НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Кафедра комп'ютерних інтелектуальних систем та мереж

КОЧ Імам Меліх

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

ХМАРНІ СХОВИЩА ДАНИХ

Спеціальність 123 – Комп`ютерна інженерія

Спеціалізація – Комп'ютерні системи та мережі

Керівник: Тішин П.М, к.ф-м.н, доцент

Одеса – 2022

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

КОЧ Імам Меліх
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи)__ Хмарні сховища даних

керівник проекту (роботи)____Тішин П.М. к.ф-м.н, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ректора ОНПУ від "_06__"___06___2022_ року №_187-в__

2. Строк подання студентом проекту (роботи)___13.06.2022

3. Вихідні дані до проекту (роботи)_завдання на розробку

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)__1 Сервіси зберігання даних

2 Завдання на розробку

4 Мережева структура хмарного сховища даних

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Розподілене зберігання даних, Інформаційна структура мережі, Загальна логічна структура мережі, Структура сегменту віртуального хостінгу, Структура мережі віртуальних серверів, Мережа NOC та SOC, Структура серверів віртуального хостінгу

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Сервіси зберігання даних		
2	Завдання на розробку		
3	Мережева структура хмарного сховища даних		

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ _____
(підпис) (прізвище та ініціали)

Відомість кваліфікаційної роботи бакалавра

№ рядка	Найменування	Кільк.	Примітка
1	Пояснювальна записка	40	
2	Розподілене зберігання даних	1	
3	Інформаційна структура мережі	1	
4	Загальна логічна структура мережі	1	
5	Структура сегменту віртуального хостінгу	1	
6	Структура мережі віртуальних серверів	1	
7	Мережа NOC та SOC	1	
8	Структура серверів віртуального хостінгу	1	
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

				АМДП.АМ181.1026		
Зм. Лист	*№ докум.*	*Підпис*	*Дата*			
Розробив	Коч Імам Меліх			Хмарні сховища даних	*Літ.*	*Лист* 1 / *Листів* 1
Перевірив	Тішин П.М					
Реценз.					НУ«ОП» КІСМ	ІКС АМ181
Н. Контр.						
Затвердив						

АНОТАЦІЯ

Коч Імам Меліх. Хмарні сховища даних – кваліфікаційна робота бакалавра. Одеса, 2022: 40с., 7 рис., 10 джерел.

В кваліфікаційній роботі представлено розробку мережі сховища даних для розгортання серверної інфраструктури, яка реалізує сервіси для клієнтів організації. Особливу увагу приділено серверам мережі, так як різні мережеві сервіси вимагають різноманітного апаратного та програмного забезпечення. З точки зору мережі, реалізовано внутрішні сервіси для забезпечення функціонування хостінгу, такі як моніторинг, поштова система, dns система, фільтрація трафіку та інші захисні заходи.

В ході проведення проектування було розроблено мережеві структури сховищ даних, такі як інформаційна структура, логічна структура та інші, які дозволяють визначити організаційну структуру організації та визначити основні принципи сегментації мережі. Сегментація мережі була виконана з використанням механізмів віртуалізації мереж, що дозволяє ізолювати фізичні та логічні об’єкти сховищ даних.

ХМАРНІ СХОВИЩА ДАНИХ, ВІРТУАЛЬНИЙ ХОСТІНГ, ВІРТУАЛЬНІ СЕРВЕРИ, МЕРЕЖЕВІ СЕРВІСИ, ДАТА-ЦЕНТРИ, КОМП’ЮТЕРНІ МЕРЕЖІ

ABSTRACT

Koch I.M Cloud storage - bachelor's thesis. Odessa, 2022: 40p., 7 pic., 10 sources.

The qualification work presents the development of a cloud storage network for the deployment of server infrastructure that implements services for customers of the organization. Particular attention is paid to network servers, as different network services require a variety of hardware and software. From the network point of view, internal services have been implemented to ensure the functioning of the hosting, such as monitoring, mail system, dns system, traffic filtering and other security measures.

During the design, network structures of the cloud storage were developed, such as information structure, logical structure and others, which allow to determine the organizational structure of the organization and to determine the basic principles of network segmentation. Network segmentation was performed using network virtualization mechanisms, which allows to isolate the physical and logical objects of the cloud storage.

CLOUD STORAGE, VIRTUAL HOSTING, VIRTUAL SERVERS, NETWORK SERVICES, DATA CENTERS, COMPUTER NETWORKS

ЗМІСТ

ВСТУП

В сучасних умовах, всім організаціям, від маленьких підприємств до великих корпорацій, необхідно використовувати інформаційні технології, які розширюють можливості бізнесу. Використання таких технологій вимагає в наявності певної інфраструктури:

– комп'ютерна мережа. Забезпечує об'єднання пристроїв в єдину інфраструктуру (принтери, сканери, комп'ютери, сервери та інше);

– сервери. Використовуються для розгортання сервісів та проектів організації;

– мережеве обладнання. Використовується для комутації, маршрутизації та забезпечення захисту трафіку між пристроями;

– обслуговуючий персонал. Забезпечує діяльність усіх зазначених вище компонентів.

Для забезпечення всього вище зазначеного, керівництво організації повинно здійснити фінансові витрати на закупівлю обладнання, проектування структури системи, підтримку спроектованої системи та багато іншого. Все це вимагає суттєвих витрат як грошей, так і часу. До того ж, важко передбачити усі ситуації, в яких буде функціонувати інформаційна система:

– зовнішні фізичні впливи (переривання живлення, природні катаклізми);

– зовнішні втручання (вірусні атаки, хакерські атаки);

– внутрішні проблеми (вихід з ладу обладнання, помилки при налаштуванні).

Все це призводить до великих витрат та складнощів обслуговування системи, яка при цьому необхідна для організації.

В таких випадках, дуже часто, адекватним рішенням є перенести частину відповідальності за підтримку системи третім особам, що зменшує навантаження на організацію. Третіми особами в даному випадку можуть виступати спеціальні сховища та дата-центри, які спеціалізуються на наданні широкого спектру послуг, серед яких найчастіше всього зустрічається наступне:

- віртуальний хостінг для розміщення веб-сайтів клієнтів;
- віртуальні сервери для надання ізольованих операційних систем;
- виділені сервери для надання повноцінного серверу в оренду;
- поштові сервіси для реалізації корпоративної пошти;
- доменна система для використання власних доменних імен;
- віртуальна телефонія;
- захист інформації та інше.

При організації співпраці компанії та дата-центру, як правило, виграють обидві сторони, так як компанія економить витрати бюджету на підтримку інфраструктуру та найм співробітників, необхідність аналізувати ризики інформаційної та інших загроз.

Виходячи з цього, проектування та використання дата-центрів завжди буде актуальними задачами мережевих інженерів та адміністраторів, мати спрос та клієнтів. Організаціям не треба витрачатись на дороге обладнання та кваліфікованих співробітників, тому що структура системи винесена за рамки організації до хмарних сервісів або віддалених мереж і керівництву необхідно лише організувати віддалене використання сервісами та проектами компанії.

1 СЕРВІСИ ЗБЕРІГАННЯ ДАНИХ

1.1 Основні поняття та визначення

Хостинг сервіс провайдер – компанія, що надає послуги з розміщення серверного обладнання, даних та сайтів на своєму технологічному просторі . Також такі компанії можуть називатись хостер, хостинг, веб-хостер, дата-центр, сховище даних.

Основний напрям діяльності[1]:

– розміщення устаткування на власних технічних платформах з забезпеченням стабільного та надійного підключення до глобальної мережі з високою пропускною здатністю, та його обслуговуванням;

– надання послуг виділеного серверу повноцінне володіння сервером з ОС;

– надання послуг віртуального виділеного серверу – забезпечення виділеної частини дискового простору на сервері та фіксовані ресурси. Власник отримує права адміністратора та самостійно керує сервером;

– надання послуг віртуального хостингу – забезпечення серверів, де зберігається багата кількість сайтів, власники подібних мають однакові права та обов’язки;

– послуги з збереженням даних;

– реєстрація доменних імен та подібне.

Основні характеристики, що визначають технічну якість послуг компанії:

– постійна доступність усіх вузлів в мережі;

– зв’язок із глобальною мережею та стабільність роботи із зовні;

– забезпечення фізичної та інформаційної безпеки устаткування та даних;

– вдосталь надання ресурсів для функціонування віртуального серверу;

– забезпечення потрібних умов безпечного функціонування[1].

Поняття віртуалізації – це як набір обчислювальних ресурсів і їх логічного з'єднання, абстраговане від апаратної реалізації та забезпечує при цьому логічну ізоляцію обчислювальних процесів, що виконуються на одному фізичному ресурсі.[2]

Віртуальна машина – ізольований програмний контейнер, де є власна ОС та програми, що замінює собою фізичний пристрій, програмна середа, що надає ресурси.

Гіпервізор – це вузькоспеціалізований пристрій. Він менший за ОС загального застосування але більш спеціалізований, не виконує сторонньої роботи. Можливості використання віртуалізації: повна на рівні серверів, на рівні ОС, на рівні мереж, на рівні додатків, на рівні робочого місця, на рівні сховищ.

Віртуалізація серверів – завантаження на одному устаткуванні кілька логічних одиниць – віртуальних машин, які будуть повністю повторювати роботу незалежних фізичних серверів.

Методи віртуалізації серверів у працях [2]-[4]:

– Повна віртуалізація – виконується ОС без усяких модифікацій, створюється та підтримується повна віртуальна система. Переваги – легкість в налаштуванні віртуальних машин між серверами з різними різними фізичними конфігураціями. Недолік – втрати продуктивності.

– Власна віртуалізація – залежить від архітектури віртуалізації процесору. Нові процесори мають нові режими виконання та структури даних, які добре працюють с віртуальною машиною. Переваги – від спрощення архітектури до збільшення продуктивності.

– Паравіртуалізація – потрібна модифікація гостьових ОС для звернення віртуальних машин до гіпервізорів.

Віртуалізація на рівні ОС – підтримка ОС устаткування кілька ізольованих розділів. Можлива при допомозі мультиплексування доступу до ядра.

Віртуалізація на рівні ядра ОС – використання одного ядра для створення незалежних паралельних операційних середовищ.

Віртуалізація мереж – налаштування та створення фізичної мережі програмними засобами. По надійності та можливостям використання схожі з фізичними, але мають переваги: незалежність від обладнання, швидка ініціалізація, можливість розвертки безперервної роботи, автоматизоване обслуговування та підтримка додатків. Забезпечують підключення робочих завантажень до логічних мережевих пристроїв та служб: логічні порти, комутаційне обладнання, захисні екрани, приватні мережі, засоби балансування навантажень и тд [5].

Віртуалізація додатків – технологія розділення та ізоляція додатків у клієнта. Додатки ізолюються у віртуальної середі між ОС та стеком додатків. Принцип дії доволі простий: віртуальна середа завантажується до додатку, відокремлює його від інших додатків та ОС. Додатки можуть зчитувати інформацію з локальних ресурсів, но запис у віртуальній середі.

Віртуалізація представлень та робочих місць – емуляція інтерфейсу користувача. Користувач працює с додатком на власному терміналі. Це дозволяє відокремити ПЗ користувача від апаратної частини.

Віртуальний робочий стіл – дозволяє керувати ресурсами комп’.тера кінцевих користувачів. Може бути така віртуалізація статичною (фізичний ПК замінюється віртуальним) або динамічною (підключення до одного з можливих робочих столів).

Віртуалізація сховищ – підтримують швидку ініціалізацію щоб розгорнути ефективні сховища с тією же швидкістю, що і віртуальна машина. Ціллю такої віртуалізації є підвищення продуктивності без придбання додаткового обладнання для збереження даних. Забезпечує ефективне керування ресурсами сховища у віртуальній інфраструктурі та має переваги.

Docker – організовує всі параметри керування в формат образу, що переноситься та забезпечує цілісність, вказує взаємозалежності, мережеві підключення, сховища та базові зв’язки. Надає типові набори інтерфейсів та елементів керування що забезпечує їх взаємодію друг із другом, але при цьому ізолює робоче навантаження друг друга та регулює використання контейнерами ресурсів. Також керує елементами безпеки [6].

1.2 Основні критерії

Основним критерієм типових компаній, що надають подібні послуги є визначення операційних систем. Оскільки це дає уяву, яке встановлюється програмне забезпечення, що буде використовуватись та за допомогою якого буде підтримуватись функціональність усіх сервісів.

Далі з критеріїв визначаються служби та можливості, а саме підтримка стандартів інтерфейсів для роботи зовнішніх програм для зв’язку з веб-сервером. Завдяки цьому буде організований шлюз для таких робот.

Не менш важливим критерієм є підтримка СКБД – систем керування базами даних.

Якісні критерії. Це ті характеристики що визначають якість наданих послуг, а саме ресурси процесору, пам’яті, пропускна здатність. Такі характеристики дають уяву про швидкодію серверу та завантаження інформації. Ці характеристики відповідають за роботу дата-центру в цілому.

Кількісні критерії компанії. Це критерії, які можна оцінити в кількісному значенні. Такі як:

- розмір дискового простору;
- кількість трафіку;
- кількість сайтів;
- кількість користувачів;
- кількість поштових клієнтів та об’єм пам’яті;
- кількість баз даних;

– кількість оперативної пам’яті та паралельних процесів.

1.3 Переваги розгортання служб зберігання даних

Підтримка сайтів та обладнання на якому розміщені дані здійснюється не самим користувачем, а службами зберігання даних – дата-центрами. Користуючись їх послугами, користувач позбавляється додаткових затрат, таких як, придбання устаткування, його розміщення та його профілактика.

Друга, не мало важлива перевага, це налаштування та робота користувача зі своїми даними. Користувачу надається панель адміністратора, де він може керувати даними, файлами, почтовими клієнтами, доступом до хостингу, зв’язок з службою підтримки та багато інше.

Але, як і у будь якої інформаційної системи, є недоліки. Основним з яких є особливість використання такої технології як розміщення кілька ресурсів на загальному, вже налаштованому сервері. Немає можливості у користувача встановлювати своє ПЗ. Але в великої кількості користувачів це не має значення. А коли потрібно більше свободи користувачу, то йому надається виділений сервер.

1.4 Безпека даних в дата-центрах

Подібні системи та центри найчастіше піддаються атакам ззовні. Тому найважливішим фактором при розробці є організація заходів безпеки. Потрібно визначити спочатку які риски та атаки існують.

Риски компрометації гіпервізорів віртуальних машин. Якщо даний вузол системи не надійний, то зловмисник в першу чергу буде його атакувати. А подібні атаки призведуть до порушень системи. Висновки – потрібно додаткові рівні ізоляції мережі та посилені міри моніторингу безпеки. На звичайні гіпервізори важко проводити атаки із-за їх спеціалізації. Але, якщо

такий факт трапиться то призведе до великих руйнувань хоча ймовірність мала [7].

Риск для безпеки, коли виділяються та вивільнюються ресурси, наприклад, сховища, що відносяться до віртуальних машин. Даний процес супроводжується записом даних до фізичної пам’яті, а якщо її не вивільнити, то є можливість компрометації даних. Висновок – контролювати використання ресурсів зберігання та пам’яті при роботі в хмарних сховищах.

Риск в можливості не визначити атаку між віртуальними машинами на одному фізичному пристрої. Висновок – використовувати фільтрації трафіку та захисні мережеві екрани. Це можна зробити завдяки використанню та керуванням вбудованих функцій гіпервізорів: віртуальні комутатори та брандмауери, що знаходяться між фізичними інтерфейсами серверу та віртуальними інтерфейсами віртуальних машин. А також використання віртуальних локальних мереж для ізоляції трафіку віртуальних машин. Але виникає недолік в масштабованості функціональності віртуальних ЛОМ за край існуючих границь для підтримки великих за розміром хмар.

Риск безпеки даних при використанні технології Docker – це достовірність образів. Є можливість виправити та оновити образ, що говорить о незахищеності елементів образу. Тому може бути порушення роботи контейнеру, витік даних або помилкова робота, що нашкодить.

1.5 Виявлення вторгнень

Це задача організувати безпеку інформації та даних при забезпеченні захисту від атак. Такий процес є превентивною мірою ідентифікації активних загроз за допомогою сповіщення, що зловмисних атакує та збирає інформацію, необхідну для проведення атаки.

Є два типи виявлення вторгнень: вузлові (знаходиться на окремому вузлі та відстежує признаки атак на вузол) та мережеві (знаходяться на окремій системі, відстежують мережевий трафік на існування атак).

Для того, щоб було можливо виявляти вторгнення потрібно розуміти які типи атак можуть бути. Атаки модифікації – це спроба змінення інформації – вона здійснюється повсюди де існує та передається інформація, та направлена на порушення цілісності даних. Можливі наступні порушення: змінення існуючої інформації, додавання нових даних, видалення існуючих даних.

Одна із самих розповсюджених атак – це атака на відмову в обслуговуванні – DoS-атака. Є кілька різновидів – це атака орієнтована та заборону основному користувачу використовувати систему та інформацію. Коли така атака направлена проти інформації, то в результаті вона є непридатною до використання[8]. Якщо проти додатків – то дія що виконувались в результаті роботи тих додатків – становиться не можливою. Відмова в доступі до системі – це виводить з ладу усю комп’ютерну систему. В результаті все що встановлено все перестає працювати. Тип такої атаки на комунікаційну систему виводить з ладу зв’язок шляхом приглушення радіопередач, або проводить масову розсилку повідомлень. Немає зв’язку до ресурсів. Є ще також багато інших типів DoS – атак.

2 ЗАВДАННЯ НА РОЗРОБКУ

Метою кваліфікаційної роботи є розробка проекту мережі для хмарного сховища даних, який надає клієнтам послуги в сфері мережевих та інформаційних технологій.

Оскільки, визначено що найкращім способом організації мережі для хмарного сховища даних є підтримка сервісу на основі дата-центру, то і вимоги до мережі та інформаційної складової також ставляться високі. Раніше визначено найкращі послуги для користувачів, що надаються, а також типові складові частини. Тому на початку потрібно визначити усі вимоги до розробки, щоб задовільнити найвибагливіших клієнтів, та забезпечити надійність даних і відмовостійкість роботи клієнтів.

Розроблена мережа повинна надавати можливість реалізовувати наступні послуги для клієнтів дата-центру:

- сервіс віртуального хостінгу. Надає можливості розгортати веб-проекти клієнтів різного типу та навантаження;
- сервіс віртуальних приватних серверів. Надає можливості розгортати складні проекти, які складно або неможливо використовувати у віртуальному хостінгу;
- сервіс виділених серверів. Надання в оренду повноцінний сервер;
- надання поштового сервісу клієнтам;
- надання DNS сервісів клієнтам;
- сервіси баз-даних.

Вимоги до сектору віртуального сховища:

- швидкість мережевих каналів - 1Гбіт/с;
- підтримка мов програмування - PHP, Python, NodeJS;
- підтримка баз даних - MySQL, PostqreeSQL;

- розмежування доступу до каталогів серверу;
- антивірусний захист;
- антиспам захист;
- DDoS захист;
- резервування даних клієнтів;
- резервування конфігурацій серверів.

Вимоги до сектору віртуальних приватних серверів:

- підтримка основних серверних операційних систем - CentOS (та його заміни), Ubuntu Server, Debian, Arch;
- швидкість передачі даних - до 100Мбіт/с на кожну віртуальну машину;
- технології віртуалізації - KVM;
- захист від DDoS атак;
- антивірусний захист;
- використання системи керування віртуальними машинами;
- використання білінгового контролю;
- резервування даних клієнтів;
- резервування конфігурацій серверів.

Вимоги до виділених серверів:

- швидкість передачі даних - від 10 до 500 Мбіт/с;
- можливість заміни комплектуючих (накопичувачі, ОЗП, процесори);
- захист від DDoS атак ззовні;
- захист від DDoS атак від серверу;
- віддалена інвентаризація серверу;
- резервування за запитом.

Вимоги до поштової системи:

- використання smtp, pop та imap для клієнтів;
- збереження листування на сервері в каталозі клієнта;
- підтримка сертифікатів безпеки;

- підтримка DKIM;
- підтримка DMARC;
- захист від спаму.

Вимоги до системи DNS:

- можливість реєструвати доменні імена для клієнтів;
- наявність власних ns серверів імен;
- синхронізація із сервери вищих рівнів;
- надання клієнтам можливості керування власними ресурсними записами на сервері;
- аутентифікація серверів.

Вимоги до системи резервування:

- загальний об'єм дискового простору повинен перевищувати максимальний об’єм серверів на 20%;
- використання ізольованої приватної мережі для здійснення копіювання даних на сервера резервування;
- автоматизація резервування за часом та навантаженням;
- надання можливості клієнтам самостійно завантажувати резервні копії;
- надання клієнтам самостійно створювати резервні копії (не більше 2);
- контроль цілісності резервних даних;
- видалення неактуальних резервних копій (клієнт видалений, старі копії).

Визначені усі вимоги для окремих послуг, та завдання до організації захисту. Для того, щоб розпочати розробку мережі для хмарного сховища даних, потрібно на початку провести аналіз, та визначити методи, способи та сучасні рішення. Після чого можна переходити до розробки проекту мережі, де можна показати та відобразити візуально структури даного центру.

Структура мережі передбачає, що на її базі буде функціонувати інформаційна система, функції якої полягають у наступному:

- надання сервісів віртуального хостінгу;
- надання сервісів віртуальних приватних серверів;
- надання сервісів виділених серверів;
- надання поштових сервісів;
- центр створення сертифікатів;
- центр забезпечення захисту інформації;

Усе це дозволяє створити комплексну інформаційну еко-систему, яка дозволяє розміщувати, зберігати та обробляти інформацію клієнтами із забезпеченням належного рівня захисту.

3 МЕРЕЖЕВА СТРУКТУРА ХМАРНОГО СХОВИЩА ДАНИХ

3.1 Розподілене зберігання даних

При зберіганні даних в мережі хмарного дата-центру необхідно організувати дотриманість наступних умов:

- цілісність. Уся інформація, яка зберігається в системі, повинна бути незмінною, або має бути можливість відновити її з певної контрольної точки;
- доступність. Система та її архітектура, повинні забезпечити безперервний доступ до інформації або до її репліки (актуальної копії);
- розподіленість. Інформація повинна бути доступна з декількох областей зберігання, що обумовлює попередні два пункти, а також дозволяє отримувати доступ до даних для географічно більш близьких точок запиту.

В даному проекті для зберігання даних використовується розподілена файлова система, яка дозволяє зберігати дані не в ієрархічній структурі, а в плоскому адресному просторі із використанням індексації об’єктів зберігання.

Цілісність та доступність інформації забезпечується за рахунок реплікації отриманих для зберігання даних по різних серверах, стійках та дата-центрах. Як показує система на рисунку 3.1, кожний блок даних зберігається в локальному сховищі даних в двох екземплярах та один екземпляр зберігається у віддаленому хмарному сховищі.

Таким чином забезпечується глибина реплікації 3 (три екземпляра кожного блоку даних). Контролер сховища містить інформацію про всі сервери системи та контролює їх стан. При виході з ладу будь-якого серверу, стойки або дата центру, система запускає процес реплікації об’єктів по інших підсистемах до моменту відновлення втрачених сегментів.

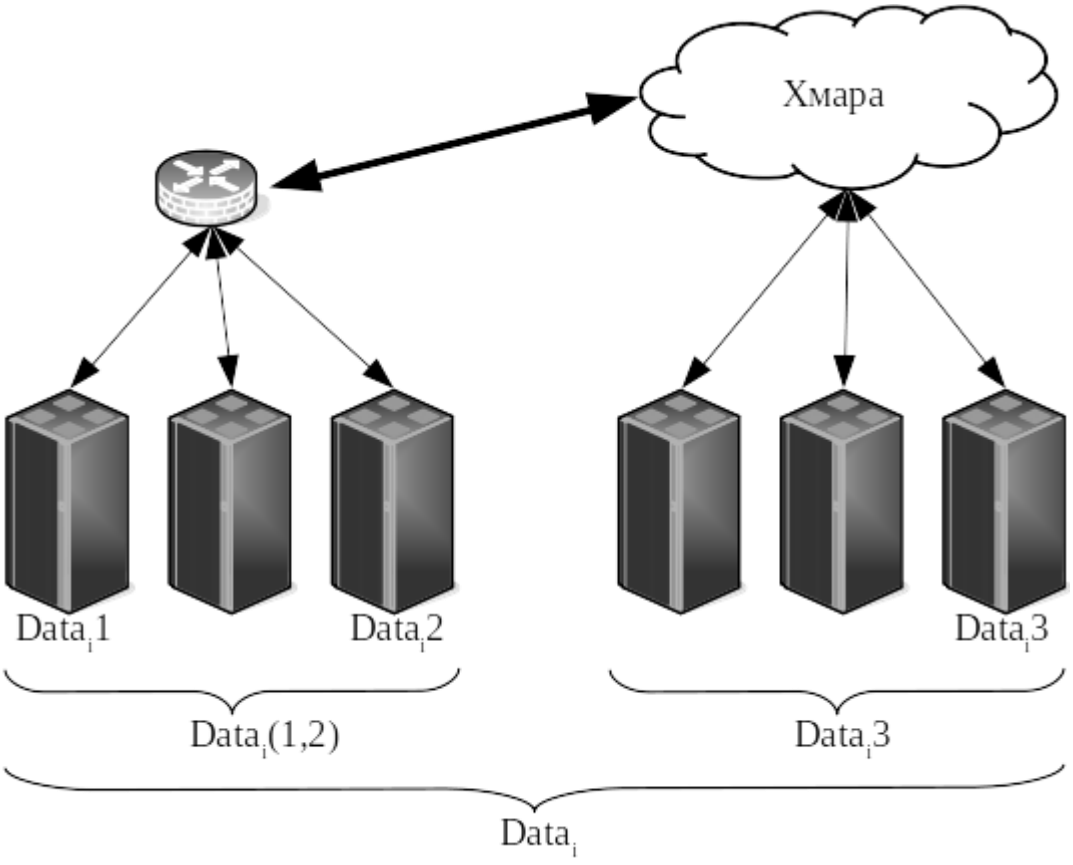

Рисунок 3.1 – Розподілене зберігання даних

Інформація, яка зберігається в системі розмежується на спеціальні групи, до яких залучаються диски систем зберігання. Таким чином, розмежується доступ до інформації за рахунок приналежності до певної групи.

Таким чином, зорганізується самостійна система зберігання, яка може без втручання інженерів контролювати свій стан та самостійно відновлюватись в разі певних збоїв чи помилок.

3.2 Інформаційна структура мережі

Інформаційна структура мережі використовує наступні структурні одиниці:

- сервіс віртуального хостінгу;

- сервіс віртуальних приватних серверів;
- сервіс виділених серверів;
- ядро мережі;
- сервісні сервери;
- центр забезпечення операцій;
- центр забезпечення безпеки
- центр сертифікації.

Кожний сервіс використовує свої правила використання, має свої особливості доступу до ресурсів та контролю з боку адміністраторів мережі.

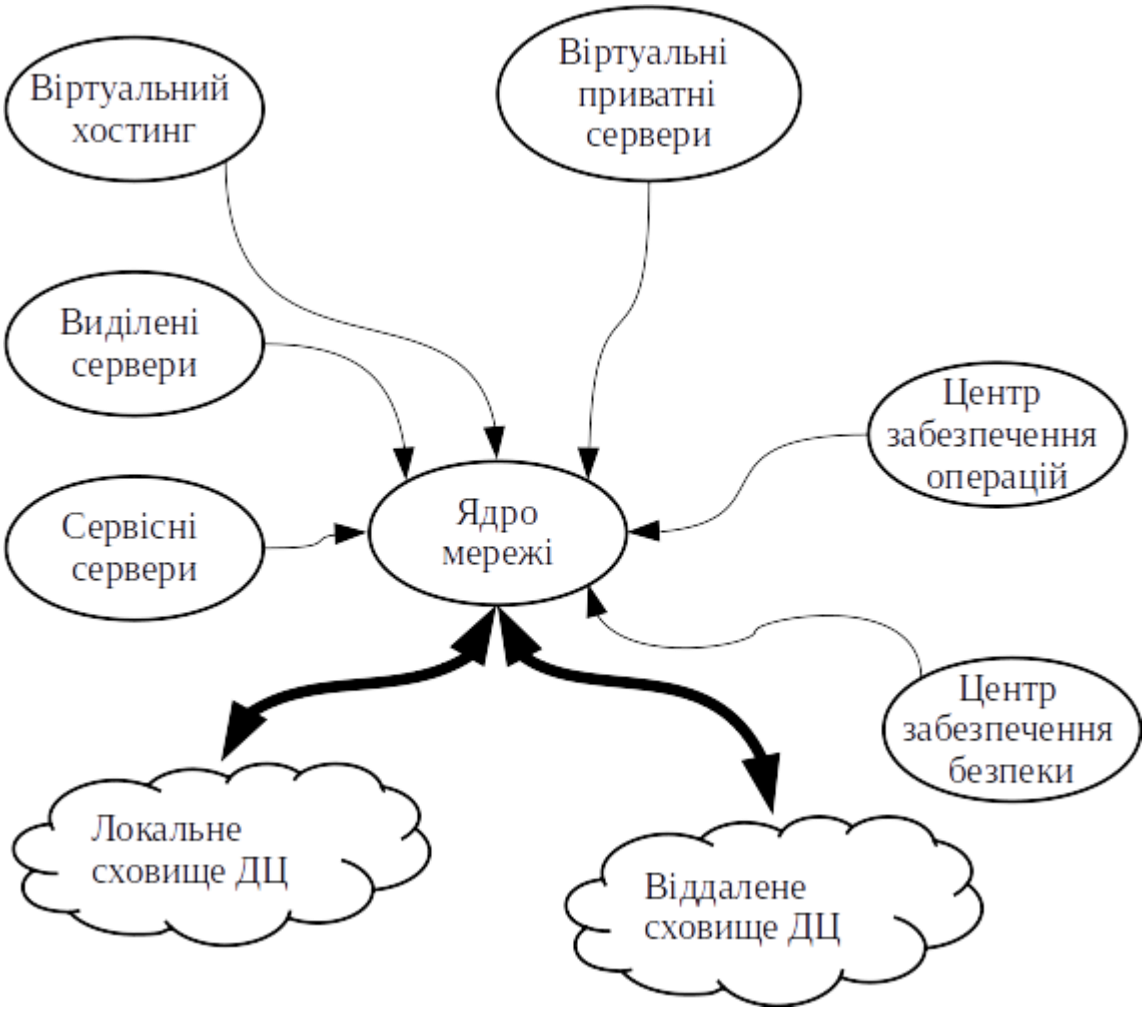

Рисунок 3.2 - Інформаційна структура мережі

Мережева взаємодія кожного сегменту мережі здійснюється через ядро мережі. Ядро мережі забезпечує комутацію всередині мережі,

маршрутизацію із зовнішньою мережею Інтернет, а також додаткові маніпуляції з трафіком для здійснення керування та захисту мережі.

Віртуальний хостінг забезпечує клієнтів сервісом розташування веб-сайтів. Даний сегмент системи очікується найбільш завантаженим мережевим трафіком, який забезпечується запитами та відповідями до веб-сторінок.

Сервіс віртуальних приватних серверів призначений для надання клієнтам окремих серверів які використовують технології віртуалізації, що дозволяє в рамках одного фізичного серверу розгортати до 50 віртуальних серверів.

Сервіс виділених серверів передбачає надання користувачам окремої ноди серверу або класичного компьютеру в користування для цілей клієнту.

Дані сервіси передбачають інтенсивний мережевий обмін із зовнішньою мережею Інтернет, а також можливості доступу до даних серверів для клієнтів дата центру. Це накладає певні особливості в організацію фільтрації трафіку, керуванні та захисті в даних групах серверів.

Використання інших структурних одиниць направлене на забезпечення функціонування усіх сервісів дата центру.

Сервісні сервери призначені для забезпечення функціонування усіх сервісів дата центру, як для клієнтів, так і для адміністраторів систем:

- DNS система дата центру використовується для розповсюдження доменних імен клієнтів та компанії;
- поштові сервери забезпечують відповідні сервіси з організації обміну поштової інформації, а також використовуються в керуванні доступу до облікових записів;
- термінальний сервер центру забезпечення операцій використовується для забезпечення доступу до інших серверів для адміністраторів мережі;
- термінальний сервер центру забезпечення захисту використовується для забезпечення доступу до інших серверів для адміністраторів безпеки;

– сервер моніторингу використовується для контролю та інформування про події в мережі та на обладнанні;

– інтерфейсний сервер забезпечує веб-систему дата-центру та супутніх систем (внутрішній форум, інтерфейс блокування та інше, система інвентаризації, панель керування);

– сервер аутентифікації забезпечує контроль доступу до систем дата-центру.

Центр забезпечення операції призначений для роботи системних адміністраторів. Через термінальні системи, шляхом підключення до відповідних серверів, співробітники здійснюють контроль та конфігурацію усіх серверів дата-центру.

Центр забезпечення захисту використовується для здійснення співробітниками функцій з конфігурації систем захисту мережі та кінцевих вузлів, проведення аналітики по инцидентам, які виникають в системі та прогнозуванню ризиків інформаційної системи.

3.3 Логічна структура мережі

Логічна структура мережі поділена на підсистеми, відповідно до функціональних сервісів, які вони забезпечують:

– сегмент системи віртуального хостінгу дата-центру;

– сегмент віртуальних приватних серверів;

– сегмент виділених серверів;

– сегмент мережі керування;

– сегмент ядра мережі.

Кожний сегмент мережі має власні особливості організації доступу користувачів, фільтрації трафіку та організації серверної структури.

Ядро мережі складається з двох мережевих шлюзів, які реалізують сервісні служби з забезпечення безпеки та трьох комутаторів третього рівня, які реалізують сервісні служби маршрутизації, комутації та інші мережеві

сервіси, які забезпечують передачу даних всередині мережі та зв’язок із зовнішніми транзитними провайдерами.

В кожному сегменті мережі, які реалізують рівень доступу, використовуються комутатори другого рівня, які забезпечують базові функції комутації, фільтрації та доступу до мережі. Разом із ядром/розподілом вони об’єднуються в сегмент мережі керування, котрий необхідний для окремого керування мережевим обладнанням дата-центру.

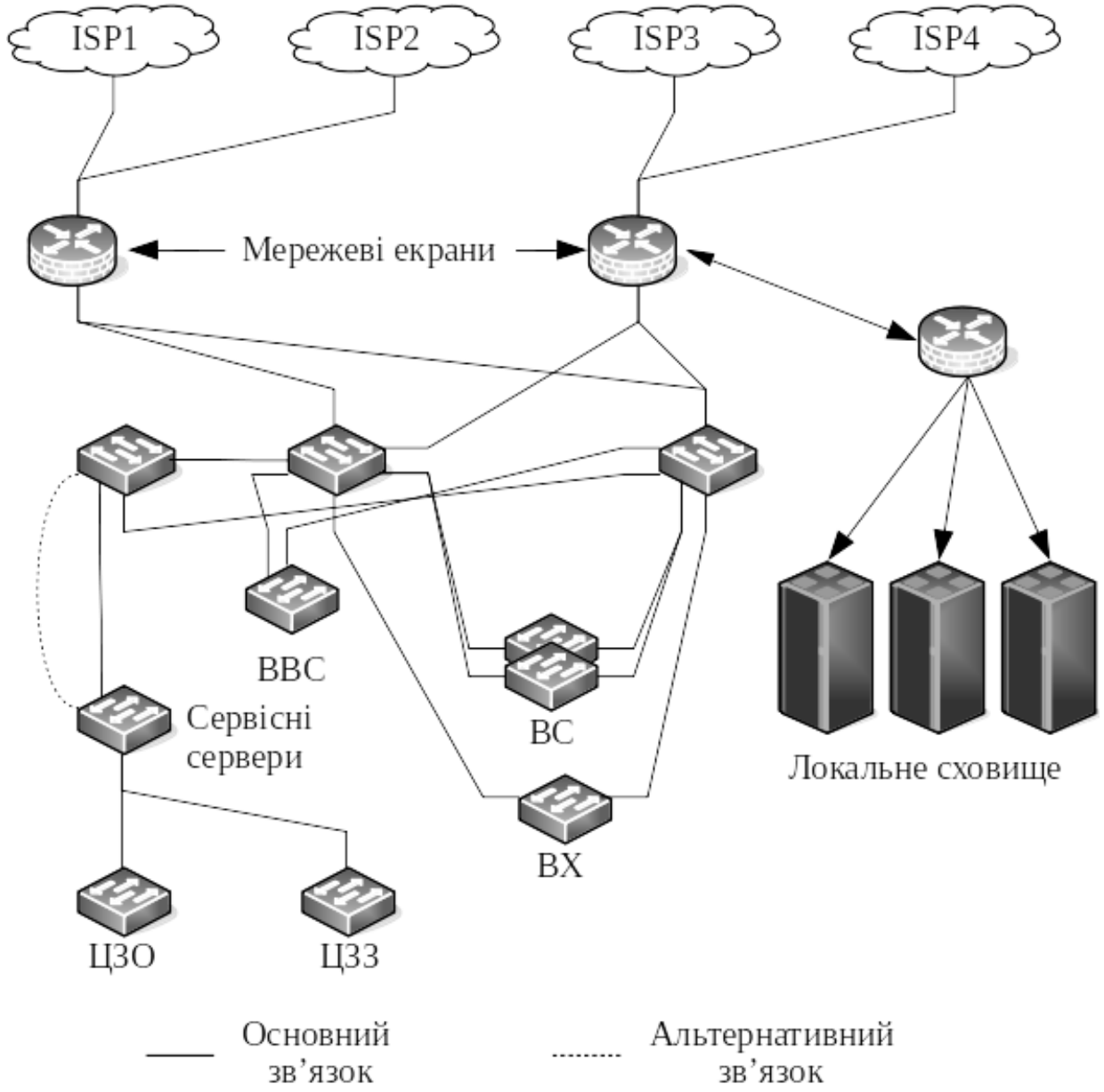

Рисунок 3.3 - Загальна логічна структура мережі

Кожний комутатор доступу зв’язаний з ядром мінімум двома фізичними кабелями для забезпечення доступності та відмовостійкості мережі. Частина таких з’єднань є активними та використовують балансування навантаження, а частина реалізують резервні лінії зв’язку.

Сегмент віртуального хостінгу. Структура серверів віртуального хостигу передбачає розгортання багатокористувальницкої операційної системи, де кожний з клієнтів отримує власний каталог для розміщення програмного забезпечення для своїх сайтів та інших файлів. Кількість користувачів на кожному сервері залежить від заповнення дискового простору, використання оперативної пам’яті та завантаження процесору. Структурна схема підмережі віртуального хостінгу представлена на рисунку 3.4.

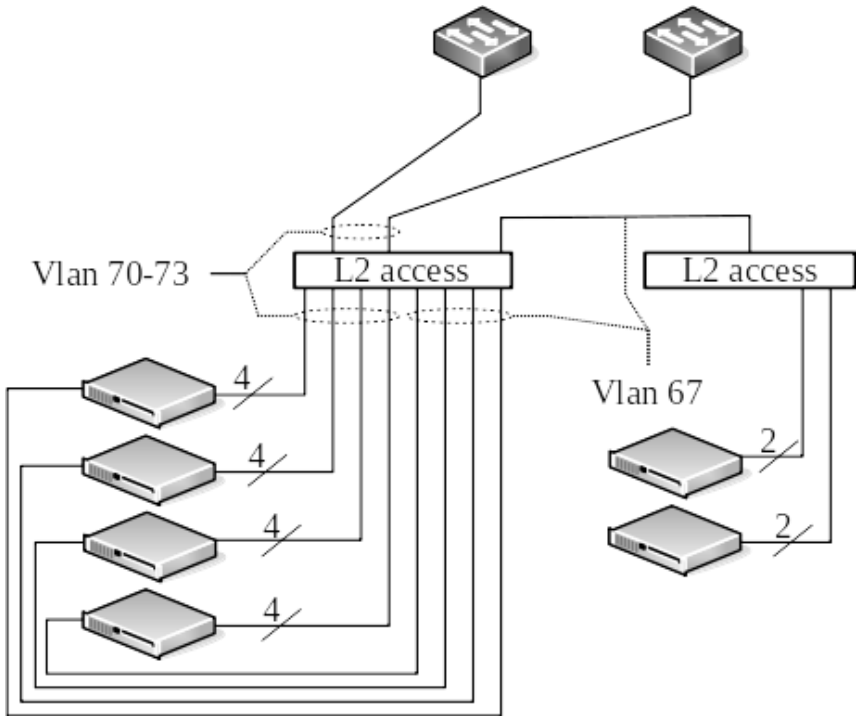

Рисунок 3.4 - Структура сегменту віртуального хостінгу

Чотири сервери, які в своєму складі мають по чотири ноди підключені до комутатору рівня доступу з використанням двох віртуальних мереж:

– віртуальна мережа доступу, яка використовується для керування пристроями та надання сервісів клієнтам;

– віртуальна мережа для здійснення резервування даних з серверів віртуального хостінгу.

Кожний сервер підключений до власної віртуальної мережі, кожна з яких забезпечує використання 24 мережевих адрес. Окремий фізичний інтерфейс використовується для трафіку між сервером віртуального хостінгу та сервером збереження резервних копій. На кожні два сервери віртуального хостінгу задіяно один сервер резервування.

Сегмент віртуальних приватних серверів. Структура серверів віртуальних серверів (рисунок 3.5) передбачає виділення частини ресурсів основного серверу для клієнтів, де вони зможуть встановлювати будь-яку операційну систему, розгортати власні сервіси та керувати аспектами функціонування серверу та операційної системи.

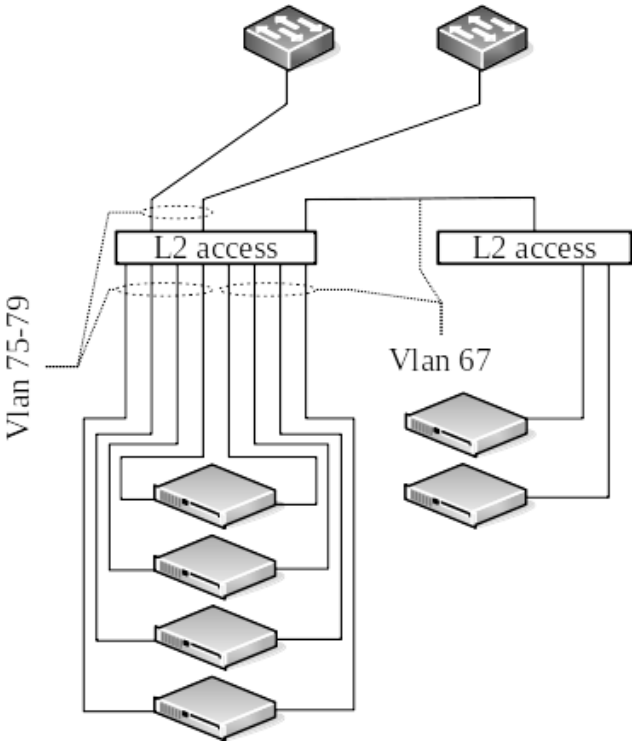

Рисунок 3.5 - Структура мережі віртуальних серверів

Кожному серверу виділено великі підмережі для надання кожному виртуальному серверу мінімум однієї мережевої адреси. Як і для віртуального хостінгу, на кожні два сервери виділено один сервер резервування, зв’язок з яким здійснюється по окремій віртуальній мережі.

Сегмент виділених серверів. Структура мережі виділених серверів передбачає надання клієнтам серверів в оренду. Для цього використовуються стійкові сервери або класичний форм-фактор ПК.

В мережі виділених серверів використовуються два типи серверів - стійкові сервери та класичний форм-фактор.

Сервери, які встановлюються в мережеві стійки містять по чотири окремих ноди, що дозволяє в одному сервері надавати послугу чотирьом користувачам. На момент проектування мережі, в системі передбачено 30 таких серверів, тобто 210 відокремлених серверів із гнучкою конфігурацією, яку можна змінювати, не вимикаючи систему.

Сервери типу “tower” є окремими пристроями, які надаються одному клієнту. Використання таких серверів дешевше на початковому етапі використання, проту знижує можливості безперервної модернізації, в перспективі призводить до більших витрат електроенергії. В подальшому заплановано повний перехід на стійкові сервери, а на даний момент використовується 100 серверів форм-фактору “tower”.

Система керування сертифікатами безпеки. Центр керування сертифікатами є окремим ізольованим сегментом, який не має жодного зв’язку із зовнішніми мережами. Така архітектура обумовлена вкрай високим рівнем ризику розголошення приватного ключа центру сертифікації. Система повинна забезпечити захист від порушення конфіденційності та цілісності приватного ключа від таких загроз як:

- вірусні атаки;
- пошкодження файлової системи;
- пошкодження серверу сертифікації;
- несанкціонований доступ до системи;
- ін’єкції програм;
- електромагнітні сигнали;

З точки зору мережевої взаємодії, центр сертифікації спроектовано як напів ізольовану мережу з дворівневим типом ієрархії із проміжними підсистемами контролю та захисту.

При надходженні запиту на отримання сертифікату, сам запит проходить попередню перевірку на мережевому ектрані, де визначається достовірність даних про одержувача, здійснюється попередній контроль формату запиту.

Після цього, запит обробляється на терміналі адміністратора для форматування даних для обробки на сервері сертифікації.

Після цього, проводиться глибока перевірка даних на визначення прихованих загроз, відхилень від поведінки, обробка в пісочниці та інші інтелектуальні заходи захисту інформації та аналізу загроз.

Після перевірок, запит надходить на вторинний сервер сертифікації, де формується SSL-сертифікат, зберігається у спеціальному сховиці та надсилається до замовника. Кореневий сервер вимкнений, і задіюється за необхідністю оновлення сертифікату вторинного серверу.

Мережі адміністраторів системи. Мережа центру контролю операцій та центру забезпечення захисту використовується для надання робочих місць для адміністраторів та інженерів дата-центру.

Кожний з адміністраторів має власний віртуальний сервер, підключення до якого здійснюється з терміналу (рисунок 3.6).

В мережі центру забезпечення операцій розташовано основні сервери, які забезпечують головні сервіси дата-центру:

– поштовий сервіс для забезпечення клієнтів власними поштовими сервісами;

– DNS система дата-центру забезпечує перетворення мережевих адрес в доменні імена для внутрішніх адрес дата-центру, а також для зовнішніх адрес клієнтів;

– сервер контрольної панелі хостінгу забезпечує візуальний інтерфейс керування серверами та сервісами цих серверів. Також, даний сервер використовується як веб система дата-центру;

– термінальний сервер 1 забезпечує підключення адміністраторів та інженерів мережі для здійснення службових обов’язків з підтримки сервісів системи;

– термінальний сервер 2 виконує роль VPN шлюзу для здійснення доступу до сервісів системи з зовнішніх мереж.

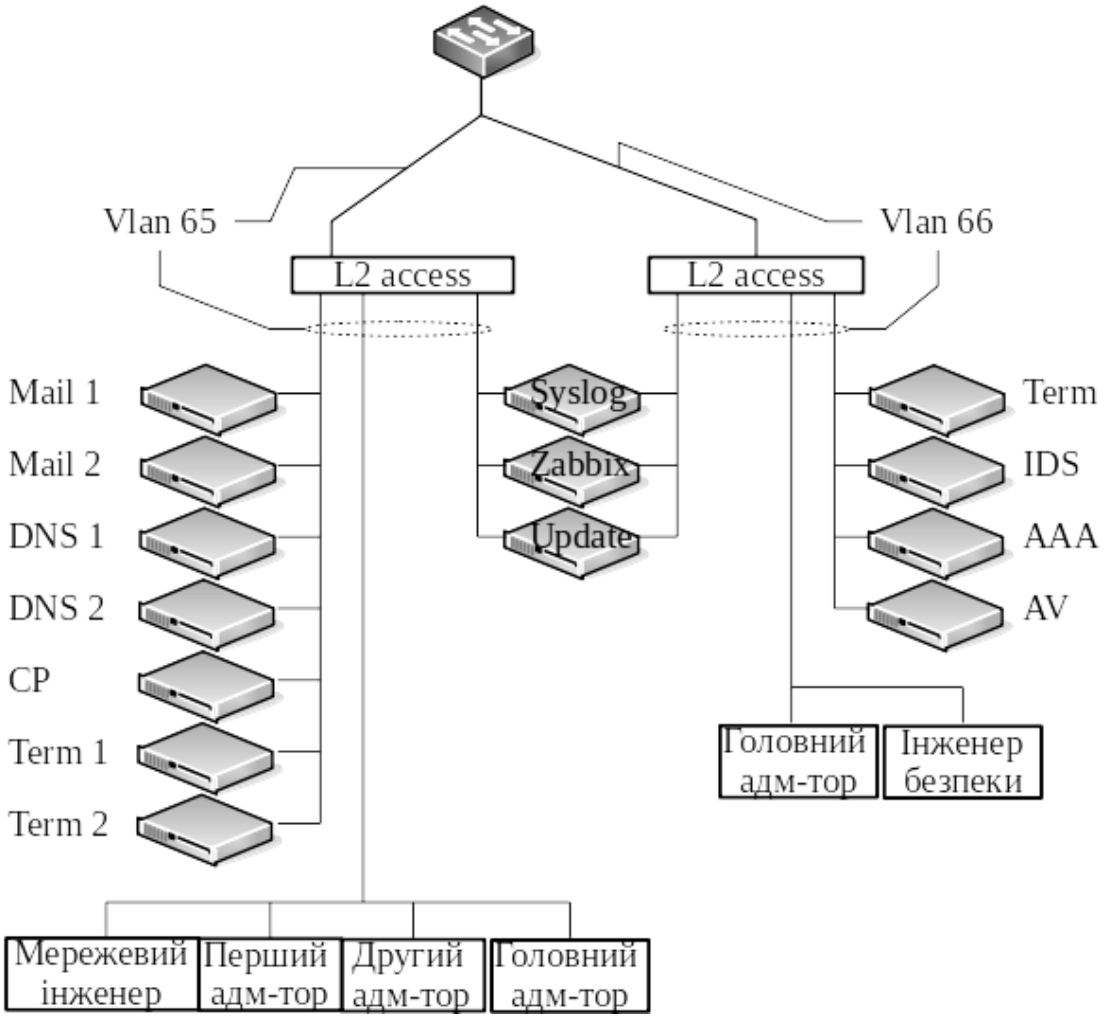

Рисунок 3.6 - Мережа NOC та SOC

В мережі центру забезпечення захисту використовуються чотири основних сервери:

– сервер антивірусного захисту використовується для віддаленого сканування серверів дата-центру;

- сервер AAA використовується для здійснення контролю доступу до сервісів та пристроїв дата-центру;
- сервер IDS здійснює аналіз трафіку для сервісних серверів з ціллю виявлення зловживань та неправомірних дій в мережі;
- термінальний сервер використовується, аналогічно попередньої мережі, для доступу адміністраторів безпеки до мережі та відповідних сервісів.

Також, в мережі використовуються сервери, доступ до яких необхідний для адміністраторів всіх груп і, відповідно, ці сервери розташовані в обох віртуальних мережах:

- сервер журналювання збирає інформацію про події на всіх серверах віртуального хостінгу, віртуальних серверів, сервісних серверів та мережевого обладнання;
- сервер моніторингу використовується для контролю та інформування про мережевий трафік та стан серверів та сервісів дата-центру;
- сервер оновлень збирає інформацію про стан операційних систем на предмет необхідності їх оновлень або програм на цих серверах. Також виконує роль пісочниці для цих оновлень для запобігання встановлення небажаних програм.

Всі сервісні сервери вимагають використання публічних адрес для роботи з мережею інтернет та приватного діапазону для резервування. Таким чином всі публічні адреси, для всіх серверів дата-центру, призначаються у відповідній віртуальній мережі, а приватні в мережі резервування.

3.4 Організація віртуальних мереж

Віртуальні мережі в системі дата-центру використовуються для забезпечення наступних функцій:

- ізоляція серверів по групах, відповідно до виконання сервісів;
- ізоляція серверів всередині конкретного сегменту;

- маршрутизація для серверів до зовнішніх мереж;
- розмежування доступу до ресурсів та сервісів.

З точки зору ізоляції, трафік кожного серверу, який має певну кількість мережевих адрес, не створює широкомовних запитів до інших серверів свого сегменту, або іншого сегменту серверів.

З точки зору маршрутизації, даний підхід дозволяє здійснювати балансування навантаження на мережеве обладнання, перенапрявляючи трафік серверів по різних мережевих провайдерах, а також розмежуючи потоки запитів та відповідей, якщо є потреба.

3.4.1 Визначення підмереж серверів

Кожний з серверів дата-центру виконує певні функції, виконання яких потребує різної кількості адрес. Виходячи з цього, було визначено наступні вимоги до різних груп серверів:

- сервери віртуального хостінгу вимагають одну адресу для здійснення керування, одну адресу для зв’язку із системою резервування та п’ять адрес для розподілення між сайтами користувачів;
- сервери віртуальних серверів вимагають одну адресу для здійснення керування, одну адресу для зв’язку із системою резервування та адреси для кожного віртуального серверу. Мінімальною кількістю адрес на кожного клієнта є одна, проте клієнт може замовити додаткові адреси, що також необхідно передбачити;
- виділені сервери вимагають одну адресу для здійснення керування, одну адресу для зв’язку із системою резервування та адреси для кожного віртуального серверу. Мінімальною кількістю адрес на кожного клієнта є одна, проте клієнт може замовити додаткові адреси, що також необхідно передбачити;
- мережеве обладнання вимагає використання мережевих адрес для здійснення керування, проте, для цього, можна використовувати приватний діапазон мережевих адрес;
- система резервування вимагає по одній адресі на сервер.

Мережі для адміністраторів також вимагають використання мережевих адрес, що обумовлює задіяння як приватного діапазону мереж, так і публічних, у зв’язку з наступними вимогами: в будь-який момент в цетрах керування повинні бути:

- два мережевих адміністратора;
- один мережевий інженер;
- один адміністратор безпеки 1го рівня;
- один адміністратор безпеки 2го рівня;

Виходячи із задіяння заданої кількості мережевих адрес, можна робити висновки про закупівлю відповідних підмереж адрес та створення адресної схеми мережі дата-центру.

3.4.2 Адресна схема віртуальних мереж

Для організації адресної схеми мережі дата-центру було прийнято використання двох основних схем та однієї альтернативної:

- схема публічних адрес використовується для надання сервісів дата-центру в мережі Інтернет;
- схема приватних адрес використовується для здійснення резервування даних та інших внутрішніх потреб дата-центру;
- для поступового впровадження адресації 6-ї версії, було впроваджено відповідну схему адресації.

Для запобігання великого широкомовного трафіку, у великих мережах (Dedicated, VDS) основну мережу також було роздроблено на складові.

Схема публічних адрес IPv4. В мережі дата-центру, наявності публічних адрес вимагають наступні пристрої:

- сервери віртуального хостінгу в мережі VH;
- сервери віртуалізації VDS;
- сервісні сервери дата-центру (поштові, моніторинг, DNS тощо);
- виділені сервери.

Для серверів віртуального хостінгу виділено підмережу на 128 адрес, яка була розбита на 16 підмережі по 6 доступних адрес, що дозволяє

адресувати кожну ноду за заданою схемою: одна головна адреса та 5 додаткових. Додаткові адреси довільним чином призначаються сайтам, які розгортаються на відповідній ноді.

Для серверів віртуалізації не має можливості заздалегідь розрахувати необхідну кількість адрес, так як окрім обов'язкової однієї мережевої адреси, клієнт може замовити певну кількість додаткових. Крім того, неможливо точно спрогнозувати скільки саме віртуальних машин буде розгорнуто на кожному сервері. Виходячи з цього, для даного класу серверів виділено 6 підмереж по 253 адрес кожна.

Це дозволяє базово адресувати 1518 адрес, однак, схемою допускається додаткове розбиття даних діапазонів, в разі такої потреби. Мінімальною необхідністю для даного сегменту є наявність 1000 мережевих адрес, отже отримана схема передбачає достатню надлишковість для розбиття та додавання нових серверів.

Для сегменту виділених серверів було призначено такий самий діапазон мережевих адрес та для таких самих цілей. Кожний сервер обов'язково отримує одну мережеву адресу, та, за окремим замовленням, до 8 додаткових адрес. Так саме, отримані 6 мереж можна додатково сегментувати для зручності ізоляції окремих серверів один від одного.

Ще одна мережа на 253 адреси була сегментована для адресації сервісних серверів дата-центру. Для цього було отримано 2 мережі по 32 адреси, що дозволяє надати кожному серверу публічної адреси, а також мати додаткові, альтернативні адреси на випадок необхідності переключення на інше дзеркало.

Також, окрему мережу публічних адрес виділено для мережевих пристроїв, проте, використання цих адрес суттєво обмежено. Інші отримані підмережі занесено в резерв, та будуть використовуватись в разі розширення послуг, або вичерпанні мережевих адрес в наявних мережах.

Схема приватних адрес. Діапазон приватних адрес використовується для внутрішніх потреб адміністраторів, зокрема:

- доступ адміністраторів до термінальних серверів з робочих місць;
- доступ адміністраторів до термінальних серверів з власних пристроїв;
- експерименти з моделями серверів та сервісів;
- внутрішня мережа керування мережевими пристроями;
- ізольована мережа для центру сертифікації;
- ізольований доступ до серверів резервування.

Основною задачею розгортання приватної мережі є забезпечення трафіку із серверами резервування та доступ адміністраторів до термінальних серверів.

На відміну від публічних адрес, для визначених задач достатньо по одній приватній мережі для кожного пристрою.

По 16 приватних адрес виділено для серверів віртуального хостінгу та серверів віртуалізації - по чотири на сервер, по одній кожній ноді в сервері. По одній адресі виділено кожному мережевому пристрою для керування цими пристроями.

По одній адресі виділено усім сервісним серверам дата-центру та серверам резервування.

Для всіх пристроїв мережі, крім мережевих комутаторів та подібних пристроїв, приватні адреси виділяються виключно для здійснення резервування даних на серверах. Також не було проведено сегментування мережі на підмережі. Замість цього було використано списки контролю доступу, що дозволило обмежити не тільки широкомовний трафік між пристроями, але й будь який інший трафік.

Також, з рисунку можно було побачити, що використовуєтсья тільки друга половина стандартної приватної мережі 192.168.0.0/24. Перша половина використовується для доступу адміністраторів, надання адрес резервування для виділених серверів, та тестових пристроїв для дослідження.

Схема публічних адрес IPv6. Враховуючи вичерпання мережевих адрес четвертої версії, було поставлено завдання передбачити перехід на адресацію

шостої версії. До того ж, клієнти самі можуть замовити використання на їх серверах адресацію шостої версії. Виходячи з цього, було придбано блок відповідних адрес шостої версії з префіксом /48, що для провайдерів України дає можливість адресувати більше 2 мільйонів пристроїв.

3.5 Сервери сховища даних

В мережі сховища даних визначено чотири основні типи призначення серверів:

- сервери для надання віртуального хостінгу;
- сервери для здійснення віртуалізації;
- сервери для оренди окремих нод:
- сервісні сервери хостінгу.

Було прийнято, що сервери для кожного типу сервісу зручніше комплектувати за схожими конфігураціями. Це додає більшої надійності системі та зручності адміністрування за рахунок наступних факторів:

- використання типових блоків під заміну;
- використання типових команд та конфігурацій для серверів;
- зручніше проводити модернізацію.

Таким чином, більшість серверів сховища даних мають ідентичну або дуже близьку апаратно-програмну конфігурацію.

3.5.1 Сервісні сервери

Для більшості серверів було використано сервери на дві ноди, тобто в рамках одного фізичного серверу розташовано два сервісні сервери. Сервісні сервери було поділено на групи і розташовано в нодах серверів за наступними ознаками:

- сервери mail1 та dns1 було розташовано на одному сервері server1;
- сервери mail2 та dns2 було розташовано на одному сервері server2;
- сервери term, term1 та term2 було розташовано на одному сервері server4;

- сервер контрольної панелі розташовано на окремому tower сервері server3 разом із сервером AAA;
- сервер моніторингу та syslog сервер розташовано на сервері server5;
- сервер оновлень та антивірусний сервер розташовано на сервері server6;
- сервер IDS розташовано на 2 нодах серверу server 7.

Технічні характеристики серверів схожі, різниця полягає в оброці даних та структурі сервісів конкретного серверу.

Поштові та dns сервери. В системі використовується по два поштових сервера та серверів імен. Для економії ресурсів та балансування навантаження, вони розміщені попарно на різних фізичних серверах на окремих нодах.

Поштовий сервіс складається з трьох основних складових - сам сервіс, який реалізує функціонування відправки та доставлення пошти, каталог користувальницьких поштових скринь та журнали. Сервіс функціонує відповідно заданих налаштувань та конфігурації, блокує пошту, яка відповідає шаблонам спаму та ігнорує блокування для адрес, які додані до списку ігнорування. В секції журналів зберігається вся інформація про події, які стосуються сервісу. Каталог поштових скринь зберігає поштову інформацію клієнтів із розмежуванням по користувачам та поштовим доменам.

Сервіс імен складається із спеціального сервісу named, який здійснює перетворення доменних імен в адреси. Також в спеціальному каталозі зберігаються ресурсні записи для кожного зареєстрованого доменного імені в сховищі даних.

Сервер контрольної панелі та сервер аутентифікації. Контрольна панель реалізує веб-інтерфейс доступу до ресурсів клієнтів та працівників. Вона працює, використовуючи базу даних клієнтів, з якими пов’язані їх тарифні плани та обмеження. Також, засобами контрольної панелі здійснюється контроль послуг, які надаються клієнтам, здійснення

квітування між клієнтами та співробітниками, а також використання сертифікатів безпеки. Також на даному сервері розгорнуто веб-сервер організації, для доступу до приватних кабінетів клієнтів та інших функцій системи.

AAA сервер здійснює класичні, для даного типу пристроїв функції. Він використовує спеціальну базу даних для ідентифікації суб'єктів, які намагаються отримати доступ до системи, обладнання або сервісів.

Термінальні сервери. Термінальні сервери використовуються для однієї цілі - авторизованого підключення до інших пристроїв сховища даних, та зберігання скриптів, які використовують адміністратори систем.

Структура кожного термінального однотипна, що обумовлює ідентичну організацію файлового простору. З точки зору безпеки здійснюється постійний контроль того, хто отримує доступ до серверу і ведеться постійне журналювання всіх відвідувань. Для кожного адміністратора організовано домашній каталог для власних файлів та наробіток. В адміністративному каталозі розташовані перевірені скрипти для здійснення контролю поштових та днс сервісів, а також для здійснення перевірки функціонування сервісів.

Так як на сервері використовується три ноди з чотирьох, четверта використовується як резервна. Якщо одна з нод виходить з ладу, на резервну оперативно синхронізується її копія, яка функціонує як оригінал.

3.5.2 Сервери віртуального хостінгу

Структура серверів віртуального хостінгу (рисунок 3.7) організована таким чином, що до серверів та окремих файлових блоків мають доступ множина клієнтів, що обумовлює необхідність великого ступеню ізоляції між ними для запобігання впливу на функціонування клієнтських сайтів.

У кожного клієнта власний каталог, який сприймається ним як кореневий. В ньому вони можуть розташовувати файли сайтів, інші файли, поштові повідомлення, журнали та файли сертифікатів.

Для програмування клієнтам доступно серверні мови програмування PHP, Python та NodeJS. Панель налаштована таким чином, що клієнт може використовувати будь-яку версію для власних проектів.

На сервері розгорнуто веб-сервер Apache із Nginx проксуванням. Це дозволяє переспрямовувати запити на домени клієнтів до відповідного клієнтського каталогу із сайтом.

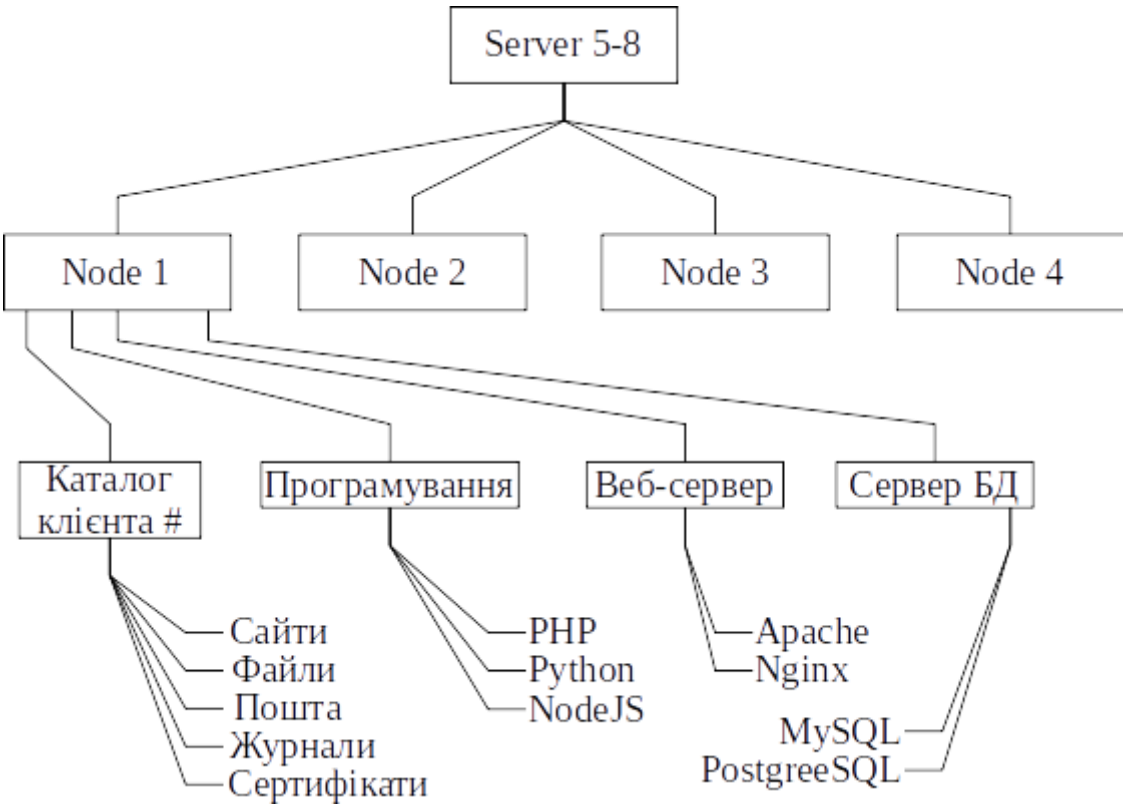

Рисунок 3.7 - Структура серверів віртуального хостінгу

Враховуючи, що клієнтські проекти можуть потребувати використання баз даних, на сервері розгорнуто системи MySQL та PostgreeSQL, які доступні для використання на сайтах клієнтів.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було проведено розробку мережевої та серверної структури для хмарного сховища даних. Робота не охоплювала питання інформаційної безпеки, проте була зосереджена на проектуванні мережевої інфраструктури сховища.

Мережева структура сховища даних складається з комутаторів, серверів та кабельної структури. Сервери виконують службові або сервісні функції для клієнтів. Мережева структура представлена різноманітними структурами, такими як інформаційна структура та логічна структура, які описують взаємодію компонентів сховища даних. Основною задачею при проектуванні мережевої структури сховища даних було забезпечення резервування зв’язків та мережевого обладнання для забезпечення безперервності надання сервісів для клієнтів організації.

Серверний парк сховища даних призначений для виконання наступних послуг для клієнтів:

- віртуальний хостінг сайтів;
- віртуальні приватні сервери;
- виділені сервери;
- поштові сервіси;
- сервіси імен;
- панелі керування та інше.

Для кожного сервісу було визначено окремий тип серверної конфігурації, в залежності від функцій, котрі сервер буде виконувати. Сервісні сервери також обиралися відповідно до тих задач, які вони виконують в рамках функціонування сховища даних.

Перевагою даного проекту є забезпечення широкого переліку сервісів для клієнтів:

- розташування власних веб-сайтів;
- розташування власних проектів;
- реєстрація та керування доменними іменами;
- використання поштових сервісів;
- зберігання файлів на віддаленому хості;
- керування функціонуванням сайтів, проектів та серверів;
- автоматизація сервісних задач (резервування, розсилка, оновлення та інше).

Всі ці можливості дозволяють клієнтам зосередитись на бізнес процесах, які реалізуються їх інформаційними системами, а не на самих інформаційних системах. Також, до переваг можна віднести економію витрат на володіння системою та персонал, який необхідний для її підтримки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Палаш Б. В. Обзор рынок хостинг-провайдеров – 2019 – [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/obzor-rynka-hosting-provayderov/viewer

2. Гордиевских В.М. Сущность, структура и классификация современніх технологий виртуализации – 2019 – [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/suschnost-struktura-i-klassifikatsiya-sovremennyh-tehnologiy-virtualizatsii/viewer

3. Квасницкий В.Н., Журавлева Т.Б. Использование технологии виртуализации при создании информационніх систем – 2012 - [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-virtualizatsii-pri-sozdanii-informatsionnyh-sistem-1/viewer

4. Михалев П.С. Анализ современной технологии виртуализации – 2014 - [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/analiz-sovremennoy-tehnologii-virtualizatsii/viewer

5. Хрулев П.А., Бодрова А.А., Логвин В.И. Проектирование защищенной информационной системы на основе сервера виртуализации – 2015 - [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/proektirovanie-zaschischennoy-informatsionnoy-sistemy-na-osnove-servera-virtualizatsii/viewer

6. Васильев П.А. Развертывание сервера с помощью технологии Docker – 2016 - [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/razvertyvanie-servera-s-pomoschyu-tehnologii-docker/viewer

7. Филин С.А. Организаци системы управления эксплуатацией центра обработки данных – 2018 - [Електронний ресурс]. URL:

https://cyberleninka.ru/article/n/organizatsiya-sistemy-upravleniya-ekspluatatsiey-tsentra-obrabotki-dannyh/viewer

8. Бодняков А.С. Основные режимы работы системы предотвращения вторжений для вычислительного кластера – 2018 - [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/osnovnye-rezhimy-raboty-sistemy-predotvrascheniya-vtorzheniy-ids-ips-suricata-dlya-vychislitelnogo-klastera/viewer

9. Белов М. А., Лупанов П. Е., Токарева Н. А., Черемисина Е. Н. Концепция усовершенствованной архитектуры виртуальной компьютерной лаборатории для эффективного обучения специалистов по распределённым информационным системам различного назначения и инструментальным средствам проектирования – 2017 - [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/kontseptsiya-usovershenstvovannoy-arhitektury-virtualnoy-kompyuternoy-laboratorii-dlya-effektivnogo-obucheniya-spetsialistov-po/viewer

10. Степанов А. Облачные вычисления как средство повышения устойчивости бизнеса – 2011 - [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/oblachnye-vychisleniya-kak-sredstvo-povysheniya-ustoychivosti-biznesa/viewer