МАГІСТЕРСЬКА РОБОТА

15.04 – МР. 1859 “С” 2021.01.11.013 ПЗ

Ліпатов Роман Миколайович

2022 р.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.78:004.056.53

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету	Завідувач кафедри
Інформаційних технологій	Комп'ютерних систем, мереж та кібербезпеки
_____ Глазунова О.Г., д.пед.н, проф.	_____ Касаткін Д.Ю, к.п.н., доцент.
підпис ПІБ, вчене звання і ступінь	підпис ПІБ, вчене звання і ступінь
«__» _____ 2022 р.	«__» _____ 2022 р.

МАГІСТЕРСЬКА РОБОТА

На тему: «Дослідження хмарних технологій захисту комп'ютерного мережевого трафіку»

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма Комп'ютерні системи та мережі

Орієнтація освітньої програми _____

Керівник дипломного проекту: _____ Сагун А.В.
підпис ПІБ

Виконав: _____ Ліпатов Р.М.
підпис ПІБ

КИЇВ-2022

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
_____ / Лахно В.А., д.т.н., проф. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 20__ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ

Ліпатов Роман Миколайович
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): 123 - комп'ютерна інженерія
Освітня програма: комп'ютерні системи та мережі
Орієнтація освітньої програми:

Тема магістерської роботи: «Дослідження хмарних технологій захисту комп'ютерного мережевого трафіку»

затверджена наказом ректора НУБіП України від "01" листопада 2021 р. № 1859 «С»
Термін подання завершеної роботи на кафедру: 17 листопада 2022 р.
Вихідні дані до магістерської роботи: існуюча інформаційно-комунікаційна система підприємства, хмарна платформа PaaS, віртуальні образи комутаторів vIOS, система віртуальних контейнерів.

Перелік питань, що підлягають дослідженню:
1. Аналіз структури та задач хмарних сервісів для центрів обробки даних
2. Планування структури і складу технологій захисту комп'ютерного мережевого трафіку ЦОД
3. Реалізація хмарного захищеного ЦОД

Перелік графічного матеріалу (за потреби):

Дата видачі завдання " 01 **"** листопада 2021 р.

Керівник магістерської роботи _____ Сагун А.В.,к.т.н.,доцент.
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Ліпатов Р.М.
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка задачі магістерської роботи	01.11.2021	Виконано
2	Аналіз предметної області	10.12.2021	Виконано
3	Аналіз структури та задач хмарних сервісів для центрів обробки даних	15.07.2022	Виконано
4	Планування структури і складу технологій захисту комп'ютерного мережевого трафіку ЦОД	15.18.2022	Виконано
5	Реалізація хмарного захищеного ЦОД	30.09.2022	Виконано
6	Оформлення пояснювальної записки	10.11.2022	Виконано
7	Оформлення графічного матеріалу	20.10.2022	Виконано
8	Оформлення списку використаних джерел	25.10.2022	Виконано
9	Отримання рецензії	28.10.2022	Виконано
10	Захист магістерської роботи	17.10.2022	

Студент _____ Ліпатов Р.М.
(підпис) (ініціали та прізвище)

Керівник проекту (роботи)_____Сагун А.В.
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка: 53 сторінки, 28 рисунків, 4 таблиці, 15 джерел.

ХМАРНИЙ СЕРВІС, PaaS, ОБРАЗ КОМУТАТОРА vIOS, ЦЕНТР ОБРОБКИ ДАНИХ, ВІРТУАЛЬНИЙ КОНТЕЙНЕР.

Об’єкт розробки – технологія захисту хмарного центру обробки мережевої інформації.

Мета роботи – полягає у вивченні та дослідженні технологій захисту мережевого трафіку хмарного захищеного ЦОД з використанням віртуалізації.

Предмет – хмарні технології захисту мережевого трафіку віртуальних компонентів ЦОД.

Проект складається з трьох розділів.

Перший розділ присвячений аналізі структури та задач хмарних сервісів та центрів обробки даних. Виконується аналіз існуючих типів мережевих інфраструктур для створення на її базі технологій захисту комп'ютерного мережевого трафіку.

У другому розділі проведено планування структури і складу технологій захисту комп’ютерного мережевого трафіку ЦОД.

Третій розділ присвячено реалізації хмарного захищеного ЦОД. В розділі проведено встановлення віртуальних контейнерів та інших необхідних додатків, які забезпечують роботу корпоративного ЦОД та налаштовано супутні сервіси в хмарі, які забезпечують захист доступності мережевого трафіку.

В ході виконання роботи було досягнуто мету – вивчено та досліджено технологій захисту трафіку хмарного захищеного ЦОД з використанням віртуалізації.

Встановлено, що незважаючи на те, що в Україні існують регламентуючі документи щодо безпеки хмарних сервісів, користуватися лише методами з ДСТУ не можна — вони не враховують останніх змін у сфері таких технологій, розгортання та загроз.

ЗМІСТ

ВСТУП

Хмарні технології і сервіси різного призначення використовують для роботи, в науці, охороні здоров'я, у приватному житті. Практично будь-який сайт або сервіс в інтернеті так чи інакше існує або може бути перенесений в хмару. Великі обсяги даних, які генерує кожна людина та будь-яка компанія, потребують зберігання і захисту. Тому питання безпеки хмарних технологій це пріоритет як для постачальника послуг, так і для клієнтів.

Захист даних в хмарі – це складний багаторівневий процес. Захист інформації в публічній хмарі передбачає, що найбільше дій відбувається на стороні постачальника послуг, з боку клієнта необхідно лише дати згоду (підтвердити оферту) на двофакторну авторизацію або придумати надійний пароль. Публічні хмарні сервіси рідко використовують для потреб бізнесу через невисоку гнучкість та низьку масштабованість, тому для захисту даних в мережі найбільше використовують гібридні хмарні сервіси.

Найбільш критичні дані, які захищаються в хмарі є персональні та конфіденційні дані, тому хмарні сервіси, які їх захищають повинні гарантувати захист конфіденційності, цілісності і доступності даних при збереженні спостережності.

Актуальність дослідження хмарних технологій захисту комп'ютерного мережевого трафіку пояснюється перспективами і затребуваністю даної технології.

Об’єктом роботи є технологія захисту хмарного центру обробки мережевої інформації.

Предметом роботи є хмарні технології захисту мережевого трафіку віртуальних компонентів ЦОД.

Метою роботи є вивчення та дослідження технологій захисту мережевого трафіку хмарного захищеного ЦОД з використанням віртуалізації.

Новизна роботи полягає у розробці та дослідженні хмарної технології захисту комп'ютерного мережевого трафіку для інформаційної системи в складі ЦОД.

Для досягнення мети слід вирішити такі **задачі:**

- проаналізувати хмарні технології захисту комп'ютерного мережевого трафіку в структурі хмарних сервісів та центрів обробки даних
- спланувати структури та механізмів захисту центру обробки даних на базі технологій віртуалізації
- реалізувати та протестувати моделі хмарних захищених ЦОД.
- визначити параметри та характеристики технологій захисту комп'ютерного мережевого трафіку

Структура та обсяг роботи. Робота складається із вступу, 3 розділів та висновків, переліку використаних джерел з 16 найменувань на 2 сторінках.

Загальний обсяг роботи складає 56 сторінок, з них 55 сторінки основного тексту.

РОЗДІЛ 1

СТРУКТУРА ТА ЗАДАЧІ ХМАРНИХ СЕРВІСІВ ТА ЦЕНТРІВ ОБРОБКИ ДАНИХ

1.1 Стандарти та правила захисту комп'ютерного мережевого трафіку

При експлуатації сертифікованої системи захисту інформації передбачаються спеціальні заходи захисту трафіку в мережі. Існує офіційна система відповідальності за недостатні заходи хмарної безпеки, є правила, що їх регламентують. Для України це гармонізований з європейським та американським стандартом ДСТУ:

- ICO/МЕК 27000 - 2012;
- ICO/МЕК 27001 - 2006;
- 50922 - 2006;
- 53114 - 2008.

Дані документи розроблені без врахування постійно змінних списків загроз та сучасних способів захисту даних у хмарі. Насправді, виконання вимог даних стандартів – це великий перелік відповідальності для споживачів та постачальників послуг та умовні рекомендації щодо методів забезпечення безпеки. Виконувати вимоги стандартів беззастережно немає потреби, адже список загроз та методів захисту щодня зростає, а ДСТУ не змінюються настільки ж часто. При проектуванні технологій захисту інформації слід перевірити, чи відповідають передбачені базові методи захисту даних у хмарі рекомендаціям. Для споживачів послуг більш актуальним документом є SLA. В цьому документі прописані конкретні послуги, які надає провайдер, та способи їх захисту.

1.1.1 Хмарні технології захист та безпека корпоративного мережевого трафіку

Основні види загроз для інформації та мережевого трафіку практично завжди незмінні, так само, як і причини для виникнення даних загроз. Є лише кілька основних причин:

– вторгнення;
– вірусне та шпигунське ПЗ;
– соціальна інженерія (людський чинник усередині компанії).

При виборі технології захисту розглядаються загрози, які залежать від зовнішніх факторів, наприклад, перегрівання обладнання у Дата-центрі. Надійні тримачі хмарних послуг розміщують своє обладнання в ЦОД не нижче рівня TIER III, де ризик поломок, перегріву, затоплення настільки мінімальний, що не відбувається практично ніколи.

Щоб захистити дані в хмарі від вторгнення, вірусних програм або витоку даних, необхідно налаштувати контроль доступу. Це не тільки логін і пароль, це глобальне поняття, яке стосується всіх засобів безпеки. Іншими словами, завдання захисту даних полягає в тому, щоб не просто налаштувати доступ для користувачів, а не допустити вторгнення ззовні.

Серед хмарних технологій захисту комп'ютерного мережевого трафіку можна виділити такі:

- мережні віртуальні пристрої (Firewall)
- програми захисту веб-інтерфейсу
- безперервний моніторинг мережевої активності.

В той же час, шифрування, двофакторна автентифікація та базове антивірусне програмне забезпечення повинні бути реалізовані на стороні провайдера. Якщо постачальник послуг не пропонує засобів базового захисту даних у хмарі, то варто це робити самостійно, оскільки безпека завжди є двостороннім процесом.

Для великої компанії організація інформаційної системи в хмарі передбачає багаторівневу архітектуру, великий набір послуг. Це тягне за собою відповідні витрати на експлуатацію і використання. Чим більше організація, тим вищий вплив людського фактора та можливість витоку даних.

Для вирішення проблеми корпоративної безпеки та зниження витрат зараз користуються можливостями архітектури захисту інформації у хмарних технологіях.

Існує декілька видів функціонування хмарних послуг:

Iaas – Infrastructure as a Service — інфраструктура як послуга, наприклад, віртуальні сервери та віртуальна мережа, клієнт може встановлювати будь-яке програмне забезпечення та програми (рис. 1.1)

Рис.1.1 – Схема Iaas – Infrastructure as a Service

Paas – Platform as a Service — платформа як послуга, наприклад веб-сервер або база даних, клієнт управляє програмами, операційною системою управляє провайдер (рис.1.2).

В моделі IaaS постачальник послуг зобов'язаний забезпечити, що лежить в основі фізичних ресурсів рівня інфраструктури (серверів, центрів обробки даних, контроль хмарного середовища, електричні, серверні кімнати). В той

же час покупець здійснює розгортання та впровадження різного програмного забезпечення, такого, як операційні системи чи програми-додатки.

(PaaS (Platform as a Service)

Рис.1.2 – Схема Paas – Platform as a Service

В моделі організації хмарної інфраструктури PaaS постачальник послуг зобов'язується забезпечити інфраструктуру базових сервісів, забезпечуючи операційні системи (Windows, Linux), сервери баз даних, веб-сервери, контролери домену та інш, а також проміжне програмне забезпечення резервного копіювання послуг у сервісних моделях. Наприклад, IIS, .NET, Apache, MySQL.

Завдання покупця даної послуги полягає в тому, щоб контролювати розгортання додатку верхнього шару із затвердженим середовищем.

SaaS — Software as a Service — програмне забезпечення як послуга, наприклад, електронна пошта чи інший офісний додаток; клієнт користується програмою, базовими налаштуваннями програми управляє провайдер (рис.1.3).

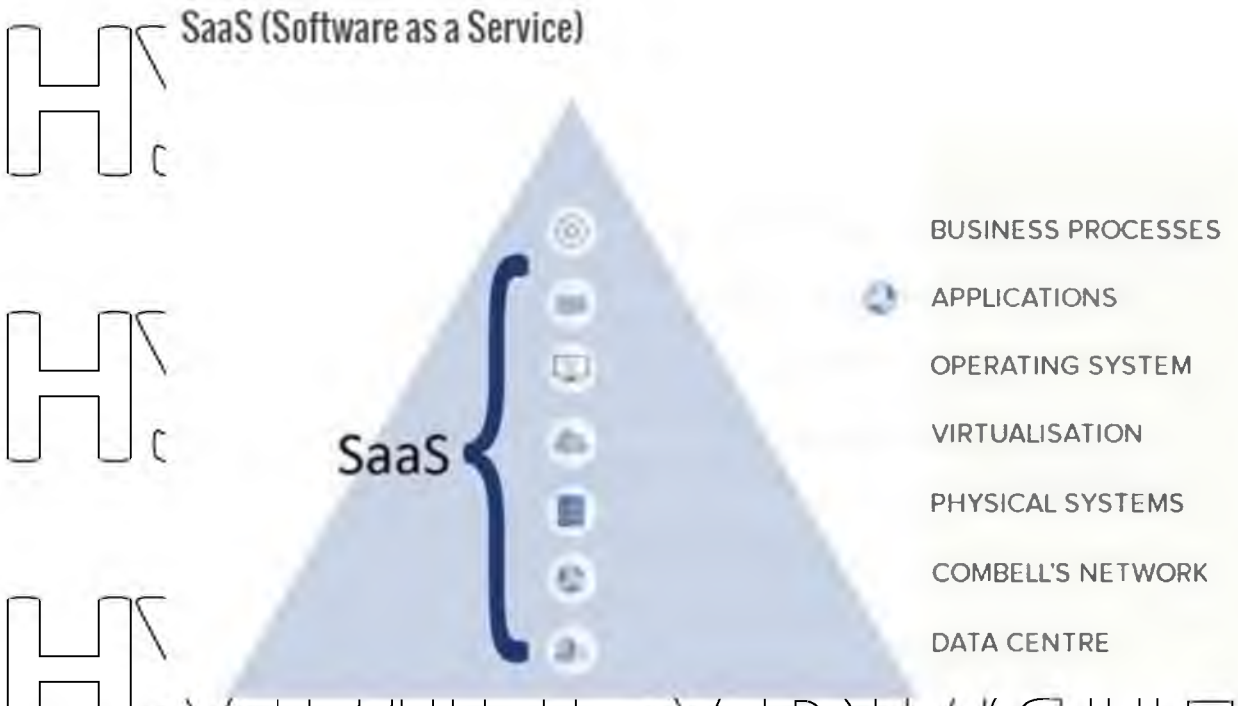

Рис.1.3 – Схема SaaS – Software as a Service

Постачальник послуг по схемі SaaS зобов'язаний забезпечити програмні рішення для кінцевих споживачів задовольняти потреби, такі як OA, CRM, MIS, ERP, HRM, CM, Office 365, ICloud, G Suite.

Для покупця немає необхідності розглядати будь-яку форму експертизи, він отримує повний пакет хмарних послуг відповідно до своїх вимог, роблячи свою повсякденну роботу та життя простіше.

1.2 Архітектура захисту даних в хмарі

Базове поняття хмарних сервісів «як послуга» означає, що провайдер має сервери, які він зберігає в ЦОД. За допомогою ряду пристроїв, програмного забезпечення та коду провайдер розподіляє фізичні потужності своїх серверів між орендарями, які стримують набір певних функцій у форматі «як послуга».

У вигляді послуг можна отримати:

- інфраструктуру (ОС, потужності);
- апаратне забезпечення;
- програмне забезпечення;
- платформу;

- базу даних;
- робочий стіл.

Для ефективного захистити дані у хмарі та заощадження ресурсів є простий спосіб - скористатися сервісом платформа-як-послуга (PaaS) та Софт-як-послуга (SaaS).

Перевага використання служби PaaS полягає у делегуванні деяких елементів безпеки постачальнику хмарних послуг. Це практично завжди вигідно для невеликих та середніх організацій. У середовищі PaaS (платформа) або SaaS (ПЗ) компанія користується заходами захисту, які пропонує постачальник.

При потребі повноцінного контролю над усіма заходами безпеки даних у хмарі, вам підійде модель IaaS (Інфраструктура-як-послуга), яка забезпечує більш детальні елементи управління та дозволяє їх вибирати.

1.2.1 Фільтрація даних і контроль використання ресурсів

Основною причиною фільтрації даних та контролю ресурсів при організації захисту трафіку є запобігання несанкціонованому доступу до хмарних послуг. Хакерський доступ може бути не лише ззовні. Співробітники компанії також можуть негативно впливати на безпеку в якості інсайдерів, відвідуючи сумнівні сайти або надсилаючи конфіденційну інформацію не за призначенням. Основний спосіб коректно відфільтрувати відомості та проконтролювати доступ до ресурсів полягає у використанні Firewall (брандмауера) в оптимальній конфігурації.

Брандмауери почали використовувати для захисту даних у хмарах не так давно. Сучасні Firewall (NGFW) відрізняються інтегрованими функціями безпеки для хмарних сервісів:

- функції NAT/PAT;
- глибока перевірка пакетів – з поведінковим підписом або IDS/IPS;
- спеціалізовані веб-елементи керування — правила WAF.

РОЗДІЛ 2

ПЛАНУВАННЯ СТРУКТУРИ І СКЛАДУ ТЕХНОЛОГІЙ ЗАХИСТУ КОМП'ЮТЕРНОГО МЕРЕЖЕВОГО ТРАФІКУ ЦОД

2.1 Мережева інфраструктура інформаційної системи модельного підприємства

В рамках дослідження маємо модельне підприємство – інтернет магазин. Для такого об’єкту передбачається, що його хмарна інформаційна система повинна функціонувати безперебійно та обов’язковою вимогою щодо захисту є необхідність гарантувати неможливість підміни вмісту сайту. Будь-яка підміна контенту на web-сторінці спричинить збитки та компрометацію ділової репутації даного інтернет магазину.

2.1.1 Інформаційно-комунікаційна система підприємства

Схема планованої мережевої інфраструктури вузла комп’ютерної мережі підприємства наведена на рис.2.1.

Як видно з рис.2.1, ІКС підприємства складається з двох сегментів: LAN1, LAN2. Для забезпечення надійного каналу мережевого трафіку магазин під’єднаний до точок Інтернет доступу від двох незалежних провайдерів – ISP1, ISP2. Такі заходи забезпечують кращу доступністі інформації, яка отримується по 2 незалежним мережевим інтерфейсам: Net1 і Net2.

Комп’ютери менеджерів контенту Інтернет-магазину - VPC6, VPC7, VPC11 в LAN1 мають статичні IP. На цих комп’ютерах них розташовані: web-сервер, поштовий сервер та файловий сервер компанії.

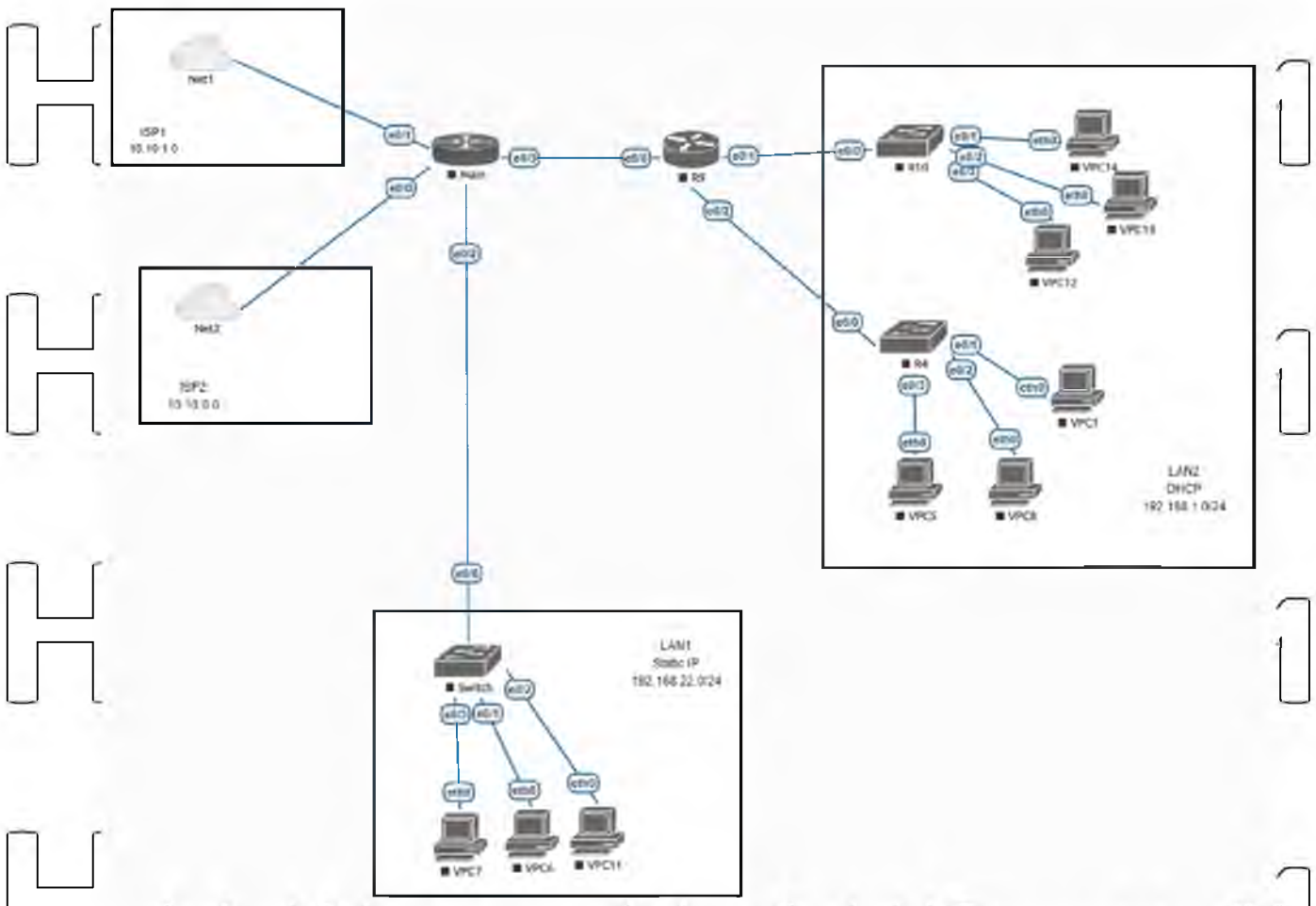

Рис.2.1 – Схема ІКС підприємства

Комп'ютери VPC6, VPC7, VPC11 в LAN1 підключаються до загальної мережі через статичні IP. Саме на них фізично розташовані web-сервер, поштовий сервер та файловий сервер (кожний з серверів на окремому ПК для мінімізації наслідків сторонніх втручань). В мережі LAN2 наявні комп'ютери отримують динамічні IP адреси через службу DHCP. Вони використовуються в якості хост-платформ для різноманітних сервісів підприємства.

2.2 Платформи для розміщення віртуальної інфраструктури ЦОД

Модель хмарної технології захисту трафіку можна побудувати на декількох наявних платформах хмарних обчислень типу PaaS. Розглянемо три

найбільш популярні існуючі хмарні платформи, які підходять для розгортання хмарних технологій захисту комп'ютерного мережевого трафіку [7]:

- AWS (Amazon Web Services)
- GCP (Google Cloud Platform)
- Microsoft Azure.

Розглянемо їх далі детальніше.

2.2.1 Amazon Web Services (AWS) є платформою хмарних обчислень. Така платформа здається в оренду приватним особам, компаніям та урядовим організаціям, приватним особам на основі платної підписки. Дана платформа може ліцензуватися, як безкоштовна, але така можливість доступна лише на перші 12 місяців. Технологія, за якою побудована платформа AWS дозволяє її абонентам клієнту отримувати повноцінний віртуальний кластер, що складається з декількох комп'ютерів. Такий кластер доступний для своїх користувачів через мережу Інтернет. Для доступу до нього можна використовувати будь-який доступний web-клієнт.

Наявна в складі платформи AWS система віртуалізації надає можливість віртуальним машинам мати практично всі атрибутами реальних комп'ютерів, включно і апаратні пристрої: процесор; відеокарту, мережевий адаптер; локальну та оперативну пам'ять, жорсткий диск або SSD-накопичувач тощо. На такі машини користувач може встановити операційну систему на свій вибір та налаштовувати мережеве оточення; встаньовити та налаштувати необхідні програмні додатки, такі як: веб-сервер, база даних, корпоративні поштові сервіси, система керування контентом.

Кожна клієнтська система в рамках платформи AWS віртуалізує також засоби консольного введення/виводу (клавіатура, дисплей тощо). Такі можливості дозволяють користувачу платформи AWS підключитися до свого своєї розгорнутої хмарної інфраструктури в AWS через web-браузер. За допомогою браузера користувач входить до системи, налаштовує її та використовує свої віртуальні сервіси аналогічно до того, як він використовує

фізичний комп'ютер або сервер. Платформа дозволяє налаштувати систему таким чином, щоб надавати у зручний спосіб інтернет-орієнтовані сервіси, послуги клієнтам.

Технологія віртуальних контейнерів AWS засновується на використанні серверних кластерів (фермах). Ці ферми фізично розташовані по всьому світі. Плата за користування AWS платформою базується на використанні апаратних засобів, програмного забезпечення, операційних систем, мережевих функцій, які користувач обирає самостійно. Вона базується на вимозі щодо доступності, надлишковості (redundancy), безпеки та деяких інших додаткових параметрах. Користувачу доступна можливість зарезервувати віртуальний комп'ютер (Virtual Machine - VM), кластер віртуальних комп'ютерів (VM Cluster) або фізичний комп'ютер (Server), який призначений для його виняткового користувацького використання. Можливо зарезервувати цілий кластер фізичних комп'ютерів (Server Cluster).

2.1.2 Платформа Microsoft Azure являє собою хмарну платформу та інфраструктуру, яка розроблена компанією Microsoft. Дана платформа призначена в першу чергу для розробників додатків в сфері хмарних обчислень. Основним призначенням платформи є спрощення процесу створення он-лайн додатків. Особливо тісно Azure підтримує технології віртуалізації Microsoft.

Платформа Windows Azure складається з таких компонент:

1. Windows Azure — середовище виконання програмних додатків, які засновані на операційних системах, таких, як Windows Server. Azure також є місцем зберігання даних (Data Storage Space). Система Azure функціонує на віртуальних машинах за допомогою технології, яка аналогічна технології Hyper-V.
2. Обчислення здійснюються процедури обчислень для розміщених додатків.
3. Зберігання — механізм зберігання даних в хмарі.

4. Компонент керування реляційною БД SQL Azure надає можливість використовувати реляційну базу даних для запуску додатків в хмарі.

Платформа Windows Azure AppFabric — це компонент, що забезпечує хмарній платформі додаткову функціональність у вигляді комплексу різних послуг та сервісів.

2.1.3 Платформа Google Cloud Platform є популярною платформою компанії Google. Вона містить і реалізує декілька технологій, які дозволяють побудувати розвинуту систему захисту комп'ютерного мережевого трафіку, наприклад:

- інфраструктура як послуга (IaaS)
- платформа як послуга (PaaS)
- безсерверні обчислення (Cloud Computing).

Google Cloud Platform є програмно-апаратним хмарним засобом, який розроблений для роботи з великим обсягом даних і побудови мережевих інфраструктур великого масштабу. Даний засіб дозволяє реалізувати технології захисту мережевого трафіку довільного складу і конфігурації. Він доступний широкому колу користувачів та дає можливість працювати з різними інструментами для реалізації хмарних обчислень і надання хостингу з використання віртуальних контейнерів програмних додатків. Це рішення дозволяє обрати або побудувати керовану прикладну платформу, використовувати технології віртуальних контейнерів для отримання більшої гнучкості або створити власну хмарну інфраструктуру з максимальним контролем та рівнем безпеки.

Google Cloud Platform (GCP) – набір інструментів рівня IaaS, PaaS, ML та інтерфейси API для розробників і бізнесу. Платформа забезпечує і підтрмує віртуальні машини, хостинг додатків і контейнерів, машинне навчання, сервіси зберігання і обробки даних – все це та багато іншого входить до складу

платформи і може бути використано для цифрової трансформації та створення цифрових продуктів.

Платформа GCP дозволяє створювати, контролювати і використовувати хмарне сховище під різні завдання, наприклад:

- створення власних хмарних інфраструктури;
- обчислення і хостинг;
- міграція в хмару.

На сервісах платформи GCP працюють: міжнародна платіжна система PayPal, інтернет-магазин eBay, інтернет-сервіс Spotify та Twitter.

Платформа AWS надає послуги для розміщення мережевої інфраструктури по всьому світу. Платформи Azure і GCP також розміщуються у декількох географічно розподілених місцях по всьому світу, але різниця полягає в кількості зон доступності. Платформа AWS має 66 зон доступності, Azure доступна в 140 країнах світу, а Google Cloud Platform доступна в 20 регіонах.

Таким чином, всі розглянуті платформи перспективні для використанні в якості місця розгортання хмарних сервісів бізнес-рівня, побудови віртуальних мереж.

З точки зору перспективності розглянутих платформ можна побачити, що зростання продажів рішення AWS від Amazon становило 17,7 мільярдів доларів США у 1 кварталі 2020 року (зріст доходу на 50% у порівнянні з попереднім кварталом) відповідно до звіту про фінансові прибутки. В той же час платформа Amazon AWS отримує за той же період доходи у 13,5 мільярдів доларів США за квартал (зростання на 32% за 1 квартал 2021 року). Рішення від Google - GCP дає компанії дохід у 4,05 мільярда доларів США (рис.2.2).

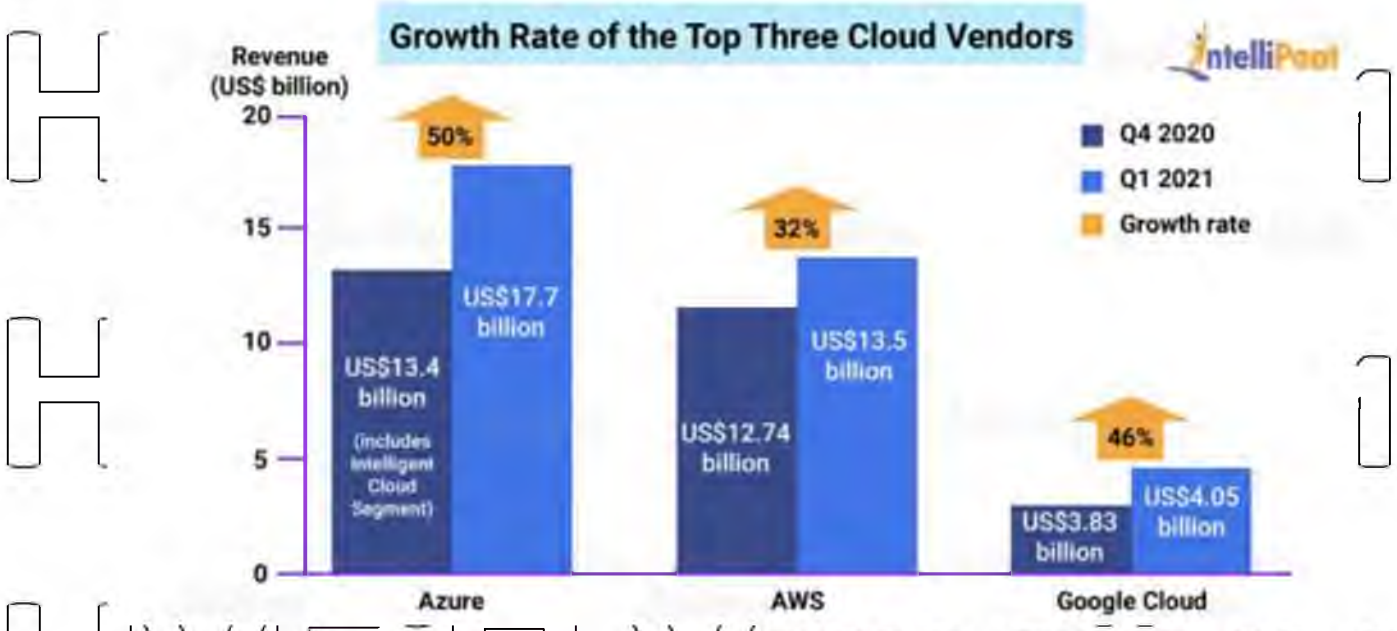

Рис.2.2 – динаміка збільшення популярності найбільших трьох хмарних платформ, оцінена у доларах

У звітах від агенції Canalys згадується, що станом на квітень 2021 року світовий ринок хмарних рішень зріс на 35%, а у 2 кварталі 2021 року – до 41,8 мільярда доларів. При цьому на ринку хмарних рішень для розміщення мережевої інфраструктури платформа AWS займає 32% ринку, Azure - 19% і Google - 7% вартості продажів в даному сегменті (рис.2.3) [7].

Таким чином, хмарні рішення для розміщення мережевої інфраструктури мають велику популярність та гарні перспективи на ринку ЦОД.

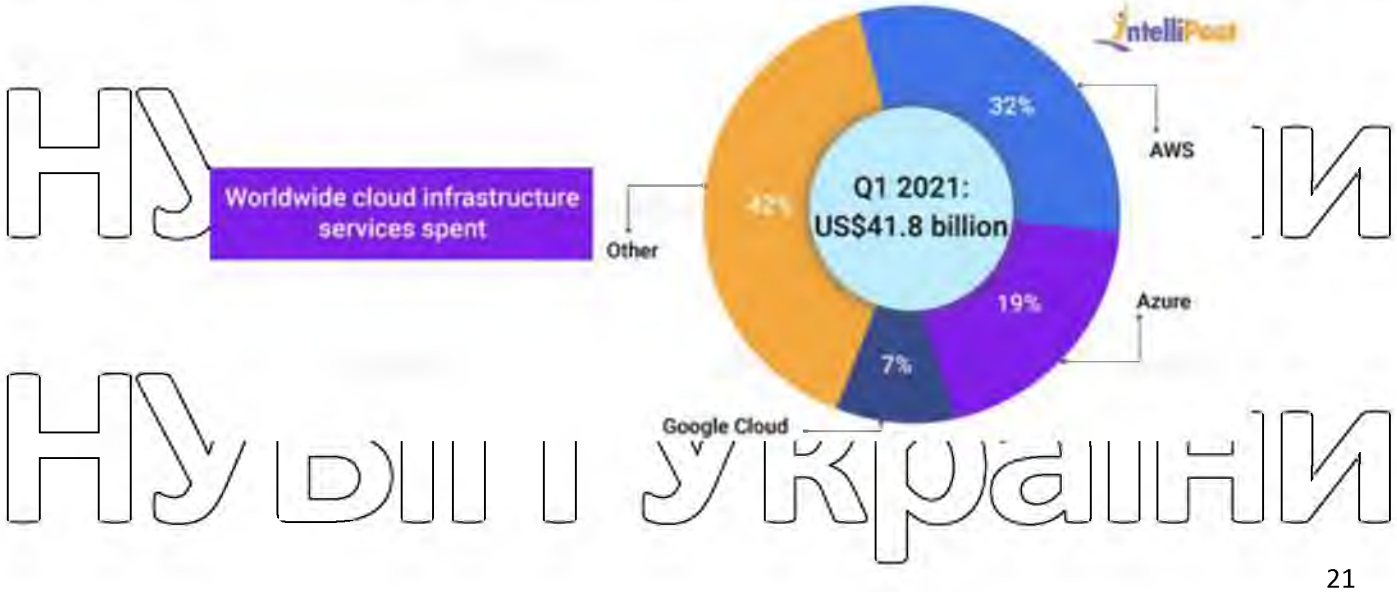

Рис.2.3 – Обсяг продажу хмарних рішень від 3 найбільших виробників на 1 квартал 2021 року

При виборі цільової хмарної платформи слід врахувати додаткові переваги, які полягають в більшому терміні присутності на ринку обчислювальних послуг хмарної платформи AWS. Ця платформа є найбільш розвиненою та функціонально багатшою, порівняно з рішеннями від Google та Microsoft.

Платформа AWS пропонує більше 200 різних сервісів, тоді як Azure пропонує приблизно 100. Платформа GCP, з іншого боку, пропонує понад 60 хмарних сервісів, які придатні для створення ІДОД [8].

В таблиці 2.1 наведено пропозиції послуг від платформ AWS, Azure та GCP, які належать до доменів обчислень, баз даних, зберігання та мереж тощо.

Таблиця 2.1 - Сервіси хмарних платформ

Сервіси	Назва та тип у платформі		
	AWS	Azure	GCP
IaaS	Amazon Elastic Compute Cloud	Virtual Machines	Google Compute Engine
PaaS	AWS Elastic Beanstalk	App Service and Cloud Services	Google App Engine
Containers	Amazon Elastic Compute Cloud Container Service	Azure Kubernetes Service (AKS)	Google Kubernetes Engine
Serverless Functions	AWS Lambda	Azure Functions	Google Cloud Functions

Всі розглянуті платформи мають компоненти для повноцінної взаємодії з СУБД (таблиця 2.2).

Таблиця 2.2 – Компоненти для роботи з базами даних хмарних платформ

Сервіс	Назва та тип у платформі		
	AWS	Azure	GCP
RDBMS	Amazon Relational Database Service	SQL Database	Google Cloud SQL
NoSQL: Key–Value	Amazon DynamoDB	Table Storage	Google Cloud DatastoreGoogle Cloud Bigtable
NoSQL: Indexed	Amazon SimpleDB	Azure Cosmos DB	Google Cloud Datastore

Для зберігання даних у кожної з розглянутих платформ передбачені декілька видів технологій (таблиця 2.3).

Таблиця 2.3 – технології зберігання даних на хмарних платформах

Сервіс	Назва та тип у платформі		
	AWS	Azure	GCP
Object Storage	Amazon Simple Storage Service	Blob Storage	Google Cloud Storage
Virtual Server Disks	Amazon Elastic Block Store	Managed Disks	Google Compute Engine Persistent Disks
Cold Storage	Amazon Glacier	Azure Archive Blob Storage	Google Cloud Storage Nearline
File Storage	Amazon Elastic File System	Azure File Storage	ZFS/Avere

Для реалізації мережевих комунікацій, балансування трафіку та інших мережевих технологій розглянути хмарні платформи надають наступні компоненти (таблиця 2.3).

Таблиця 2.3 - Мережеві компоненти хмарних платформ

Services	AWS	Azure	GCP
Virtual Network	Amazon Virtual Private Cloud (VPC)	Virtual Networks (VNets)	Virtual Private Cloud
Elastic Load Balancer	Elastic Load Balancer	Load Balancer	Google Cloud Load Balancing
Peering	Direct Connect	ExpressRoute	Google Cloud Interconnect
DNS	Amazon Route 53	Azure DNS	Google Cloud DNS

Одним з важливих факторів вибору хмарної платформи для реалізації на ній моделі захищеного ЦОД є вартість володіння та супроводу. В таблиці 2.4 наведено порівняння цінових моделей AWS, Azure та GCP на основі типу умовного фізичного комп'ютера, який вони пропонують.

Таблиця 2.4 - порівняння цінових моделей AWS, Azure та GCP

Тип платформи	AWS	Azure	GCP
Найпростіша платформа	включає 2 віртуальні процесори та 8 ГБ оперативної пам'яті, ціна 69 доларів США на місяць.	Аналогічна до AWS - екземпляра з 2 віртуальними процесорами та 8 ГБ оперативної пам'яті, ціна 70 доларів США на місяць.	Порівняно з AWS, GCP найпростіший екземпляр, з 2 віртуальними процессорами, 8 ГБ оперативної пам'яті з ціною 52 доларів США на місяць.
Продуктивна платформа	3,84 ТБ оперативної	3,89 ТБ оперативної пам'яті, 128	3,75 ТБ оперативної пам'яті та 160 vCPU.

	пам’яті, 128 vCPU, коштує 3,97 доларів США на годину.	віртуальних процесорів. Коштує 6,79 доларів США на годин	Ціна 5,32 доларів США на годину.

2.2 Вибір засобів та технології адміністрування хмарного захищеного центру обробки даних

При тестуванні засобів безпеки, а також під час навчання персоналу сценаріям атак та захисту мережевої інфраструктури використовуються засоби віртуалізації. Для цього необхідно налаштувати платформу емуляції.

Існують декілька варіантів платформ емуляції, які можна використати для створення моделі хмарного захищеного центру обробки даних:

GNS3 – це графічний мережевий симулятор, який дозволяє моделювати складні комп’ютерні мережі. Для забезпечення повного та точного моделювання GNS3 тісно пов'язана з Dynamips, емулятором Cisco IOS.

Packet Tracer – це симулятор маршрутизуючого обладнання Cisco, який широко використовується у навчанні, освіті, а також у дослідженнях для простого моделювання комп'ютерних мереж.

Симулятор Verax SNMP Simulator – це інструмент, який може імітувати кілька агентів SNMPv1/v2c на одному хості на стандартному порту 161 через multi-netting. Індивідуальні відповіді на модельовані агенти можуть бути спочатку отримані з існуючих пристроїв і змінені під час виконання за правилами користувача.

NetSim для мережевого симулятора CCNP включає окрім підтримки класичних технологій маршрутизації також нові технології - ROUTE, SWITCH та TSHOOT.

Dynamips – це комп'ютерна програма емулятора, яка використовується для емуляції роботи маршрутизаторів. Dynamips працює на Linux, Mac OS X або Windows і може емулювати апаратне забезпечення платформ

маршрутизації Cisco-серій, безпосередньо завантажуючи фактичне зображення програмного забезпечення Cisco IOS в емулятор. Dynamips емулює платформи маршрутизаторів Cisco 1700, 2600, 2691, 3600, 3725, 3745 та 7200.

Cisco Packet Tracer Mobile – це інструмент моделювання та візуалізації мережі.

В якості системи емуляції моделі захищеного ЦОД в хмарі оберемо EVE-NG.

EVE-NG - це емульоване віртуальне середовище наступного покоління, що дозволяє створити повноцінну віртуальну лабораторію з мережевим обладнанням і програмним забезпеченням провідних світових виробників. Дане середовище дозволяє підприємствам, постачальникам/центрам електронного навчання, окремим співробітникам і співробітникам групи створювати віртуальні докази концепцій, рішень і навчальних середовищ [9].

Отже перейдемо до інструментальної реалізації моделі захищеної інформаційно-комунікаційної системи підприємства з метою створення та перевірки механізмів захисту для сервісів та систем, які сформульовані в задачах захисту інформації проектованого вузла інформаційно-комунікаційної системи.

2.3 Інтеграція технологій віртуалізації для моделі хмарного ЦОД

Для встановлення EVE-NG використовувався Google Cloud Platform - наданий компанією Google набір хмарних служб, які виконуються на тій же самій інфраструктурі, яку Google використовує для своїх продуктів, призначених для кінцевих споживачів, таких як Google Search і YouTube. Крім інструментів для управління, також надається ряд модульних хмарних служб, таких як хмарні обчислення, зберігання даних, аналіз даних і машинне навчання.

Фізично, це цілісна і стабільна віртуальна машина VMware, в основі якої лежить Linux Ubuntu 16.04 x64. Залежно від обраного способу установки,

EVE-NG також може працювати і безпосередньо на Ubuntu 16.04 із спеціально зібраним ядром kernel.

Вся емульоване середовище запускається всередині цієї машини, а доступ до неї здійснюється через звичайний веб браузер. Причому, не обов'язково з цього ж комп'ютера, це може бути і доступ по мережі, включаючи Інтернет.

За допомогою браузера можна в візуальному режимі створювати мережеві топології, що включають різних виробників, запускати емульовані пристрої, підключатися до них через консоль, а також наочно стежити за споживаними обчислювальними ресурсами EVE-NG.

Для підключення до цих пристроїв можна скористатися або спеціальним попередньо встановленим клієнтом, або просто звичайним HTML5 інтерфейсом.

Залежно від типу пристрою, підключаться через консоль до них можна по протоколам telnet, RDP або VNC.

А до вже сконфігурованих відповідним чином пристроїв, можна по мережі отримувати доступ через SSH, telnet, HTTP, HTTS.

2.3.1 Хмарне сховище функціонування моделі захищеної інформаційно-комунікаційної системи підприємства

Як вже зазначалося, в якості хмарного сховища будемо використовувати Google Cloud Platform. Це наданий компанією Google набір хмарних служб, які виконуються на тій же самій інфраструктурі, яку Google використовує для своїх продуктів, призначених для кінцевих споживачів, таких як Google Search і YouTube. Крім інструментів для управління даний сервіс надає ряд модульних хмарних служб, таких як хмарні обчислення, зберігання даних, аналіз даних і машинне навчання.

2.4 Вибір та обґрунтування системи керування додатками хмарного ЦОД

Система docker - система контейнеризації програм з відкритим вихідним кодом. Наприклад, зараз існує декілька сотень типів Linux-дистрибутивів. Кожний тип Linux-дистрибутива має свої власні особливості по встановленню і налаштуванню додатків. Наприклад:

- відмінність процедури встановлення пакетів (apt-get, yum, dnf)
- відмінність пакетної бази (потрібний пакет може бути відсутнім)
- назва пакета, його версія та механізм установки можуть відрізнятися
- пакети зібрані з різними опціями та розширеннями
- файли конфігурації розміщуються в різних місцях
- тощо.

Все це створює серйозні проблеми при перенесенні працюючого додатка з одного типу Linux-дистрибутиву на інший.

Docker вирішує цю проблему шляхом створення образу файлової системи, що включає крім програми всі необхідні бібліотеки і файли конфігурації. Таким чином, встановивши образ docker-програми, створеної для одного типу дистрибутива (наприклад, Ubuntu), можна на його основі запустити контейнер, який виконує програму на іншому дистрибутиві (наприклад, ALTLinux).

При роботі з web-додатками та їх робочими версіями docker дозволяє розгорнути найбільш популярні сервери, такі, як: nginx, php, mysql, phpmyadmin та будь-які інші додатки. Причому, відпадає потреба їх встановлювати та «засмічувати» систему.

Docker має засоби ізоляції сервісів від інфраструктури, що дає можливість значно спростити процес розгортання та експлуатації готових додатків. Така ізоляція підвищує безпеку даних і дозволяє запускати декілька віртуальних контейнерів на одному хості одночасно. Контейнери не вимагають наявності гіпервізора. Вони запускаються безпосередньо в ядрі

хост-ПК. Таким чином досягається можливість запуску великої кількості віртуальних контейнерів, що на порядки більше ніж кількість можливих запущених віртуальних машин, на одному фізичному обладнанні.

Інструмент Docker надає вбудовані інструменти та платформу для керування життєвим циклом віртуальних контейнерів. За допомогою Docker відбувається пакування додатків та їх компонентів до контейнера.

Таким чином, клієнт, який орендує хмарну платформу GCP після розробки свого додатку може розгорнути на встановлених серверах вручну або за допомогою оркестратора всі необхідні для функціонування ЦОД контейнери. Така техніка розгортання буде абсолютно однаковою незалежно від місця розгортання додатку (локальний дата центр, хмарний провайдер або гібридне оточення.

Docker використовує звичайну клієнт-серверну архітектуру (рис.2.4) [10].

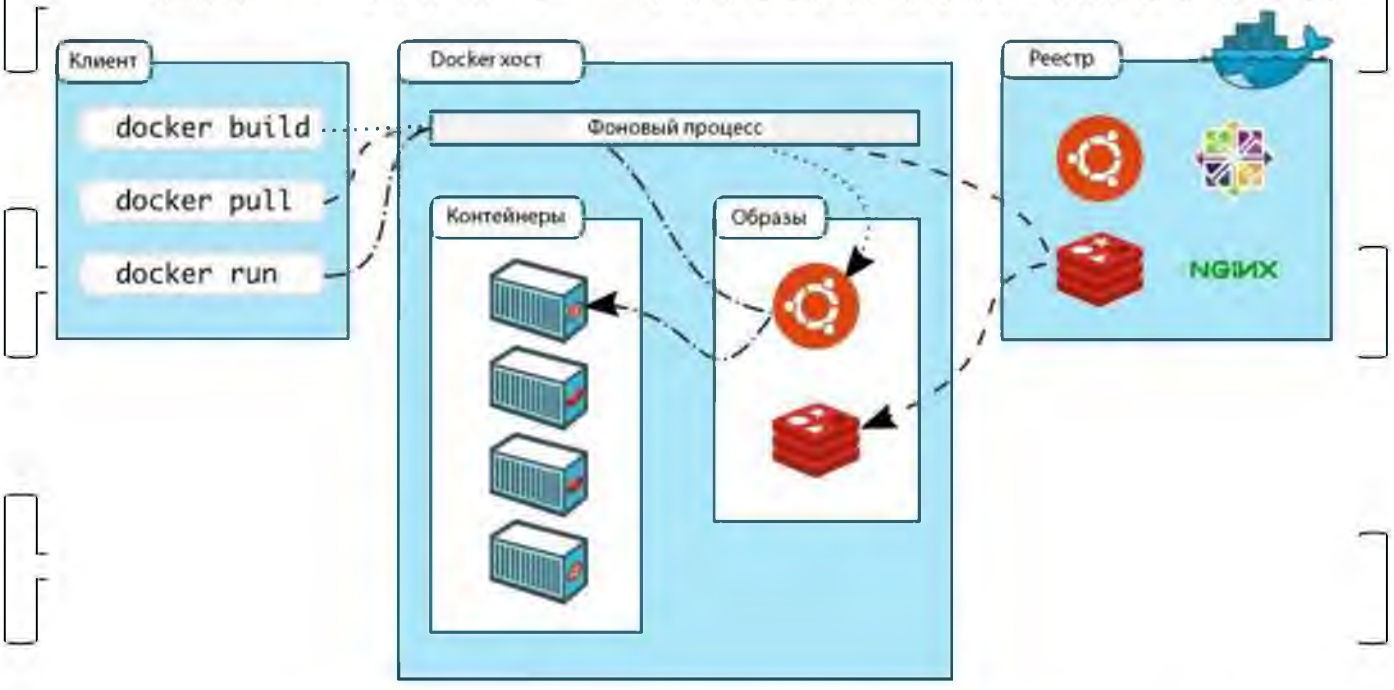

Рис. 2.4 Прицнипова схема представлення архітектури Docker

Docker - клієнт в процесі роботи взаємодіє з фоновим процесом – серверною частиною Docker, яка, в свою чергу запускає віртуальний контейнери. Клієнтська частина і фоновий процес можуть виконуватися в середовищі однієї ОС. Також існує можливість підключати клієнтські додатки до віддаленого фонового процесу.

Фоновий процес Docker здатен приймає запити і керувати об'єктами Docker.

Фоновий процес керує наступними об'єктами:

- образи;
- контейнери;
- мережеву взаємодію;
- томи.

Основною задачею Docker - клієнта є взаємодії з сервером. При виконанні команди клієнтська частина відправляє отриману команду фонового процесу, а той, в свою чергу, її виконує. Docker- клієнт може взаємодіяти з великою кількістю різних docker - серверів.

РОЗДІЛ 3

РЕАЛІЗАЦІЯ МОДЕЛІ ХМАРНОГО ЗАХИЩЕНОГО ЦОД З ВРАХУВАННЯМ ТЕХНОЛОГІЇ ЗАХИСТУ КОМП'ЮТЕРНОГО МЕРЕЖЕВОГО ТРАФІКУ

3.1 Організація розміщення мережевої інфраструктури проекту Google Cloud Platform (GCP)

Після вибору хмарного сховища для розташування моделі ЦОД, зареєструємо обліковий запис GCP, після чого у стартовому вікні GCP обираємо пункт «Выберите проект».

В наступному вікні обираємо пункт «Создать проект». Вводимо ім'я проекту і натискаємо кнопку «Создать» (рис.3.1).

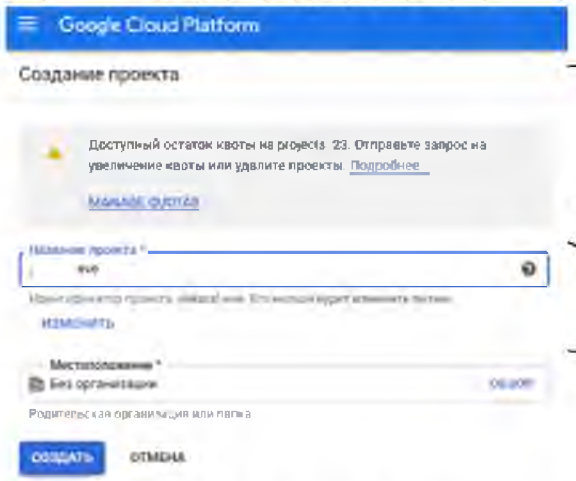

Рис. 3.1 – Створення проекту

В створеному хмарному дисковому сховищі розгорнемо програмні відображення ОС, які відповідають реальним, присутнім в ІКС підприємства, топологія та компоненти ІКС якого описані в п. 2.1.1.

Панель для адмін стрування GCP має вид, показаний на рис.3.2.

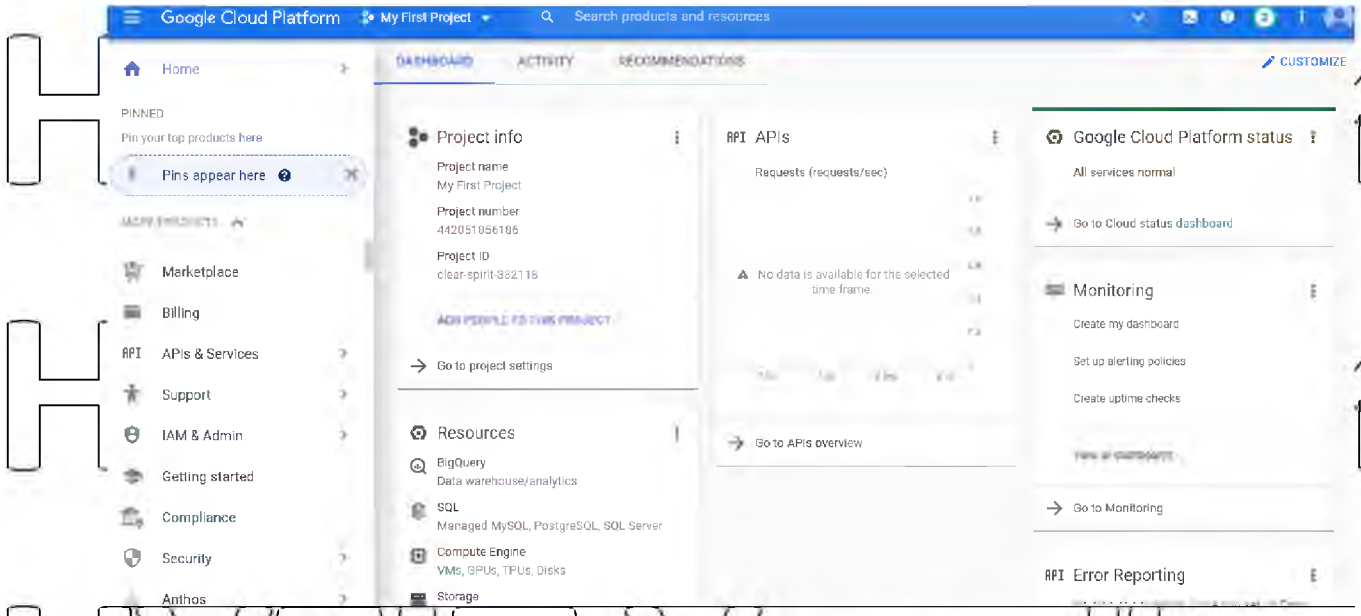

Рис.3.2 - Панель для адміністрування GCP

В панелі адміністрування переходимо в Compute Engine і створюємо нову віртуальну машину, через яку будемо здійснювати розгортання моделі захищеного НОД (рис.3.3).

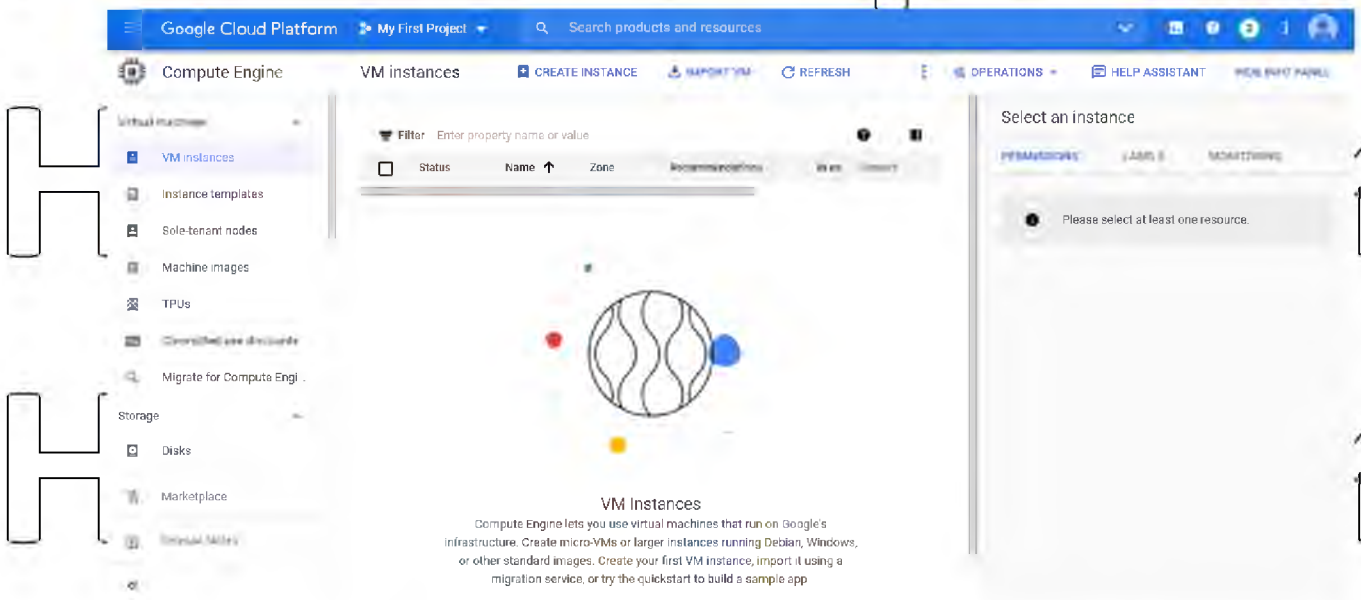

Рис.3.3 – створення віртуальної машини в Compute Engine

Задаємо необхідне ім'я віртуальної машини та її характеристики в розділі Compute Engine панелі GCP (рис.3.4).

Рис.3.4 – введення імені екземпляру віртуальної машини в розділі Compute Engine

Створення екземпляру віртуальної машини в хмарній платформі передує етапу розгортання образів реальних ОС та маршрутизаторів, отже, далі переходимо до цього процесу.

3.2 Створення образу та віртуальної машини Ubuntu

Для створення вкладеного образу побудованого на базі Ubuntu 16.04 необхідно спочатку активувати «Cloud Shell», натиснувши піктограму «Activate Cloud Shell».

Після цього у нижній частині сторінки відкриється панель термінала Cloud Shell. Для створення вкладеного образу необхідно виконати команду: «gcloud compute images create nested-ubuntu-xenial --source-image-family=ubuntu-1604-lts--source-image-project=ubuntu-os-cloud--licenses=https://compute.googleapis.com/compute/v1/projects/vm-options/global/licenses/enable-vmx.».

Після того як образ буде створено, термінал повідомить наступним повідомленням зі статусом «READY» (рис.3.5).

```
Created [https://www.googleapis.com/compute/v1/projects/rare-mechanic-281713/global/images/nested-ubuntu-xenial].
NAME                  PROJECT                FAMILY  DEPRECATED  STATUS
nested-ubuntu-xenial  rare-mechanic-281713                       READY
lukashenkodima53@cloudshell:~ (rare-mechanic-281713)$
```

Рис. 3.5 – Створення образу Ubuntu

Таким чином, створено перше програмне відображення – ОС Linux, на базі якого працює один із сервісів.

Створена і запущена віртуальна машина в дашборді має вигляд, наведений на рис. 3.6.

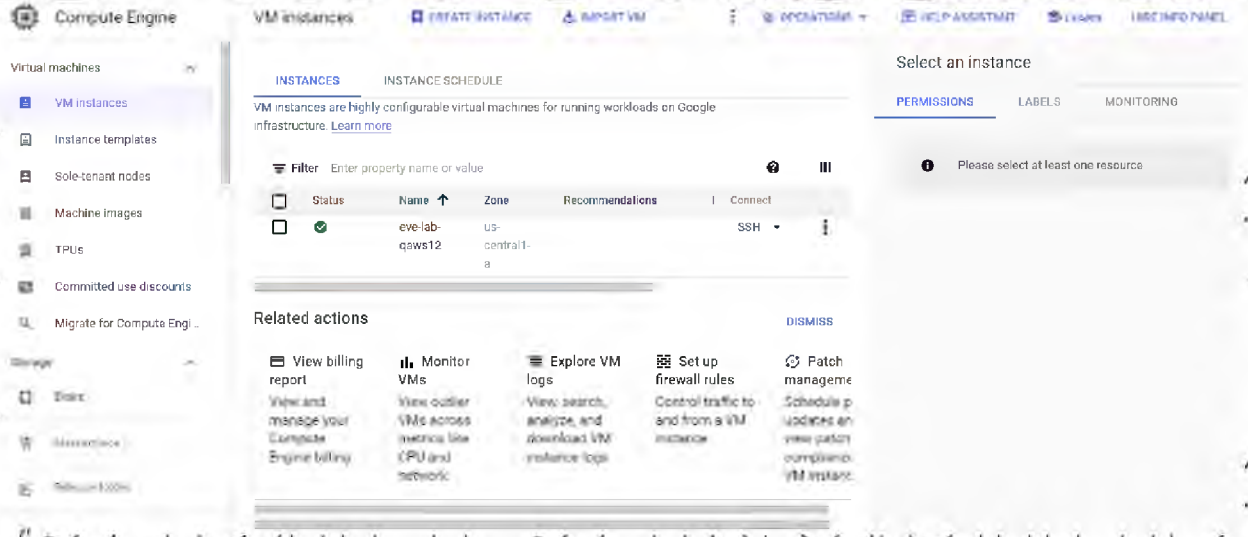

Рис.3.6 – Створена і запущена віртуальна машина в дашборді

Підключаємось до створеної віртуальної машини через SSH- з'єднання (рис.3.7).

Рис.3.7 – підключення до створеної віртуальної машини через ssh

Для налаштування диску натискаємо «Изменить», переходимо на вкладку «Пользовательские образы» і в полі «Образ» обираємо створений користувацький образ Ubuntu. Встановлюємо розмір диску в 100 Гб.

На завершальному етапі налаштування параметрів віртуальної машини встановлюємо «галочку» напроти пунктів «Разрешить трафик HTTP», «Разрешить трафик HTTPS» та натискаємо «Создать» (рис.3.8).

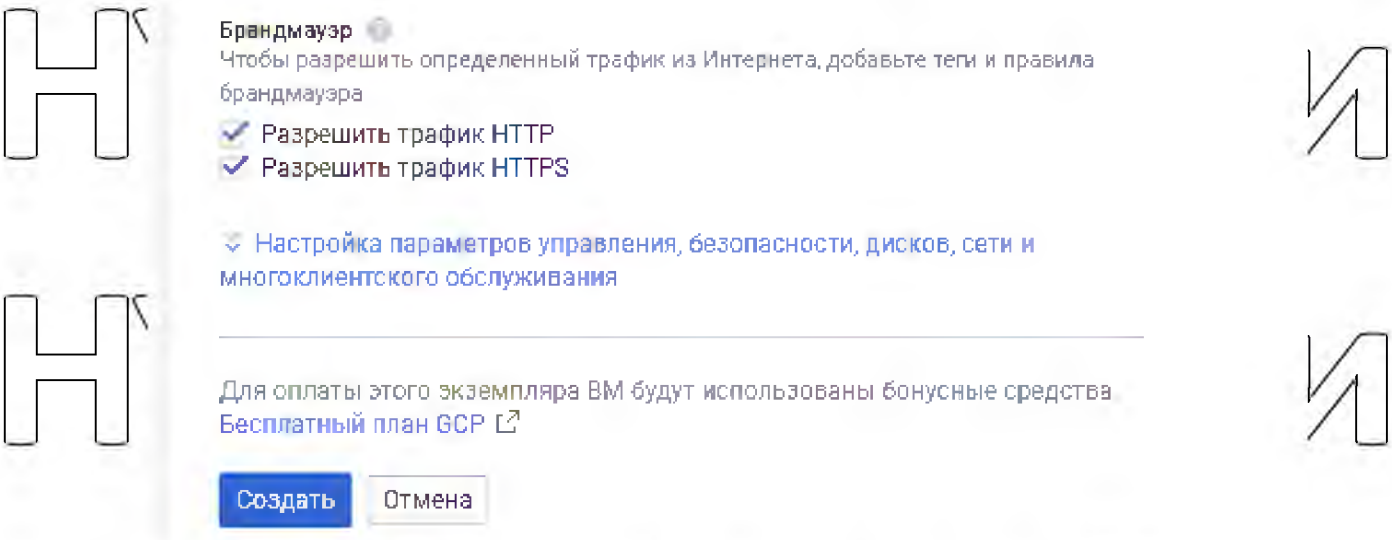

Рис. 3.8 – Налаштування завантажувального диску

3.3 Встановлення середовища моделювання eve-ng

Важливим є створення в хмарі елементів топології корпоративної мережі. Середовище віртуалізації eve-ng дозволяє створити топологію з використанням різних моделей маршрутизаторів - mikrotik, cisco тощо. В ньому існую можливість додавати сервери та багато іншого.

Для того, щоб встановити дане середовище та забезпечити його функціонування необхідно мати такі ресурси в хмарі:

1) можливість розгортання віртуальної машини
2) Вільне місце від 20 ГБ
3) Підтримка апаратної віртуалізації на рівні CPU (Intel-VT/AMD-V
4) ОЗП від 4 ГБ

Встановлюємо EVE NG (рис.3.9).

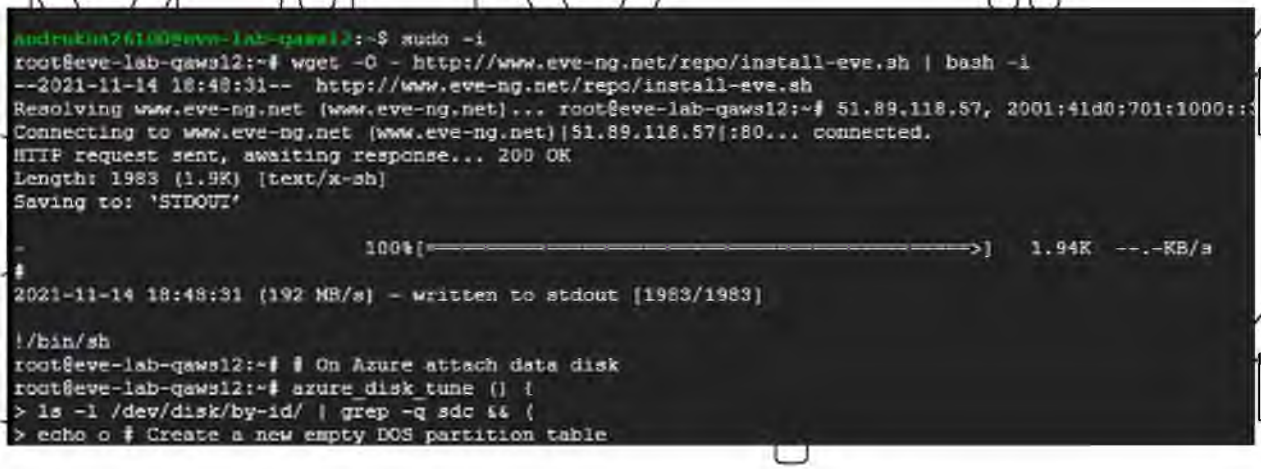

Рис.3.9 – Встановлення пакету EVE-NG

Запущена віртуальна машина із встановленим EVE-NG має вигляд, показаний на рис.3.10.

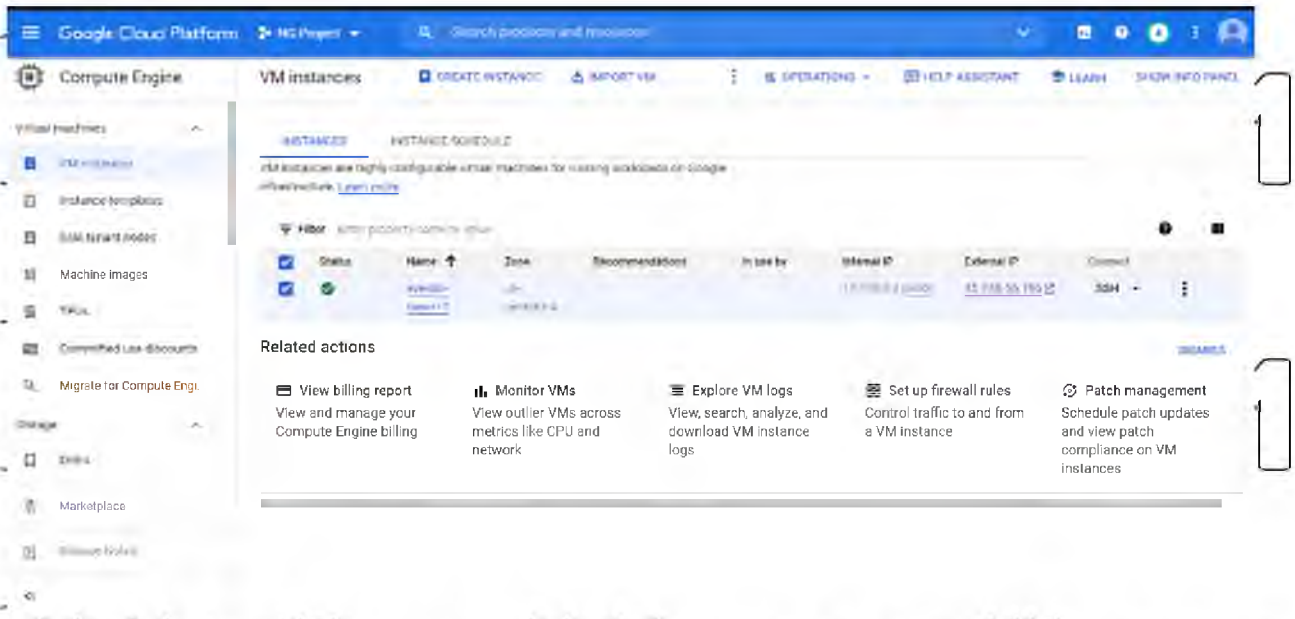

Рис.3.10 – Зовнішній вигляд запущеної віртуальної машини зі встановленим EVE-NG

Підключаємось через SSH-з'єднання до віртуальної машини для того щоб загрузити туди образи роутера та маршрутизатора (рис.3.11)

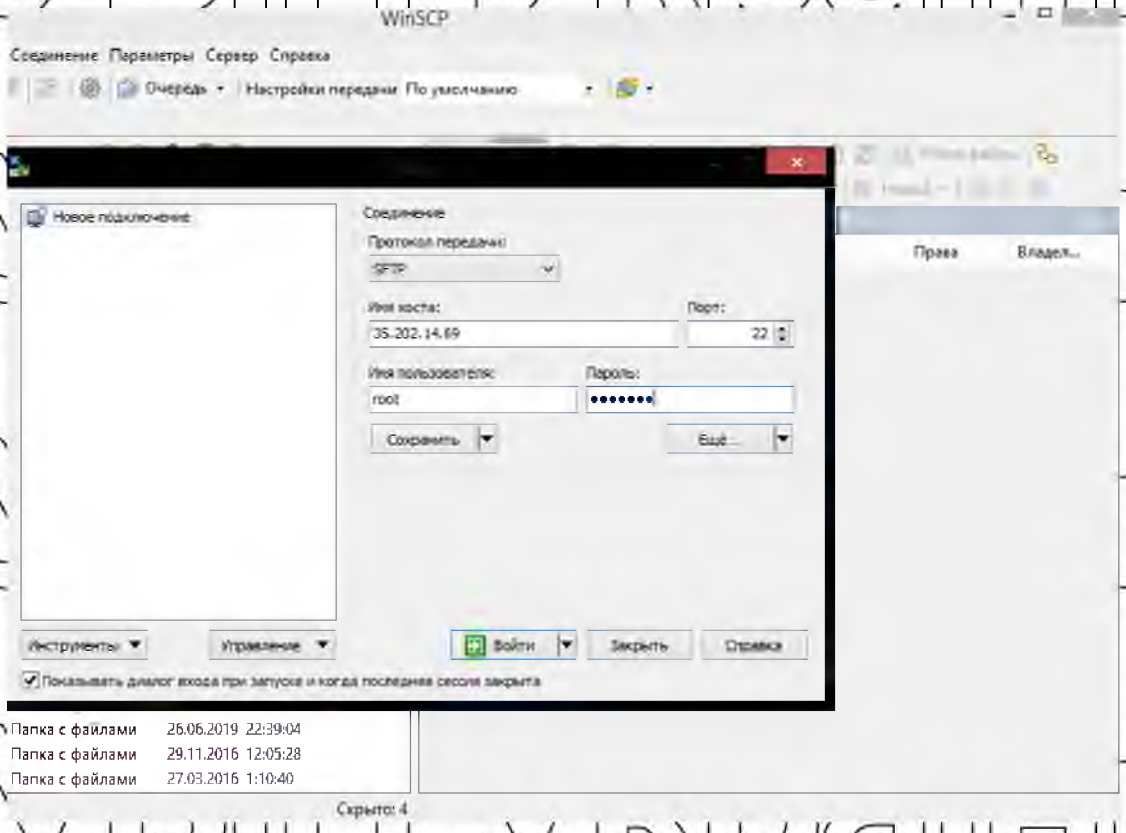

Рис.3.11 – Підключаємось через SSH-з'єднання до віртуальної машини

Генеруємо ліцензійний ключ для програми EVE-NG (рис.3.12).

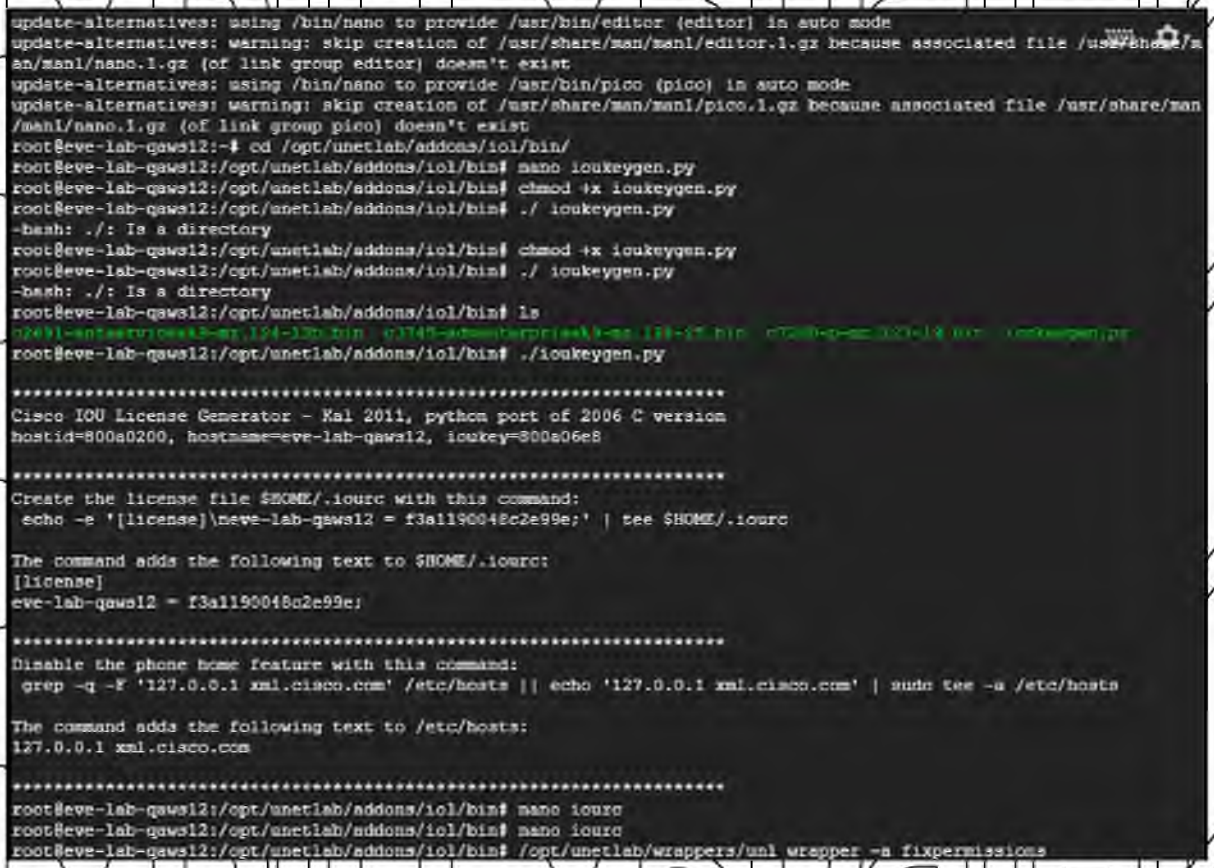

Рис.3.12 – Генерування ліцензійного ключа для роботи з EVE-NG

Взагалі, джерелом віртуальних образів маршрутизаторів виступають фірми – розробників тих чи інших моделей. Тому, перш за все – плануємо необхідно топологію мережевої інфраструктури, визначаємося з технологіями захисту, після чого переходимо до отримання даних образів. Такий образ являє собою файл, які містить повнофункціональну програмну модель-емуляцію апаратного пристрою з усіма необхідними комунікаційними інтерфесами, вбудованою ОС та іншими апаратними та програмними властивостями.

Вигляд каталогу із згенерованим ключем EVE-NG та завантаженими образами маршрутизаторів показаний на рис.3.13.

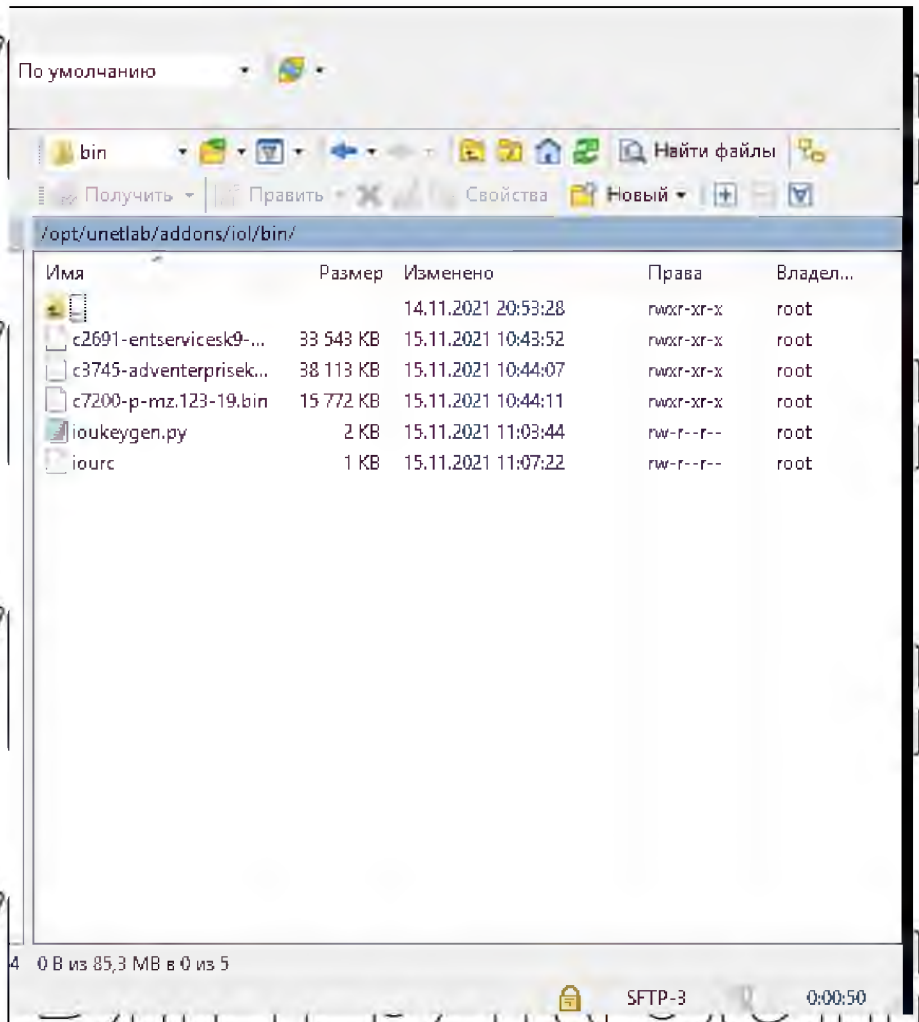

Рис.3.13 – Вигляд каталогу із згенерований ключем та завантаженими образами маршрутизаторів

В моделі хмарного ЦОД будемо використовувати soft-образи таких мережевих маршрутизаторів:

- маршрутизатор Cisco 2691 - модульний маршрутизатор для малих (до 20 осіб) і середніх (до 250 осіб) офісів. В даному маршрутизаторі передбачено можливість передачі голосу і факсових повідомлень. Пропонований до нього набір модулів дозволяє використовувати маршрутизатор Cisco 2691 в якості серверів доступу та міжмережевих екранів, для передавання голосу та факсів через мережі TCP/IP. Маршрутизатор Cisco 2691 має 2 порти Fast Ethernet, 2 слоти WAN, один слот для мережевого модуля та один слот для AIM модуля;

- серія маршрутизаторів Cisco 3700 призначена для віддалених офісів, які потребують високого рівня інтеграції сервісів. Він пропонує широкий набір мережевих та голосових інтерфейсів в одному пристрої. При використанні цієї платформи користувачі, завдяки високопродуктивним модулям розширення (HDSM) та сервісним модулям (AIM). Даний маршрутизатор інтегрує високопродуктивну маршрутизацію/комутацію за допомогою WAN з'єднань. Cisco 3700 надає рішення, здатне підтримувати велику кількість традиційних телефонних пристроїв спільно з пристроями IP-телефонії. Використання 16- або 36-портових EtherSwitch модулів з підтримкою Inline Power, аналогових та цифрових інтерфейсів, а також голосових можливостей Cisco IOS дозволяє поєднати окремі мережі PBX телефонії та передачі даних, об'єднавши їх в одну;

- маршрутизатор Cisco серії 7200 відносяться до класу провайдерських. Даний пристрій здатний забезпечувати швидкісний трафік інтернету (максимальний показник обробки сягає 2 млн. пакетів за секунду). За швидкість маршрутизації даних роутерів відповідає технологія Network Processing Engine G2. До базового функціоналу модельного ряду 7200 належать такі опції:

– забезпечення апаратного VPN-шифрування (здійснюється завдяки механізму VPN Services Adapter);

– великий асортимент конфігурацій;

– адаптація під інтерфейси від DS-0 до OC-3, а також оптимізація для роботи з такими сервісами як Fast Ethernet, Packet over SONET і Gigabit Ethernet.

Роутер має високу стійкість до відмов. З технічного заповнення маршрутизаторів серії 7200 виділяється технологія Cisco IP Next-Generation Network, що забезпечує користувачеві високий показник швидкості передачі. Також практично весь модельний ряд оснащений інтегрованим вбудованим сервісом мережі.

Переходимо до EVE-NG і авторизуємося в ній (рис.3.14). Після завантаження на екрані відобразиться вітання у вигляді IP адреси та рядком для введення логіну, а після пароля.

Після цього сервер повинен завантажитися повністю. Далі можна заходити на веб-інтерфейс по ip, з логіном «admin» з паролем «eve» (рис.3.14).

Рис.3.14 – вхід через веб-інтерфейс по ip в EVE-NG

Створюємо новий проект в EVE-NG для подальшого розгортання частини хмарної мережевої інфраструктури (рис.3.15).

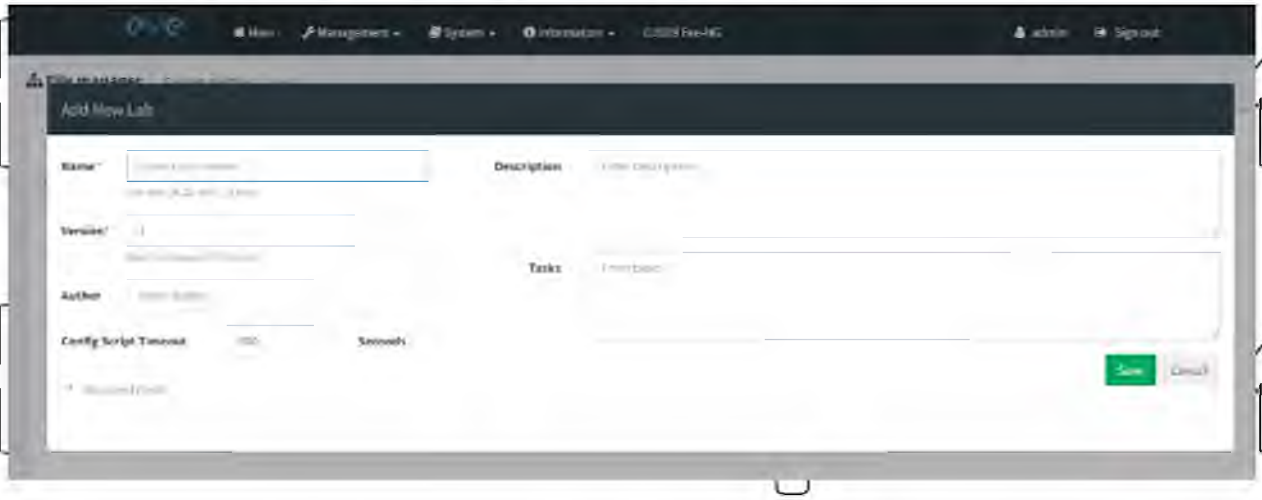

Рис.3.15 – створення нового проекту в EVE-NG

В новому проекті добавляємо об'єкти моделі хмарного ЦОД на робочу зону EVE-NG (рис.3.16).

Рис.3.16 – поле проекту EVE-NG для додавання soft-об'єктів НКС хмарного ЦОД

3.4 Встановлення образів ОС для серверів комутаційних вузлів ЦОД

Для побудови моделі хмарного ЦОД необхідно встановити образи маршрутизаторів внутрішньої інфраструктури даного ЦОД.

3.4.1 Встановлення образів Cisco IOL.

Образи Cisco IOU/IOL – це образи L2/L3 комутаторів і маршрутизаторів, які мають такі ж самі функції, що і оригінальні пристрої. Їх слід завантажити в директорію /opt/unetlab/addons/iol/bin/.

3.4.2 Windows 10 x64 та Windows Server 2016R

Встановлення Windows 10 x64 та Windows Server 2016R є ідентичним, виключаючи назви каталогів. Прикладом буде встановлення Windows 10 x64.

Для встановлення Windows 10 на сервері необхідно створити каталог за шляхом /opt/unetlab/addons/qemu/win-win10. Після створення каталогу потрібно завантажити образ з ОС Windows 10 і назвати його cdrom.iso. Після завантаження

образу необхідно створити віртуальний жорсткий диск та назвати його virtioa.qcow2 (рис.3.17).

```
root@shkurat:/opt/unetlab/addons/qemu# cd /opt/unetlab/addons/qemu/win-win10/
root@shkurat:/opt/unetlab/addons/qemu/win-win10# /opt/qemu/bin/qemu-img create -f qcow2 virtioa.qcow2 30G
Formatting 'virtioa.qcow2', fmt=qcow2 size=32212254720 encryption=off cluster_size=65536 lazy_refcounts=of
t_bits=16
root@shkurat:/opt/unetlab/addons/qemu/win-win10# ls
cdrom.iso  virtioa.qcow2
root@shkurat:/opt/unetlab/addons/qemu/win-win10#
```

Рис. 3.17 – Створення віртуального жорстокого диску

Можна приступити до самого встановлення Windows10 вже в самій лабораторії eve-ng. Встановлення схоже на інсталяцію ОС Windows 10. Відмінністю є вибір жорсткого диску, на який встановлюється ОС Windows. Для цього необхідно обрати «Загрузить», «Обзор», «Дисковод В»/storage/2003R2/amd64 або x86 (залежить від розрядності ОС).

Після завершення інсталяції вимикаємо віртуальну машину Windows та зберігаємо її. Для реалізації даного процесу необхідно дізнатись ідентифікатор роботи (у вкладці «Lab Details» - рис.3.18), POD ID

Рис. 3.18 – Ідентифікатор роботи

Якщо маніпуляція по ввімкненню або перезавантаженню віртуальної машини Windows здійснюється від імені адміністратора, то за замовчуванням він буде дорівнювати нулю. Також необхідно знати номер вузла (рис.3.19).

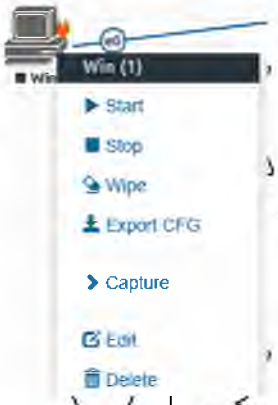

Рис. 3.19 – Ідентифікатор вузла

Перейшовши на сервер необхідно перейти в директорію вузла за допомогою команди cd. і зберегти зміни, які були внесені в вузл (рис.3.20).

Рис. 3.20 – POD ID

Завдяки цьому, на кожен вузол з ОС Windows не потрібно встановлювати ОС при його додаванні. Після збереження образу видаляємо образ cdrom.iso.

Змінюємо права доступу для всіх доданих образів за допомогою команди /opt/unetlab/wrappers/unl_wrapper -a fixpermissions (рис.3.21).

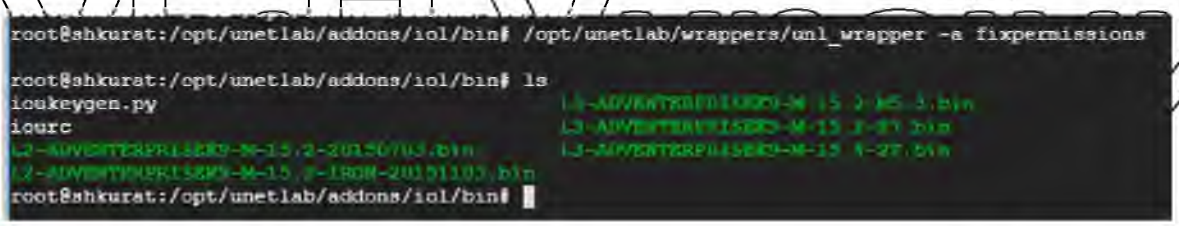

Рис. 3.21 – Зміна прав доступу

3.4.3 Встановлення образів vIOS

Встановлення образів – необхідний етап реалізації моделі ЦОД. Для цього використовується vIOS - сервер віртуального вводу-виводу [11]. vIOS це програма, розташована в логічному розділі. Дана програма полегшує спільне використання фізичних ресурсів введення-виведення між клієнтськими логічними розділами в межах одного сервера.

Для встановлення vIOS образів необхідно створюємо на сервері два каталоги viosl2-15 і vios-15. Після цього завантажуємо в створені каталоги образи і конвертуємо їх в *.qcow2 формат за допомогою команди /opt/qemu/bin/qemu-img convert -f vmdk -O qcow2 vIOS-L2.vmdk virtioa.qcow2 (рис.3.22). Після цього видаляємо файл з форматом *.vmdk.

```
root@shkurat:/opt/unetlab/addons/qemu/viosl2-15# cd /opt/unetlab/addons/qemu/vios-adventerprisek9-m.SPA.15
root@shkurat:/opt/unetlab/addons/qemu/vios-adventerprisek9-m.SPA.156-1.T# ls
vIOS-L2.vmdk
root@shkurat:/opt/unetlab/addons/qemu/vios-adventerprisek9-m.SPA.156-1.T# /opt/qemu/bin/qemu-img convert -
 qcow2 vIOS-L2.vmdk virtioa.qcow2
root@shkurat:/opt/unetlab/addons/qemu/vios-adventerprisek9-m.SPA.156-1.T# ls
vIOS-L2.vmdk  virtioa.qcow2
root@shkurat:/opt/unetlab/addons/qemu/vios-adventerprisek9-m.SPA.156-1.T# rm vIOS-L2.vmdk
root@shkurat:/opt/unetlab/addons/qemu/vios-adventerprisek9-m.SPA.156-1.T# ls
virtioa.qcow2
```

Рис. 3.22 – Конвертація образу в *.qcow2 формат

Змінюємо права на доступ для всіх доданих образів за допомогою команди /opt/unetlab/wrappers/unl_wrapper -a fixpermissions.

Після встановлюються в середовищі EVE-NG образи Cisco IOL. Під IOL мається на увазі IOS On Linux або, під IOU - IOS On Unix. IOL це симулятор Cisco, доступний тільки для внутрішнього використання [12,13,14].

Налаштування MAIN роутера

Необхідно налаштувати вхідні WAN-ліній від провайдерів для балансування навантаження сервісів хмарного ЦОД.

Спершу виконуємо ініціалізацію зовнішніх інтерфейсів маршрутизатора MAIN (рис.3.23)

```
main(config)#
main(config)#int
main(config)#interface
main(config)#interface e
main(config)#interface ethernet 0
main(config)#interface ethernet 0/
main(config)#interface ethernet 0/0
main(config-if)#de
main(config-if)#des
main(config-if)#description ISP1
main(config-if)#description ISP1
main(config-if)#ip
main(config-if)#ip
main(config-if)#ip na
main(config-if)#ip nat o
main(config-if)#ip nat outside
main(config-if)#
*Nov 17 19:02:34.680: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
main(config-if)#ex
main(config-if)#exit
main(config)#in
main(config)#interface e
main(config)#interface ethernet 0/1
main(config-if)#des
main(config-if)#description ISP2
main(config-if)#ip
main(config-if)#ip
main(config-if)#ip a
main(config-if)#ip ad
main(config-if)#ip add
```

Рис.3.23 - налаштування балансування вхідних WAN-ліній для 2х провайдерів на роутері MAIN

Для створеного у віртуальному емуляторі мережевому soft-середовищі закладаємо надмірність. Надмірність є одним з найважливіших аспектів для створюваного хмарного ЦОД на стороні глобальної мережі WAN (реалізується кількома каналами WAN, що сходяться на одному маршрутизаторі).

Найоптимальніший спосіб досягнення надмірності WAN на маршрутизаторі MAIN полягає у використанні надійних резервних статичних маршрутів з відстеження IP SLA [15].

IP SLA – це функція, включена в програмне забезпечення Cisco IOS, яка дозволяє аналізувати рівні обслуговування для IP додатків та сервісів, перевіряти якість обслуговування (QoS) на відповідність параметрам, та допомагає виявляти та локалізувати проблеми в каналах мережі. IP SLA

використовує технологію активного моніторингу трафіку (коли тестові пакети додаються до активного з'єднання) для моніторингу безперервності трафіку в компютерній мережі. В такому випадку маршрутизатори виступають в ролы IP SLA Responder, які забезпечують точність виміряних даних у мережі. IP SLA збирає інформацію про затримку, джиттер, втрату пакетів, їх шляхи, послідовність відправки та багато інших потрібних параметрів.

Маршрутизатор MAIN підключено до двох каналів WAN – ISP1 та ISP2. При використанні команди ip sla schedule 2 створюється трек, який відстежуватиме стан операції IP SLA. Якщо від IP-адреси наступного хопу немає відгуків на пінг, трек відключиться та почне працювати, коли SLA почне знову отримувати пінг-відповідь (рис.3.24)

```
main(config)#ip sla schedule 2 life forever start-time now
```

Рис.3.24 – створення каналу для відслідковування та балансування трафіку назовні

Маршрутизація на основі політик (policy based routing, PBR) дозволяє маршрутизувати трафік на підставі заданих політик, тоді як у звичайній маршрутизації, тільки IP-адреса одержувача визначає, яким чином буде переданий пакет. Параметр permit означає, що пакети, які потрапляють до опису match, будуть надіслані так як описано в set, тобто через балансування трафіку з перевіркою доступності IP 1.1.1.1 по каналу 123 за стандартною таблицею маршрутизації. Аналогічні налаштування виконується по каналу 124 балансування (рис.3.25).

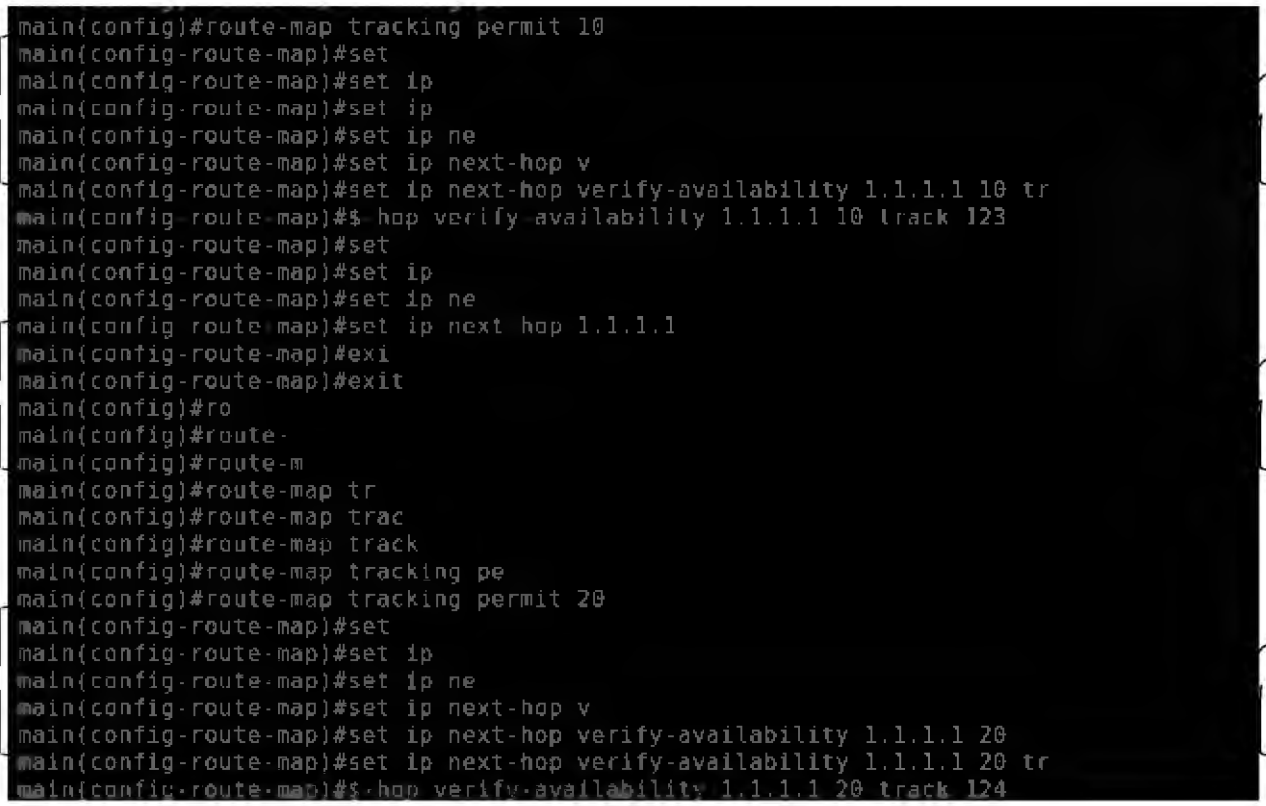

Рис.3.25 -

Перевіряємс роботу створеної системи балансування при нестабільному трафіку на лініях WAN від провайдерів ISP1 та ISP2. Для цього стану роботи зовнішнього каналу скористаємося командою sh ip sla statistics details (рис.3.26)

```
main#show ip sla statistics details
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 19:26:51 UTC Wed Nov 17 2021
Latest operation return code: Timeout
Over thresholds occurred: FALSE
Number of successes: 0
Number of failures: 47
Operation time to live: Forever
Operational state of entry: Active
Last time this entry was reset: Never



IPSLA operation id: 2
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 18:56:01 UTC Wed Nov 17 2021
Latest operation return code: Timeout
Over thresholds occurred: FALSE
Number of successes: 0
Number of failures: 52
Operation time to live: Forever
Operational state of entry: Active
Last time this entry was reset: Never
```

Рис.3.26 - перевірка роботи створеної системи балансування при нестабільному трафіку на лініях WAN від провайдерів ISP1 та ISP2

Налаштування мережевих інтерфейсів Ethernet0/0, Ethernet0/1 Ethernet0/2, Ethernet0/3, системи перенаправлення портів, алгоритмів шифрування для ssh-протокола клієнта і сервера віддаленого керування створеною в хмарі GCP мережевою емуляцією ІКС ЦОД показані на рис.3.27.

```
interface Ethernet0/0
 description ISP1
 ip address 10.10.0.1 255.0.0.0
 ip nat outside
 ip virtual-reassembly in
 no mop enabled
!
interface Ethernet0/1
 description ISP2
 ip address 102.10.2.1 255.0.0.0
 ip nat outside
 ip virtual-reassembly in
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
ipv6 ioam timestamp
!
```

Рис.3.27 – налаштування інтерфейсів мережі, протоколі та системи перенаправлення портів

Після налаштування інтерфейсів мережі, протоколі та системи перенаправлення портів сегмент мережі LAN2 буде маршрутизуватися, як одна мережа.

Налаштування роутера Office2

Створюємо та конфігуруємо сабінтерфейс для роутера Office2. Для цього обираємо логічний інтерфейс Ethernet 0/1.2. (рис.3.28). Налаштовуємо інкапсуляцію магістрального з'єднання як dot1q. (802.1Q – стандарт IEEE). Далі перевіряємо правильність налаштування даного транку (рис.3.28).

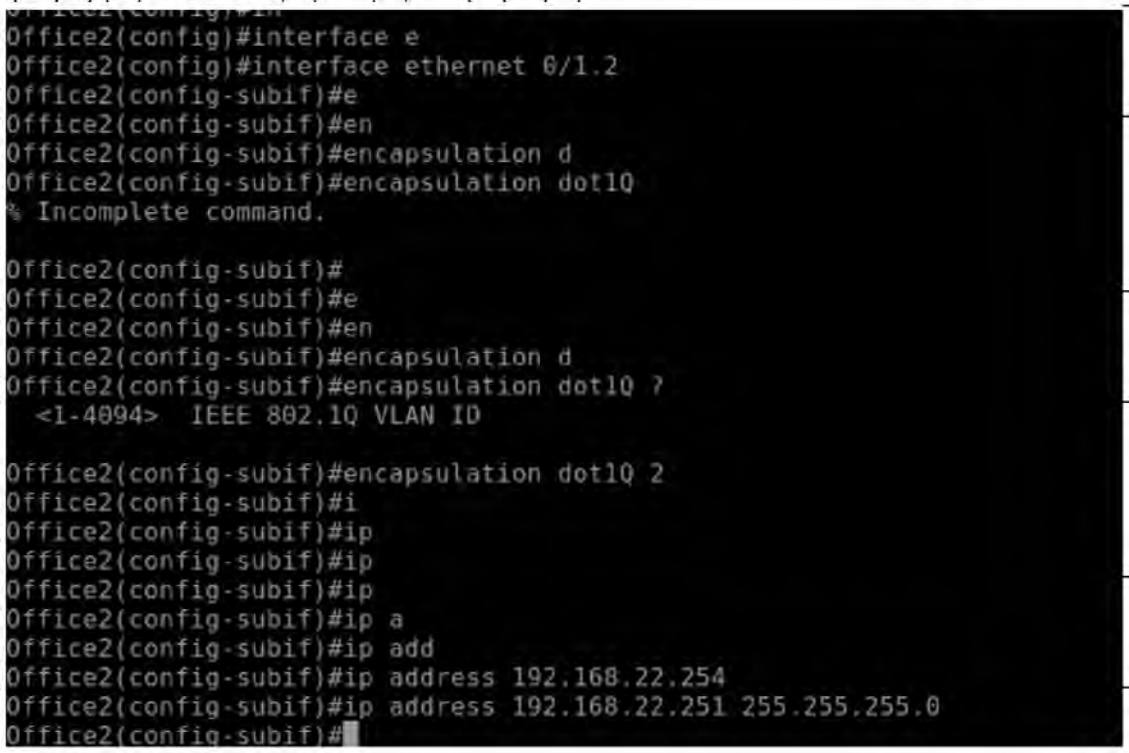

Рис.3.28 - Створення та конфігурування сабінтерфейсу для роутера Office2

Налаштовуємо тунелювання порту. В даному випадку використовуються тунелювання по стандарту 802.1Q для підтримки цілісності VLAN клієнта в мережі постачальника послуг. Налаштовуємо тунельний порт на граничному комутаторі MAIN в мережі постачальника послуг і підключаєте його до магістрального порту 802.1Q на інтерфейсі маршрутизатора, створюючи асиметричне посилання. Тунельний порт належить до однієї VLAN, яка призначена для тунелювання.

Таким чином, налаштування soft-емуляції комунікаційної інфраструктури захищеного ЦОД заверешно. Далі необхідно перейти до розгортання сервісів ЦОД в хмарі GCP.

3.7 Розгортання сервісів ЦОД в хмарі

Для того, щоб створена модель почала виконувати функції з обробки даних необхідно розгорнути в ній необхідні програмні додатки.

Використаємо програму Docker для розгортання додатків, що реалізують функції обробки даних в хмарному ЦОД. Даний інструмент призначений для управління ізольованими контейнерами в ОС Linux. Docker має засоби, які дозволяє керувати контейнерами на рівні ізоляції процесів.

Таким чином, програма Docker дозволяє запускати довільні процеси в режимі ізоляції, після чого переносити та клонувати сформовані для них контейнери в яких розміщені CMS WordPress. Таким чином, Docker створює, обслуговує і підтримує контейнери.

3.7.1 Вмикаємо віртуальну машину Windows, необхідну для роботи Docker for Windows (рис.3.29).

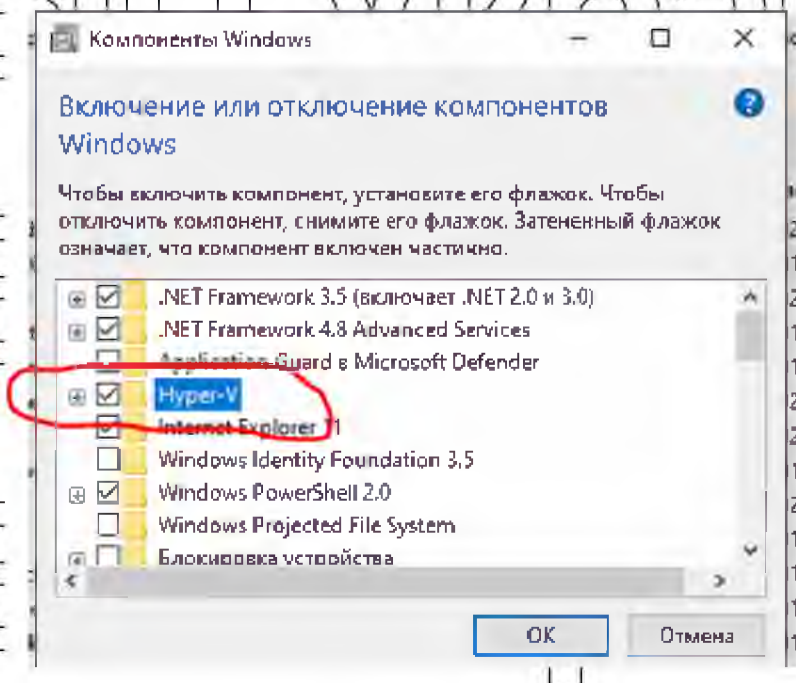

Рис.3.29 - ввімкнення системи віртуалізації в панелі налаштувань Windows

Для встановлення CMS WordPress в Dockers достатньо запустити його в docker командою:

docker run --name love-wordpress -p 8080:80 -d wordpress

Після створення віртуального контейнеру з його образу відкриваємо wev-браузер та переходимо за посиланням http://localhost:8080, та отримуємо доступ до WordPress (рис.3.30). Тестування доступу до CMS Інтернет-магазину, таким чином відбулося успішно.

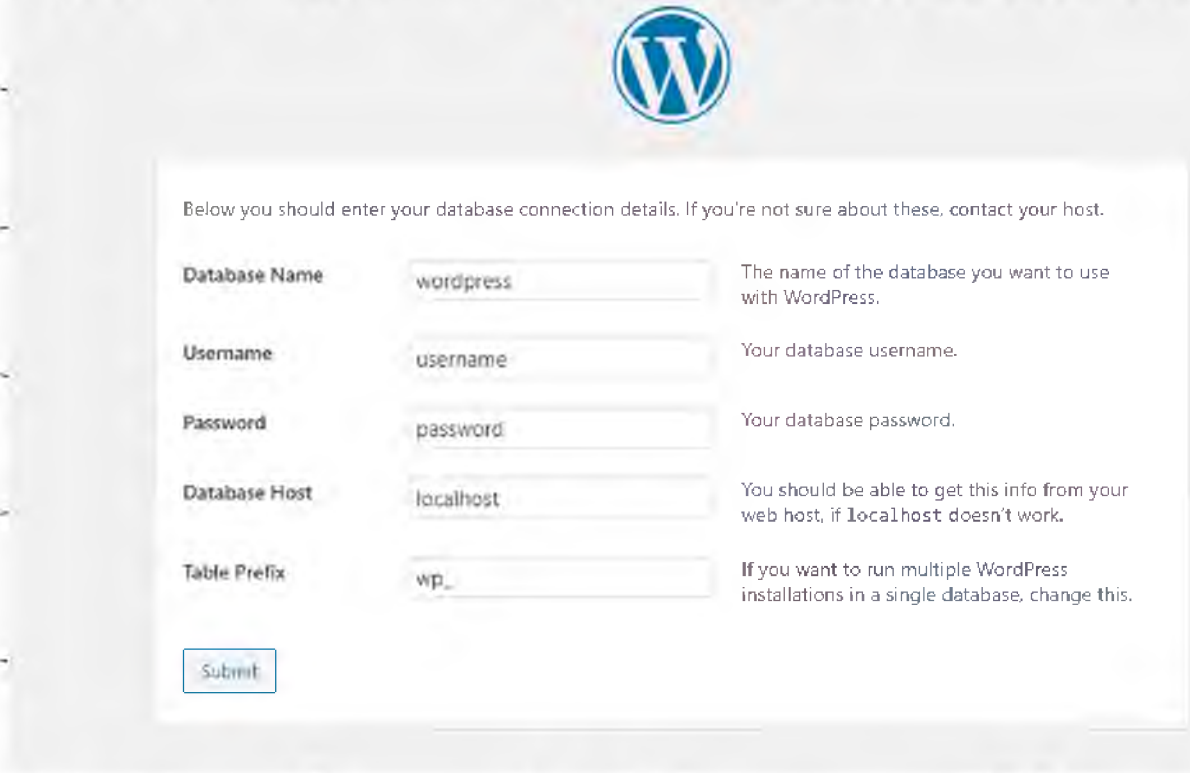

Рис. 3.30 – запущений з віртуального контейнера в Docker CMS WordPress

Аналогічним чином проводимо встановлення з існуючих віртуальних контейнерів інші необхідні додатки, які забезпечують роботу корпоративного ЦОД та налаштовуємо супутні сервіси в хмарі.

ЗАГАЛЬНІ ВИСНОВКИ

В ході виконання роботи було досягнуто мету – вивчення та дослідження технологій захисту хмарного захищеного ЦОД з використанням віртуалізації. Для цього було проведено:

- аналіз структури та задач хмарних сервісів для центрів обробки даних, характерних для конкретної інформаційно-комунікаційної системи інтернет-магазину;
- визначено тип та склад хмарного середовища для реалізації технологій захисту мережевого трафіку, яке належить до дослідження;
- обрано цільову платформу - GCP для розміщення віртуальної інфраструктури ЦОД інтернет-магазину та технологію віртуалізації EVE-NG;
- проведено практичну реалізацію моделі хмарного захищеного ЦОД та розгорнутий тестовий сервіс WordPress для функціонування інтернет магазину в середовищі віртуалізації;
- реалізовано та досліджено хмарну технологію захисту конфіденційності і цілісності інформації в рамках створеної PaaS платформи, яка базується на програмно апаратних рішеннях Cisco.

За результатами дослідження можна зробити висновок про те, що зараз захист даних у хмарі відбувається на всіх рівнях архітектури:

- в інфраструктурі;
- в програмному забезпеченні та операційних системах;
- обчислювальних ресурсах віртуальних машин платформи.

Незважаючи на те, що в Україні існують регламентуючі документи щодо безпеки хмарних сервісів, користуватися лише методами з ДСТУ не можна — вони не враховують останніх змін у сфері таких технологій, розгортання та загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Чим VPS відрізняється від VDS? [Електронний ресурс] // Блог HyperHost – Режим доступу до ресурсу: https://hyperhost.ua/info/uk/chim-vps-vidriznyaetsya-vid-vds.

2. *Mell, Peter and Grance, Timothy.* The NIST Definition of Cloud Computing (англ.). *Recommendations of the National Institute of Standards and Technology*. NIST (20 October 2011). Дата звернення 6 листопада 2011. Архівовано 21 березня 2012 року.

3. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. — L.: Springer, 2010. — 379 p. — (Computer Communications and Networks). — ISBN 9781849962407.

4. VPS-хостинг и облачный хостинг: что выбрать и в чем разница? [Електронний ресурс] // «Habr». – 2015. – Режим доступу до ресурсу: https://habr.com/ru/company/ruvds/blog/320880/.

5. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005 -99. ДСТСЗІ СБ України. Київ. – 21 с., 1999.

6. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004 -99. ДСТСЗІ СБ України. Київ. – 61 с., 1999.

7. Harvey C. AWS vs. Azure vs. Google Cloud: 2021 Cloud Platform Comparison [Електронний ресурс] / Cynthia Harvey // TechnologyAdvice – Режим доступу до ресурсу: https://www.datamation.com/cloud/aws-vs-azure-vs-google-cloud/.

8. Google Cloud Free Program. Compare AWS and Azure services to Google Cloud [Електронний ресурс] // Carbon neutral. - August 31, 2021. – Режим доступу до ресурсу: https://cloud.google.com/free/docs/aws-azure-gcp-service-comparison.

9. EVE-NG Community Cookbook. Режим доступу до сайту: https://www.eve-ng.net/index.php/documentation/community-cookbook/

10. Simonsson, Jesper; Zhang, Long; Morin, Brice; Baudry, Benoit; Monperrus, Martin (2021). "Observability and chaos engineering on system calls for containerized applications in Docker". *Future Generation Computer Systems*. **122**: 117–129. arXiv:1907.13039. doi:10.1016/j.future.2021.04.001.

11. Додавання Vios образів. Режим доступу до сайту: http://blog.netskills.ru/2016/07/10-unetlab-cisco-vios.html

12. Додавання образів Cisco IOL. Режим доступу до сайту: https://networkhunt.com/how-to-add-cisco-iou-iol-to-eve-ng/.

13. Додання Dynamips образів. Режим доступу до сайту: https://www.eve-ng.net/index.php/documentation/howtos/howto-add-cisco-dynamips-images-cisco-ios/

14. Як створити власний хост для Windows EVE. Режим доступу до сайту: https://www.eve-ng.net/index.php/documentation/howtos/howto-add-cisco-dynamips-images-cisco-ios/

15. IP SLAs Configuration Guide, Cisco IOS Release 15M&T. Chapter: Configuring IP SLAs ICMP Echo Operations [Електронний ресурс] // Cisco Inc – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_icmp_echo.html.