонованого доступу або компрометації віртуальної інфраструктури;

- оцінка 7 балів пошкодження пам'яті: може призвести до збоїв, нестабільності або неочікуваної поведінки у віртуальних машинах, впливаючи на їхню продуктивність, надійність і потенційно підриваючи стабільність віртуальної інфраструктури;
- оцінка 6 балів обхід каталогу: проходження каталогу дозволить зловмисникам виходити за межі призначеної структури каталогів у віртуальних машинах, потенційно отримуючи несанкціонований доступ до конфіденційних файлів або ставлячи під загрозу безпеку віртуальної інфраструктури;
- оцінка 7 балів обхід елементів безпеки: може послабити загальну безпеку віртуальних машин і збільшити ризик несанкціонованого доступу або компрометації у віртуальній інфраструктурі;
- оцінка 6 балів отримання інформації: розкриття інформації ставить під загрозу конфіденційність і цілісність даних у віртуальних машинах, потенційно впливаючи на загальну безпеку віртуальної інфраструктури;
- оцінка 8 балів отримання привілеїв: підвищення привілеїв у віртуальних машинах, потенційно надасть неавторизований доступ до конфіденційних ресурсів, порушуючи цілісність віртуальних машин.

Фізичний сервер зберігання даних:

- оцінка 6 балів: DoS атака, може порушити зберігання і обробку даних у віртуальній інфраструктурі., тим самим впливаючи на інші активи та функції, які покладаються на збережені дані;
- оцінка 7 балів виконання довільного коду: виконання довільного коду вплине на доступ до збережених даних, що потенційно може порушити цілісність і конфіденційність даних;
- оцінка 5 балів пошкодження пам'яті: може призвести до збоїв, нестабільності або несподіваної поведінки в процесах збереження даних, що вплине на надійність і точність зібраних даних.
- оцінка 4 бали обхід каталогу: дозволить отримати доступу до файлів або каталогів, що потенційно може призвести до розкриття даних або несанкціонованих змін;
- оцінка 4 бали обхід елементів безпеки: може дозволити зловмисникам обійти елементи керування безпекою або механізми автентифікації, потенційно отримуючи неавторизований доступ до зібраних даних або маніпулюючи процесами збереження даних;

- оцінка 5 балів отримання інформації: може поставити під загрозу конфіденційність збережених даних, впливаючи на безпеку даних віртуальної інфраструктури;
- оцінка 6 балів отримання привілеїв: підвищення привілеїв в процесах збору даних, потенційно надасть несанкціонований контроль над збереженими даними, тим самим порушуючи цілісність даних віртуальної інфраструктури.

Гіпервізор vSphere:

- оцінка 6 балів: DoS атака, може порушити доступність ресурсів віртуальної машини, потенційно вплинувши на доступність і функціональність віртуальної інфраструктури;
- оцінка 9 балів виконання довільного коду: виконання довільного коду у гіпервізорі, потенційно вплине на безпеку та цілісність віртуальних машин і всієї віртуальної інфраструктури;
- оцінка 8 балів пошкодження пам'яті: може призвести до збоїв, нестабільності або неочікуваної поведінки на рівні віртуалізації, що погіршить стабільність, надійність і безпеку віртуальної інфраструктури;
- оцінка 7 балів обхід каталогу: може призвести до отримання несанкціонованого доступу до критичних файлів гіпервізора, що ставить під загрозу безпеку віртуальної інфраструктури;
- оцінка 8 балів обхід елементів безпеки: може дозволити зловмисникам обійти елементи керування безпекою або механізми автентифікації, потенційно отримуючи неавторизований доступ до віртуальних машин або скомпрометувавши безпеку віртуальної інфраструктури;
- оцінка 7 балів отримання інформації: розкриття інформацію про конфігурацію гіпервізора, стани віртуальної машини або налаштування віртуальної мережі, потенційно допоможе зловмисникам збирати знання для подальшого використання або компрометації безпеки віртуальної інфраструктури;
- оцінка 9 балів отримання привілеїв: ескалація привілеїв дозволить отримати неавторизований контроль над віртуальними машинами, конфігураціями гіпервізора або налаштуваннями віртуальної мережі.

Гостьова ОС:

- оцінка 6 балів: DoS атака, може порушити доступність служб і програм, що працюють на віртуальній машині, потенційно вплинувши на функціональність і доступність віртуальної інфраструктури;

- оцінка 9 балів виконання довільного коду: може дозволити зловмисникам виконувати довільний код в гостьовій ОС тим самим впливаючи на цілісність гостьової ОС, а також віртуальної інфраструктури;
- оцінка 8 балів пошкодження пам'яті: пошкодження пам’яті в гостьовій ОС можуть призвести до збоїв, нестабільності або неочікуваної поведінки у віртуальній машині, ставлячи під загрозу надійність і безпеку гостьової ОС та віртуальної інфраструктури;
- оцінка 7 балів обхід каталогу: проходження каталогу в гостьовій ОС дозволить зловмисникам виходити за межі передбаченої структури каталогів у віртуальній машині, потенційно отримуючи неавторизований доступ до конфіденційних файлів або ставлячи під загрозу конфіденційність, цілісність і доступність ресурсів у віртуальній машині, впливаючи на загальну безпеку віртуальної інфраструктури;
- оцінка 8 балів обхід елементів безпеки: дозволяє обійти елементи керування безпекою, механізми автентифікації або засоби захисту на рівні програми у віртуальній машині, потенційно отримуючи несанкціонований доступ або підриваючи безпеку гостьової ОС;
- оцінка 7 балів отримання інформації: розкриття інформації в гостьовій ОС можуть розкрити конфіденційну інформацію у віртуальній машині, що потенційно призведе до витоку даних, несанкціонованого доступу або розкриття цінної інформації;
- оцінка 9 балів отримання інформації: підвищення привілеїв у віртуальній машині, потенційно надасть неавторизований контроль над гостьовою ОС або ресурсами віртуальної машини.

vSphere Client:

- оцінка 4 бали DoS: атака може порушити доступність і зручність використання клієнту, потенційно вплинувши на керування та адміністрування віртуальної інфраструктури;
- оцінка 7 балів виконання довільного коду: призводить до порушення конфіденційності, цілісності і доступності віртуальної інфраструктури;
- оцінка 6 балів пошкодження пам'яті: може вплинути на керування та адміністрування віртуальної інфраструктури;
- оцінка 4 бали обхід каталогу: наприклад, зловмисник визначає цільову інсталяцію vSphere Client, потім запускає клієнт vSphere і встановлює з’єднання з цільовим сервером vCenter або хостом ESXi. Використовуючи функції керування файлами клієнта vSphere, зловмисник намагається

маніпулювати шляхами файлів, щоб вийти за межі передбаченої структури каталогів. У разі успіху зловмисник може отримати доступ до конфіденційних файлів, таких як файли конфігурації, журнали або навіть облікові дані, які не повинні надаватися неавторизованим користувачам;

- оцінка 5 балів обхід елементів безпеки: наприклад, зловмисник визначає цільову інсталяцію vSphere Client, потім запускає клієнт і встановлює з'єднання з цільовим сервером vCenter або хостом ESXi. Використовуючи слабкі місця у механізмах автентифікації, обходить автентифікацію і видає себе за користувачів.
- оцінка 6 балів отримання інформації: розкриття інформації через проходження клієнту для подальшого використання або компрометації безпеки інтерфейсу керування;
- оцінка 7 балів отримання привілеїв: підвищення привілеїв неавторизованого користувача дозволить отримати доступ до функцій керування, конфігурацій або поставивши під загрозу безпеку віртуальної інфраструктури.

VMware vCenter:

- оцінка 7 балів: DoS атака, може порушити доступність функцій управління та контролю, потенційно вплинувши на загальне управління та адміністрування віртуальної інфраструктури;
- оцінка 9 балів виконання довільного коду: порушить цілісність і конфіденційність даних керування та віртуальної інфраструктури;
- оцінка 8 балів пошкодження пам'яті: може порушити роботу критично важливих служб керування, до нестабільності або неочікуваної поведінки на сервері, що ставить під загрозу надійність і безпеку функцій управління та контролю;
- оцінка 6 балів обхід каталогу: проходження каталогу на сервері VMware vCenter можуть дозволити зловмисникам вийти за межі передбаченої структури каталогів;
- оцінка 7 балів обхід елементів безпеки: може дозволити зловмисникам обійти елементи керування безпекою або механізми автентифікації, потенційно отримуючи неавторизований доступ до функцій керування, конфігурацій або скомпрометувавши безпеку віртуальної інфраструктури;
- оцінка 8 балів отримання інформації: розкриття інформації в сервері VMware vCenter Server можуть розкрити конфіденційну інформацію про конфігурації керування, стани віртуальної машини або облікові дані

адміністратора, потенційно допомагаючи зловмисникам збирати знання для подальшого використання або скомпрометувати безпеку віртуальної інфраструктури;

- оцінка 9 балів отримання привілеїв ескалації привілеїв у сервері VMware vCenter Server можуть дозволити зловмисникам підвищити свої привілеї на сервері, потенційно отримуючи неавторизований контроль над функціями керування, конфігураціями або підриваючи безпеку віртуальної інфраструктури.

Active Directory:

- оцінка 7 балів: DoS атака, спрямована на інфраструктуру Active Directory, може порушити доступність служб каталогів, потенційно вплинувши на автентифікацію користувача, авторизацію та загальний контроль доступу у віртуальній інфраструктурі;
- оцінка 9 балів виконання довільного коду: виконання коду в Active Directory можуть дозволити зловмисникам виконувати довільний код в інфраструктурі, потенційно порушуючи цілісність служб каталогів і безпеку віртуальної інфраструктури;
- оцінка 8 балів пошкодження пам'яті: може призвести до збоїв, нестабільності або неочікуваної поведінки в інфраструктурі, ставлячи під загрозу надійність і безпеку служб каталогів і контролю доступу;
- оцінка 6 балів обхід каталогу: може дозволити зловмисникам вийти за межі передбаченої структури каталогу, потенційно отримуючи неавторизований доступ до конфіденційної інформації або скомпрометувавши безпеку засобів контролю доступу;
- оцінка 7 балів обхід елементів безпеки: може дозволити зловмисникам обійти елементи керування безпекою або механізми автентифікації, потенційно отримуючи неавторизований доступ до служб каталогів, облікових записів користувачів або скомпрометувавши засоби керування доступом у віртуальній інфраструктурі;
- оцінка 8 балів отримання інформації: розкриття конфіденційної інформації про облікові записи користувачів, членство в групах або облікові дані адміністратора, потенційно допомагаючи зловмисникам збирати знання для подальшого використання або скомпрометувати безпеку віртуальної інфраструктури;
- оцінка 9 балів отримання привілеїв: може дозволити зловмисникам підвищити свої привілеї в інфраструктурі, потенційно отримуючи

неавторизований контроль над обліковими записами користувачів, елементами керування доступом або ставлячи під загрозу безпеку віртуальної інфраструктури.

Служби VMware:

- оцінка 6 балів: DoS атака, націлена на служби VMware, може порушити доступність критично важливих служб, необхідних для роботи та керування віртуальною інфраструктурою, потенційно вплинувши на загальну функціональність і доступність;
- оцінка 8 балів виконання довільного коду: може дозволити зловмисникам виконувати довільний код у службах, потенційно порушуючи безпеку та цілісність віртуальної інфраструктури та пов’язаних служб;
- оцінка 7 балів пошкодження пам'яті: може призвести до збоїв, нестабільності або неочікуваної поведінки в службах, що ставить під загрозу надійність і безпеку віртуальної інфраструктури;
- оцінка 5 балів обхід каталогу: проходження каталогу в службах VMware можуть дозволити зловмисникам вийти за межі призначеної структури каталогів у службах, потенційно отримуючи неавторизований доступ до конфіденційних файлів або ставлячи під загрозу безпеку служб;
- оцінка 6 балів обхід елементів безпеки: може дозволити зловмисникам обійти елементи керування безпекою або механізми автентифікації в службах, потенційно отримуючи неавторизований доступ або ставлячи під загрозу безпеку віртуальної інфраструктури;
- оцінка 8 балів обхід елементів безпеки: можна за допомогою служб VMware розкрити конфіденційну інформацію;
- оцінка 8 балів отримання привілеїв: зловмисники можуть підвищити привілеї в службах, потенційно отримуючи неавторизований контроль над критичними функціями, конфігураціями або ставлячи під загрозу безпеку віртуальної інфраструктури.

База даних:

- оцінка 7 балів: DoS атака, спрямована на базу даних, може порушити її доступність, потенційно вплинувши на критичні служби та програми;
- оцінка 9 балів виконання довільного коду: зловмисники можуть виконати довільний код у базі даних, потенційно порушуючи конфіденційність, цілісність і доступність даних, що зберігаються у віртуальній інфраструктурі;

- оцінка 8 балів пошкодження пам'яті: може призвести до збоїв, нестабільності або неочікуваної поведінки в базі даних, що ставить під загрозу надійність і безпеку зберігання та отримання даних у віртуальній інфраструктурі;
- оцінка 6 балів обхід каталогу: проходження каталогу в базі даних можуть дозволити зловмисникам виходити за межі призначеної структури каталогів у базі даних, потенційно отримуючи неавторизований доступ до конфіденційних даних або ставлячи під загрозу безпеку зберігання та вилучення даних;
- оцінка 7 балів обхід елементів безпеки: може дозволити зловмисникам обійти елементи керування безпекою або механізми автентифікації, потенційно отримуючи неавторизований доступ до даних або ставлячи під загрозу безпеку зберігання та отримання даних у віртуальній інфраструктурі;
- оцінка 8 балів отримання інформації: в базі даних можуть розкрити конфіденційну інформацію, що зберігається в базі даних, потенційно допомагаючи зловмисникам збирати знання для подальшого використання або скомпрометувати безпеку даних у віртуальній інфраструктурі;
- оцінка 9 балів отримання привілеїв: ескалації привілеїв у базі даних можуть дозволити зловмисникам підвищити свої привілеї в базі даних, потенційно отримуючи несанкціонований контроль над даними, функціями керування даними або ставлячи під загрозу безпеку віртуальної інфраструктури.

Конфігурація віртуальної машини:

- оцінка 3 бали: DoS атака, націлена на конфігурації віртуальних машин, може порушити доступність і функціональність уражених віртуальних машин, потенційно впливаючи на служби та програми, що працюють у віртуальній інфраструктурі;
- оцінка 6 балів виконання довільного коду виконання коду в конфігураціях віртуальних машин можуть дозволити зловмисникам виконувати довільний код у віртуальних машинах, потенційно порушуючи їхню цілісність, безпеку та загальну функціональність віртуальної інфраструктури;
- оцінка 7 балів отримання привілеїв: ескалації привілеїв у конфігураціях віртуальних машин можуть дозволити зловмисникам підвищити свої привілеї у віртуальних машинах, потенційно отримуючи

неавторизований контроль над ресурсами, конфігураціями або ставлячи під загрозу безпеку віртуальної інфраструктури.

Ці бали присвоєно на основі потенційного впливу, який кожна загроза може мати на конкретні вразливості. Наведені приклади підкреслюють потенційні наслідки кожної загрози, якщо її успішно використати проти відповідної вразливості. Взаємозалежності представляють вплив певної загрози на певну вразливість. Ці бали є суб'єктивними та можуть змінюватися залежно від конкретного контексту віртуальної інфраструктури.

Проаналізувавши потенційний вплив кожної загрози на вразливості віртуальної інфраструктури необхідно підібрати засоби контролю безпеки і додати їх в матрицю контролю, вони можуть змінюватись в залежності необхідності захисту того чи іншої вразливості віртуальної інфраструктури.

Матрицю контролю загроз віртуальної інфраструктури продемонстровано в таблиці 3.10.

Таблиця 3.10 – Матриця контролю загроз віртуальної інфраструктури

	DoS	Довільне виконання коду	Пошкодження пам’яті	Обхід каталогу	Обхід елементів безпеки	Отримання інформації	Отримання привілеїв	Сукупна значущість ко
Засоби управління,	4	4	1	2	3	3	3	
Брандмауер	6	7	5	4	3	6	8	116
Хешування	3	6	4	2	1	5	7	83
Універсальна платформа для забезпечення безпеки та захисту	4	7	6	3	2	6	8	104
Антивірусне програмне забезпечення	5	8	7	5	4	7	9	129
Політика безпеки	3	5	4	2	1	4	6	73
Навчання	2	4	3	1	1	3	5	56

Проаналізуємо дані таблиці 3.10.

DoS (відмова в обслуговуванні):

- брандмауер оцінка 6 балів. Брандмауер може допомогти блокуючи зловмисний трафік і впроваджуючи політики контролю доступу. Він забезпечує помірний вплив на зниження ризику DoS-атак;
- хешування паролів оцінка 3 бали. Хешування паролів може не протистояти атакам DoS, воно сприяє загальній безпеці, захищаючи облікові дані користувача та запобігаючи неавторизованому доступу. Його вплив на пом'якшення атак DoS є слабким;
- універсальна платформа безпеки та захисту кінцевих точок оцінка 4 бали. Цей елемент керування зосереджений на безпеці та захисті кінцевих точок, що може допомогти виявити та запобігти DoS-атакам на рівні кінцевих точок. Він має помірний вплив на пом’якшення загроз DoS;
- антивірусне програмне забезпечення оцінка 5 балів. Антивірусне програмне забезпечення може виявляти та блокувати зловмисне програмне забезпечення або несанкціоновані дії, включаючи деякі форми DoS-атак. Воно забезпечує помірний вплив на зниження ризику DoS-атак;
- політика безпеки оцінка 3 бали. Чітко визначена політика безпеки може включати заходи щодо запобігання та реагування на атаки DoS, сприяючи загальній безпеці. Її вплив на пом'якшення атак DoS є помірним.
- навчання персоналу оцінка 2 бали. Навчання співробітників найкращим практикам безпеки та обізнаності може допомогти їм виявляти й повідомляти про потенційні DoS-атаки, покращуючи реагування на інциденти, але вплив на пом'якшення загроз DoS є слабким.

Виконання коду:

- брандмауер оцінка 7 балів. Брандмауер може допомогти блокувати спроби неавторизованого доступу та спроби виконання зловмисного коду, забезпечуючи сильний вплив на зниження ризику атак виконання коду;
- хешування пароля оцінка 6 балів. Хешування пароля відіграє вирішальну роль у захисті облікових даних користувача та запобіганні несанкціонованому виконанню коду;
- універсальна платформа безпеки та захисту кінцевих точок оцінка 7 балів. Цей елемент керування зосереджений на безпеці та захисті кінцевих точок, включаючи виявлення та блокування спроб виконання шкідливого коду;

- антивірусне програмне забезпечення оцінка 8 балів. Антивірусне програмне забезпечення може виявляти та блокувати відомі зловмисне програмне забезпечення або зловмисний код, забезпечуючи сильний вплив на зниження ризику атак виконання коду;
- політика безпеки оцінка 5 балів. Чітко визначена політика безпеки може включати заходи для запобігання атакам на виконання коду, наприклад методи безпечного кодування та вказівки щодо перегляду коду;
- навчання персоналу 4 бали. Навчання співробітників методам безпечного кодування та обізнаності можуть допомогти запобігти вразливостям у виконанні коду та покращити реагування на інциденти.

Пошкодження пам'яті:

- брандмауер оцінка 5 балів. Брандмауер може допомогти блокувати спроби несанкціонованого доступу та певні методи пошкодження пам’яті, надаючи помірний вплив на зниження ризику атак з пошкодженням пам’яті;
- хешування паролів 4 бали. Хешування паролів не може безпосередньо усунути вразливість пам’яті, воно сприяє загальній безпеці, захищаючи облікові дані користувача та запобігаючи неавторизованому доступу;
- універсальна платформа безпеки та захисту кінцевих точок оцінка 6 балів. Цей елемент керування зосереджений на безпеці та захисті кінцевих точок, зокрема виявленні та запобіганні атакам пошкодження пам’яті;
- антивірусне програмне забезпечення оцінка 7 балів. Антивірусне програмне забезпечення може виявляти та блокувати відомі зловмисне програмне забезпечення або зловмисну діяльність, зокрема деякі методи пошкодження пам’яті;
- політика безпеки оцінка 4 бали. Чітко визначена політика безпеки може включати заходи та вказівки для запобігання вразливості пам’яті;
- навчання персоналу оцінка 3 бали. Навчання співробітників методам безпечного кодування та обізнаності може допомогти запобігти вразливості пам’яті та покращити реагування на інциденти.

Обхід каталогу:

- брандмауер оцінка 4 бали. Брандмауер може допомогти запобігти спробам несанкціонованого доступу та блокувати атаки проходження каталогу, надаючи помірний вплив на зниження ризику загроз проходження каталогу;

- хешування паролів оцінка 2 бали. Хешування паролів безпосередньо не вирішує вразливості проходження каталогу. Його вплив на пом’якшення загроз проходження каталогу є слабким;
- універсальна платформа безпеки та захисту кінцевих точок оцінка 3 бали. Цей елемент керування зосереджений на безпеці та захисті кінцевих точок, що може сприяти виявленню та запобіганню атакам проходження каталогу;
- антивірусне програмне забезпечення 5 балів. Антивірусне програмне забезпечення може виявляти та блокувати певне зловмисне програмне забезпечення або шкідливі дії, пов’язані з атаками проходження каталогу. Він забезпечує помірний вплив на зниження ризику загроз проходження каталогу;
- політика безпеки оцінка 2 бали. Чітко визначена політика безпеки може включати заходи для запобігання вразливості проходження каталогу, такі як перевірка введених даних і контроль доступу;
- навчання персоналу оцінка 1 бал. Навчання співробітників методам безпечного кодування та обізнаності можуть допомогти запобігти вразливостям проходження каталогу та покращити реагування на інциденти.

Обхід елементів безпеки:

- брандмауер оцінка 3 бали. Брандмауер може допомогти блокувати спроби несанкціонованого доступу та певні методи обходу, надаючи слабкий або помірний вплив на зниження ризику загроз обходу;
- хешування паролів оцінка 1 бал. Хешування паролів має мінімальне пом'якшення загроз обходу елементів безпеки;
- універсальна платформа безпеки та захисту кінцевих точок оцінка 2 бали. Вплив на пом'якшення загроз обходу є мінімальним;
- антивірусне програмне забезпечення оцінка 4 бали. Антивірусне програмне забезпечення може виявляти та блокувати певне зловмисне програмне забезпечення або шкідливі дії, пов’язані зі спробами обходу елементів безпеки;
- політика безпеки оцінка 1 бал. Чітко визначена політика безпеки може включати заходи для запобігання обходу елементів безпеки;
- навчання персоналу: оцінка 1 бал. Навчання співробітників має слабкий вплив на пом'якшення загроз обходу елементів безпеки.

Отримання інформації:

- брандмауер оцінка 6 балів. Брандмауер може допомогти блокувати спроби несанкціонованого доступу та певні методи розкриття інформації;
- хешування пароля 5 балів. Хешування пароля сприяє загальній безпеці, захищаючи облікові дані користувача та запобігає неавторизованому доступу;
- універсальна платформа безпеки та захисту кінцевих точок оцінка 6 балів. Елемент керування зосереджений на безпеці та захисті кінцевих точок, включаючи виявлення та запобігання спробам розкриття інформації;
- антивірусне програмне забезпечення оцінка 7 балів. Антивірусне програмне забезпечення може виявляти та блокувати певне шкідливе програмне забезпечення або шкідливі дії, пов’язані зі спробами розкриття інформації;
- політика безпеки оцінка 4 бали. Політика безпеки може включати заходи для запобігання вразливості розкриття інформації, такі як класифікація даних і контроль доступу;
- навчання персоналу 3 бали. Навчання співробітників практикам безпеки та обізнаності може допомогти запобігти розголошенню інформації та покращити реагування на інциденти

Отримання привілеїв:

- брандмауер оцінка 7 балів. Брандмауер може допомогти блокувати спроби несанкціонованого доступу та певні методи підвищення привілеїв;
- хешування паролів 6 балів. Хешування паролів безпосередньо не усуне вразливості підвищення привілеїв, але воно сприяє загальній безпеці, захищаючи облікові дані користувача та запобігаючи неавторизованому доступу;
- універсальна платформа безпеки та захисту кінцевих точок оцінка 7 балів. Цей елемент керування зосереджений на безпеці та захисті кінцевих точок, зокрема виявленні та запобіганні спробам підвищення привілеїв;
- антивірусне програмне забезпечення оцінка 8 балів. Антивірусне програмне забезпечення може виявляти та блокувати певне зловмисне програмне забезпечення або шкідливі дії, пов’язані зі спробами підвищення привілеїв;
- політика безпеки оцінка 5 балів. Політика безпеки може включати заходи для запобігання вразливості підвищення привілеїв;
- навчання персоналу оцінка 4 бали. Навчання співробітників може допомогти запобігти вразливості підвищення привілеїв і покращити

реагування на інциденти. Його вплив на пом’якшення загроз ескалації привілеїв є помірним.

Ці бали представляють рівень впливу кожного елемента керування на пом’якшення конкретних загроз. Чим вищий бал, тим сильніший вплив або ефективність контролю в зниженні ризику, пов’язаного із загрозою.

Взаємозалежності між засобами контролю стосуються того, як ефективність одного засобу контролю може залежати від наявності або впровадження іншого засобу контролю. Наприклад, ефективність керування брандмауером може залежати від реалізації елемента керування політикою безпеки, який визначає правила та конфігурацію брандмауера. Подібним чином ефективність контролю хешування паролів може залежати від впровадження навчання персоналу, оскільки навчені працівники, будуть створювати надійні паролі.

Важливо зазначити, що конкретні взаємозалежності можуть відрізнятися залежно від середовища організації, стану безпеки та інших факторів. Матриця загроз забезпечує структуру для оцінки взаємозалежностей і числових балів засобів контролю на основі їхньої ефективності в пом’якшенні виявлених загроз.

Проаналізувавши дані матриці контролю, можна зробити висновок, що можна застосувати більш доцільні засоби управління безпекою для віртуальної інфраструктури. Тому побудуємо нову матрицю контролю зі зміненими засобами управління безпекою. Матрицю контролю загроз віртуальної інфраструктури зі зміненими засобами управління безпекою продемонстровано в таблиці 3.11.

Таблиця 3.11 – Матриця контролю загроз віртуальної інфраструктури зі зміненими засобами управління безпекою

	DoS	Довільне виконання коду	Пошкодження пам’яті	Обхід каталогу	Обхід елементів безпеки	Отримання інформації	Отримання привілеїв	Разом
Засоби управління,	4	4	1	2	3	3	3	
Пісочниця мережевого	6	7	6	5	4	7	8	12
Запобігання виконанню	8	9	8	6	5	9	9	15
Універсальна платформа для забезпечення безпеки та захисту	4	7	6	3	2	6	8	104
Шифрування	4	7	6	3	6	8	6	1
Запобігання втраті даних	4	6	5	4	4	8	7	11
Контроль доступу на	3	6	5	4	4	6	7	10

Проаналізуємо оцінки таблиці 3.11.

Пісочниця мережевого трафіку:

- DoS: ізольоване програмне середовище мережевого трафіку має помірний вплив (оцінка 6 балів) на пом’якшення загроз DoS. Воно може аналізувати моделі мережевого трафіку та виявляти та блокувати підозрілий трафік, який може свідчити про атаку DoS. Наприклад, він може ідентифікувати та пом’якшувати об’ємні атаки або надмірні запити на з’єднання;
- виконання довільного коду: ізольоване програмне середовище мережевого трафіку має сильний вплив (оцінка 8 балів) на пом’якшення загроз виконання коду. Перевіряючи мережевий трафік, він може виявляти та блокувати шкідливі корисні навантаження або експлоїти, які намагаються виконати довільний код у вразливій системі;
- пошкодження пам’яті: ізольоване програмне середовище мережевого трафіку має помірний вплив (оцінка 6 балів) на пом’якшення загроз пошкодження пам’яті. Воно може ідентифікувати та блокувати мережеві атаки, спрямовані на вразливість пам’яті, наприклад переповнення буфера;
- отримання інформації: може виявити та запобігти спробам викрадання даних або несанкціонованому розвідуванню мережі.

Ізольоване програмне середовище мережевого трафіку відіграє вирішальну роль у виявленні та пом’якшенні різноманітних загроз, які залежать від мережевих комунікацій. Воно підтримує інші елементи керування, ідентифікуючи шкідливий мережевий трафік і блокуючи потенційні вектори атак.

Запобігання виконанню даних:

- DoS: може допомогти запобігти певним типам атак DoS, які використовують вразливості пам’яті.
- виконання довільного коду: блокується виконання шкідливого коду, впровадженого в пам’ять, запобігаючи успішному виконанню довільного коду;
- пошкодження пам’яті: запобігає виконанню зловмисних корисних навантажень, націлених на вразливість пам’яті, таких як переповнення буфера;
- отримання інформації: блокуючи експлойти виконання коду, це допомагає запобігти несанкціонованому доступу до конфіденційної інформації або викраденню даних за допомогою шкідливого коду.

Запобігання виконанню даних – це фундаментальний елемент керування, який допомагає захистити від багатьох загроз, які залежать від експлойтів виконання коду або пошкодження пам’яті. Він утворює критичний рівень захисту разом з іншими засобами керування.

Шифрування:

- DoS: шифрування має помірний вплив (оцінка 4 бали) на пом’якшення загроз DoS. Шифрування не може безпосередньо запобігти атакам DoS, воно може допомогти захистити критично важливі ресурси чи втручання під час атаки;
- виконання довільного коду: шифрування має сильний вплив (оцінка 7 балів) на пом’якшення загроз виконання коду. Це може допомогти захистити конфіденційні дані під час передачі чи зберігання, зменшуючи потенційний вплив успішного виконання коду;
- пошкодження пам’яті: завдяки шифруванню даних, що зберігаються в пам’яті, зловмисникам може бути складніше використовувати вразливості пам’яті або витягувати конфіденційну інформацію;
- отримання інформації: шифруючи дані, він допомагає запобігти несанкціонованому доступу або перехопленню конфіденційної інформації, що ускладнює зловмисникам отримання цінної інформації.

Шифрування є критично важливим елементом керування для захисту конфіденційності та цілісності даних. Він доповнює інші елементи керування, захищаючи дані від несанкціонованого доступу, навіть якщо інші заходи безпеки обходяться.

Запобігання втраті даних:

- DoS: запобігання втраті даних може допомогти виявити та заблокувати аномальний мережевий трафік, пов’язаний з DoS-атаками, сприяючи загальному захисту від таких загроз;
- виконання коду: може виявити та запобігти викраденню конфіденційних даних через мережеві канали або спробам неавторизованого виконання коду;
- пошкодження пам’яті: це може допомогти виявити підозрілу мережеву активність або витік даних, які можуть свідчити про атаки, пов’язані з пам’яттю;
- отримання інформації: може виявити та запобігти несанкціонованому витоку даних або спробам витоку, зменшуючи ризик розголошення конфіденційної інформації.

Запобігання втраті даних доповнює інші елементи керування, зосереджуючись на виявленні та запобіганні викраданню чи витоку даних. Це допомагає захистити конфіденційну інформацію та підтримує загальну безпеку віртуальної інфраструктури.

Контроль доступу на основі ролей:

- DoS: контроль доступу на основі ролей може допомогти запобігти неавторизованим користувачам або зловмисникам від втручання в критичні ресурси, що може призвести до сценаріїв DoS;
- виконання довільного коду: застосовуючи належний контроль доступу та дозволи користувача, він зменшує поверхню атаки та обмежує можливість виконання шкідливого коду;
- пошкодження пам’яті: контроль доступу на основі ролей має помірний вплив (оцінка 6 балів) на пом’якшення загроз пошкодження пам’яті. Обмежуючи доступ до чутливих областей пам’яті або критичних системних компонентів, це допомагає зменшити ризик атак на основі пам’яті;
- отримання інформації: контроль доступу на основі ролей має сильний вплив (оцінка 7 балів) на пом’якшення загроз отримання інформації. Застосовуючи принцип найменших привілеїв, він обмежує несанкціонований доступ до конфіденційної інформації та зменшує потенційний вплив розголошення інформації.

Контроль доступу на основі ролей є основним контролем для забезпечення обмежень доступу та привілеїв. Він працює в поєднанні з іншими елементами керування, щоб забезпечити багаторівневий підхід до безпеки та пом’якшити різні загрози.

Розуміючи бали та взаємозалежності кожного елемента керування в матриці загроз, організації можуть оцінити ефективність своїх засобів контролю щодо пом’якшення конкретних загроз і відповідно визначити пріоритети своїх заходів безпеки.

Тобто можна зробити висновки, що оцінювання ризиків стає більш доступним за допомогою матричного методу. Методологія забезпечує прозорість процесу аналізу. За допомогою неї висвітлено важливі активи для віртуальної інфраструктури. Вимоги, контрзаходи постійно змінюються, тому адаптивна і проста у використанні методологія є цінною для компаній для проведення внутрішньої оцінювання ризиків. Даний метод не вимагає значних тимчасових і фінансових витрат, а також поглибленого навчання фахівців, що його

використовують (у разі потреби досить короткострокового підвищення кваліфікації) Також, його рекомендується застосовувати для оцінювання ризиків на будь-якому рівні: організації в цілому, на рівні проекту/відділу, а також для конкретного обладнання чи процесу.

Усунення інформаційних ризиків під час роботи з віртуальним середовищем вимагає комплексного підходу, який включає впровадження надійних засобів контролю безпеки, регулярний моніторинг і сильну стратегію управління ризиками [20].

ВИСНОВКИ

У ході магістерської роботи проведено оцінювання ризиків віртуальної інфраструктури. Задля цього, проведено аналіз типів віртуалізації, вразливостей та загроз віртуальної інфраструктури, проаналізовано найважливіші актив віртуального середовища, а також аналіз методів і засобів оцінювання ризиків в контексті забезпечення інформаційної безпеки віртуальної інфраструктури.

В результаті дослідження виявлено, що найпридатніший тип віртуалізації – повна віртуалізація. Повна віртуалізація імітує базове апаратне забезпечення в програмному забезпеченні для кожної віртуальної машини, повністю відокремлюючи гостьову ОС від основного апаратного забезпечення. Цей підхід забезпечує найвищу ізоляцію та безпеку, але знижує продуктивність і додає додаткові витрати.

Також проаналізовано вразливості та загрози інформаційної безпеки віртуальної інфраструктури. Був побудований перелік слабких місць віртуальної інфраструктури.

Проаналізувавши методи і засоби оцінювання ризиків, обрано матричний метод оцінювання ризиків для віртуальної інфраструктури. Методологія забезпечує прозорість процесу аналізу. За допомогою неї можна висвітлити важливі питання безпеки, з якими стикається організація. Оскільки активи, загрози і вразливості постійно змінюються, адаптивна і проста у використанні методологія є цінною для компаній для проведення внутрішньої оцінювання ризиків.

На підставі проаналізованих активів віртуальної інфраструктури та обраного методу оцінки ризиків інформаційної безпеки, проведено оцінювання ризиків віртуальної інфраструктури на основі побудованої моделі об’єктів захисту віртуальної інфраструктури.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Шульга М. Д. Механізми захисту віртуального середовища. *Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій* : матеріали 27-го Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті», м. Харків, 10 – 12 трав. 2023 р. Харків : ХНУРЕ, 2023. С. 62 – 63.
2. Шульга М. Д. Оцінка інформаційних ризиків при роботі з віртуальним середовищем. *Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій* : матеріали 27-го Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті», м. Харків, 10 – 12 трав. 2023 р. Харків : ХНУРЕ, 2023. С. 60 – 61.
3. Difference between Virtualization & Emulation | programs that imitate hardware. URL: https://www.hitechnectar.com/blogs/virtualization-emulation/ (дата звернення: 10.04.2023).
4. Virtualization. URL: https://wiki.alquds.edu/?query=Virtualization_software_licensing (дата звернення: 10.04.2023).
5. Virtual machine (VM). URL: https://www.techtarget.com/searchitoperations/definition/virtual-machine-VM (дата звернення: 10.04.2023).
6. What Is Virtualisation? (Definition, Types And Uses). URL: https://in.indeed.com/career-advice/career-development/what-is-virtualisation (дата звернення: 11.04.2023).
7. CWE-681: Incorrect Conversion between Numeric Types. URL: https://cwe.mitre.org/data/definitions/681.html (дата звернення: 15.04.2023).
8. Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable. URL: https://www.researchgate.net/publication/303821673_Virtualization_Technology_Cross-VM_Cache_Side_Channel_Attacks_make_it_Vulnerable (дата звернення: 15.04.2023).
9. Cross-Site Request Forgery [CWE-352]. URL: https://www.immuniweb.com/vulnerability/cross-site-request-forgery.html (дата звернення: 18.04.2023).
10. CWE-332: Insufficient Entropy in PRNG. URL: https://cwe.mitre.org/data/definitions/332.html (дата звернення: 18.04.2023).
11. Role-Based Access Control (RBAC). URL: https://www.imperva.com/learn/data-security/role-based-access-control-rbac/ (дата звернення:

24.04.2023).

12. Оцінка ризиків. URL: https://buklib.net/books/26672/ (дата звернення: 21.04.2023).

13. Корченко О.Г., Шелест М.Є., Казмірчук С.В., Ткач Ю.М., Іванченко Є.В. Менеджмент інформаційної безпеки : ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. 408 с.

14. FAIR vs. Legacy Risk Quantification Methods [CWE-352]. URL: https://www.cybersaint.io/blog/a-pocket-guide-to-factor-analysis-of-information-risk-fair (дата звернення: 25.04.2023).

15. Левченко Є.Г., Швець В. А., Демчишин М.В. Економіка інформаційної безпеки : навч. посіб. Київ: НАУ, 2012. 225 с.

16. Information security risk analysis – a matrix-based approach. URL: https://www.albany.edu/~GOEL/publications/goelchen2005.pdf (дата звернення: 25.04.2023).

17. CVE List. URL: https://cve.mitre.org/cve/search_cve_list.html (дата звернення: 28.04.2023).

18. A Methodology for Enabling Forensic Analysis Using Hypervisor Vulnerabilities Data. URL: https://csrc.nist.gov/publications/detail/nistir/8221/final (дата звернення: 28.04.2023).

19. Vmware: Vulnerability Statistics. URL: https://www.cvedetails.com/vendor/252/Vmware.html (дата звернення: 28.04.2023).

20. Шульга М. Д. Інформаційні ризики при роботі з віртуальним середовищем. *Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій* : матеріали 27-го Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті», м. Харків, 10 – 12 трав. 2023 р. Харків : ХНУРЕ, 2023. С. 58 – 59.