ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри

_____

_____
(підпис) (ініціали, прізвище)

"___"_____20_ р.

Випускна кваліфікаційна робота

магістр
(освітньо-кваліфікаційний рівень)

на тему «Розробка та дослідження розподіленої інфокомунікаційної мережі аутсорсингової компанії»

Виконав: студент 2 курсу, групи ТКРм-20
(шифр групи)

спеціальності 172 телекомунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)

Аносов Юрій Анатолійович
(прізвище та ініціали) (підпис)

Керівник доц. Каф АТ Воропаєва А.О.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Покровськ – 2021 р.

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

Захист відбувся_____
(дата)
з оцінкою _____
секретар ДЕК_____
(підпис)

Випускна кваліфікаційна робота

бакалавра
(освітньо-кваліфікаційний рівень)

на тему «Розробка та дослідження розподіленої інфокомунікаційної мережі аутсорсингової компанії»

Виконав студент групи ТКР-16 Аносов Ю.А.
(підпис, дата) (ініціали, прізвище)

Керівник доц. каф. АТ Воропаєва А.О.
(підпис, дата) (ініціали, прізвище)

Зав. каф. автоматики та телекомунікацій д.т.н., доц І.С.Лактіонов
(підпис, дата) (ініціали, прізвище)

Консультанти
.
(підпис, дата) (ініціали, прізвище)

(підпис, дата) (ініціали, прізвище)

(підпис, дата) (ініціали, прізвище)

Нормоконтролер ст. викл. Д.О.Жуковська
(підпис, дата) (ініціали, прізвище)

Покровськ – 2021 р.

ДВНЗ «Донецький національний технічний університет»

Факультет комп'ютерно-інформаційних технологій та автоматизації
Кафедра автоматика та телекомунікації
Освітній ступінь магістр
Спеціальність 172 телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ:
Завідувач кафедри
_____
/_____/
"____" _____20___року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІАЦІЙНУ РОБОТУ СТУДЕНТУ

Аносов Юрій Анатолійович
(прізвище, ім'я, по батькові)

1. Тема роботи «Розробка та дослідження розподіленої інфокомунікаційної мережі аутсорсингової компанії»

керівник роботи: доц. каф. АТ Воропаєва А.О.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом від "____" _____ року №

2. Строк подання студентом роботи _____

3. Вихідні дані до роботи: результати науково-дослідної роботи, переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1) Огляд найбільш близьких технічних рішень.
2)Огляд рішень зменшення витрат на будування інформаційно-телекомунікаційних мереж.
3) Аналіз хмарних сервісів
4)Огляд доменних служби авторизації та розподілених баззи данних
5) Порівняння існуючих рішень у сфері шифрованої передачі данних

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 дипломної роботи	Строк виконання етапів роботи	Примітка
1	Проходження практики	06.09.2021	
2	Огляд найбільш близьких технічних рішень	26.09.2021	
3	Огляд рішень зменшення витрат на будування інформаційно-телекомунікаційних мереж	29.09.2021	
4	Аналіз хмарних сервісів	05.10.2021	
5	Огляд доменних служби авторизації та розподілених баззи данних	11.11.2021	
6	Порівняння існуючих рішень у сфері шифрованої передачі данних	15.11.2021	
7	Охорона праці	26.11.2021	
8	Оформлення	03.12.2021	

Студент _____ (підпис) _____ (прізвище та ініціали)

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

ЛИСТ ЗАУВАЖЕНЬ

Посада П.І.Б.	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Аносов Ю. А. Розробити та дослідити розподіленої інфокомунікаційної мережі аутсорсингової компанії./ Випускна кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 172 телекомунікації та радіотехніка. – ДВНЗ ДонНТУ, Покровськ, 2021.

Робота містить 104 сторінки, складається з вступу, п’яти розділів, висновків, переліка використаних джерел з 14 найменувань, 14 рисунків, 4 таблиць.

Метою даної кваліфікаційної роботи є розробка та дослідження розподіленої інфокомунікаційної мережі аутсорсингової компанії з можливістю широкосмугового доступу, послуг високошвидкісного доступу до мережі Інтернет, IPTV та IP телефонії.

В першій главі проведений аналіз об’єкту проектування та визначені характеристики послуг що будуть надаватись працівникам аутсорсингової компанії. Розрахований трафік мережі.

В другій главі розглянуто віртуалізацію як зменшення витрат на будування інформаційно-телекомунікаційних мережі.

В третій обгрунтовані та перелiковані хмарні сервіси котрі вікористовують IT-компанії.

В четвертій главі описуються та порівнюються доменні служби авторизації та розподілені баззи данних та визначається надійний RADIUS сервер.

В 5 главі на основі вибраного RADIUS серверу вибирається та описується найвигідніший VPN-клієнт.

Заключна глава описує основні заходи з охорони праці.

Ключові слова: МУЛЬТИСЕРВІСНА МЕРЕЖА, СКС, СХЕМА, ПОСЛУГА, ПРАЦІВНИК, ОБЛАДНАННЯ, ТЕЛЕКОМУНІКАЦІЇ, RADIUS, VPN, MAD.

Список публікацій здобувача

1. Всеукраїнської науково-практичноий форум «ТАК» доповідь «Використання технології низькоорбітальної телекомунікаційної мережі у міжнародному бізнесі» [Електронний ресурс]: «tak.donntu.edu.ua» Режим доступа: «https://tak.donntu.edu.ua/wp-content/uploads/2021/01/%D0%97%D0%91%D0%86%D0%A0%D0%9D%D0%98%D0%9A_%D0%A2%D0%90%D0%9A_2020.pdf»–Дата доступа: грудень 2021
2. Всеукраїнської науково-практичноий форум «ТАК» доповідь «Сучасна ІТ-інфроструктура міжнародних компаній» [Електронний]: «tak.donntu.edu.ua» Режим доступа: «https://drive.google.com/file/d/174sT4BeOytmqvhqw_xQzdXmrZKfFxHH1/view»–Дата доступа: грудень 2021

ABSTRACT

Anosov Yurii. Develop and research the distributed infocommunication network of an outsourcing company »./ - SHEI DonNTU, Pokrovsk, 2021.

The work contains pages, consists of an introduction, five chapters, conclusions, a list of sources used in the names, figures, tables.

The purpose of this qualification work is to develop and study a distributed infocommunication network of an outsourcing company with the possibility of broadband access, high-speed Internet access, IPTV and IP telephony.

The first chapter analyzes the design object and identifies the characteristics of services that will be provided to employees of the outsourcing company. Estimated network traffic.

The second chapter considers virtualization as a reduction in the cost of building information and telecommunications networks.

The third is substantiated and listed cloud services used by IT companies.

Chapter 4 describes and compares domain authorization services and distributed databases and identifies a reliable RADIUS server.

In Chapter 5, based on the selected RADIUS server, the most profitable VPN client is selected and described.

The final chapter describes the main measures of labor protection.

Keywords: MULTISERVICE NETWORK, SCS, SCHEME, SERVICE, EMPLOYEE, EQUIPMENT, TELECOMMUNICATIONS, RADIUS, VPN, MAD..

List of applicant's publications

1. All-Ukrainian scientific-practical forum "YES" report "The use of low-orbit telecommunications network technology in international business" [Electronic resource]: «tak.donntu.edu.ua» Access mode: «https://tak.donntu.edu.ua/wp-

content/uploads/2021/01/%D0%97%D0%91%D0%86%D0%A0%D0%9D%D0%98%D0%9A_%D0%A2%D0%90%D0%9A_2020.pdf»– Access date: December 2021

2. All-Ukrainian scientific-practical forum "YES" report "Modern IT-infrastructure of international companies" [Electronic resource]: «tak.donntu.edu.ua» Access mode: «https://drive.google.com/file/d/174sT4BeOytmqvhqw_xQzdXmrZKfFxHH1/view»– Access date: December 2021

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 12

ВСТУП 13

1 АНАЛІЗ АУТСОРСИНГОВИХ КОМПАНІЙ 17

1.1 Характеристика та опис офісу аутсорсингової компанї 17

1.2 Характеристика послуг, розробка інформаційної моделі 19

1.3 Розрахунок навантаження 22

Висновки до розділу 1 25

2 ВІРТУАЛІЗАЦІЯ - ЗМЕНШЕННЯ ВИТРАТ НА БУДУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ 27

2.1 Поняття віртуалізації 27

2.2 Типи віртуалізації 29

2.2.1 Віртуалізація операційної системи 29

2.2.2 Апаратна віртуалізація 33

2.2.3 Віртуалізація сервера 36

2.2.4 Віртуалізація зберігання 38

Висновки до Розділу 2 41

3 ХМАРНІ СЕРВІСИ 43

3.1 Загальний огляд 43

3.2 Моделі розгортання хмарних технологій 45

3.3 Основні властивості хмарних технологій 49

Висновки до розділу 3 51

4. ДОМЕННІ СЛУЖБИ АВТОРИЗАЦІЇ ТА РОЗПОДІЛЕНІ БАЗЗИ ДАННИХ 52

4.1 Поняття домену та його значення 52
4.2 Служба каталогів Active Directory..... 53
4.2.1 Переваги служби каталогів Active Directory 56
4.3 Аналоги Active Directory 58
4.4 RADIUS сервер..... 61
4.5 Порівняння сучасних RADIUS серверів 64
Висновки до розділу 4 72
5 ВИКОРИСТАННЯ VPN У ІТ КОМПАНІЯХ..... 74
5.1 Поняття VPN..... 74
5.2 VPN клієнт Cisco AnyConnect..... 77
Висновки до розділу 5 81
ВИСНОВКИ..... 84
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 87
ДОДАТОК А – ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ПРИ НАДЗВИЧАЙНИХСИТУАЦІЯХ НА ПІДПРИЄМСТВІ..... 89
ДОДАТОК Б. План бізнес центру 102
ДОДАТОК В. Структурна схема мережі..... 104

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VAD - voice activity detection;

VoD - Video- on-Demand;

ТМЗК - телефонна мережа загального користування;

СЛ - сполучна лінія;

IP - internet protocol;

VoIP - Voice over IP;

SIP - Session Initiation Protocol

QoS - quality of sendee;

ГНН - година найбільшого навантаження;

DNS - domain name sendee;

СКС - структурована кабельна система;

FTTX - Fiber To The X - оптика до точки X;

PON - passive optical network;

AON - all optical network;

P2P - peer to peer;

WDM - wave digital multiplexing;

OSI - Open System Interconnection.

MAD- microsoft active directory

VPN- Virtual private network

RADIUS- Remote Authentication in Dial-In User Service

ВСТУП

Актуальність теми. Найчастіше виникає питання про те, що значить «аутсорсингова компанія»: незнайоме англійське слово, яке утворилося в результаті злиття слів out («зовнішній») і source («джерело»). Однак відповідь можна знайти швидко і без особливих труднощів. Аутсорсингова організація — компанія, яка «надає в оренду» персонал. Такі компанії укладають договір на надання певної послуги та в рамках обумовлених умов надають фахівців, що дозволяють виконати поставлене завдання.

Виділимо переваги аутсорсингових компаній, що обумовлюють їх все більш висхідну популярність:

- Фокусування. Коштом аутсорсингу можна вирішувати стратегічні завдання, фокусуватися і концентрувати ресурси на основному виробництві, віддаючи всі додаткові завдання фахівцям з боку. Оскільки ринок припускає, що майже кожна компанія повинна знаходитися на «перехресті» різних областей, тримати фахівців з кожної сфери видається недоцільним або неможливим:

- Мінімізація витрат. Залучення аутсорсингової компанії дозволяє мінімізувати витрати на співробітників. Тій фірмі, яка користується послугою, не доведеться створювати додаткову (часом зайву) структуру, збільшувати штат постійних співробітників. Найчастіше знижуються транзакційні витрати. Аутсорсинг же дозволяє отримати фахівців з гарною підготовкою на обумовлений проміжок часу, уникаючи необхідності підбору постійних кадрів:

- Технології. Послуги аутсорсингу відкривають доступ до високих технологій. Тримати в штаті фахівців з IT-напрямку — задача з недешевих. Однак обійтися без сучасного обладнання і програмного забезпечення неможливо:

- провести апартний синтез;

- встановити відповідність розробленої мережі критеріям вимогам QoS.

Часом відзначають деякі негативні сторони, що стосуються використання аутсорсингових послуг. Однак більша їх частина обумовлена виключно неписьменною політикою з боку самих фірм. Розберемося, які недоліки часто згадують при розмові про аутсорсингові компанії:

- Збільшення витрат. Якщо невелика фірма передає занадто багато процесів, це може привести до серйозних фінансових витрат. Це особливо стосується тих випадків, коли попередньо не проводиться розрахунок очікуваного економічного ефекту і використання найманих фахівців виявляється не менш витратним, ніж утримання штату. Пов'язано це також і з тим, що деякі аутсорсингові компанії просять за свої послуги великі суми;

- Втрата контролю. Якщо співробітникам з іншої організації передана дуже велика кількість процесів, це може призвести до втрати контролю над самою організацією: розпадається нитка, що пов'язує безпосередньо управління і бізнес-практику. Керувати структурою стає складніше. Це також пов'язано з невмотивованим і неписьменним використанням послуг аутсорсингу;

-Відсутність чіткої законодавчої бази. Багаторазово зазначалося, що не всі фахівці, що приходять «ззовні», відрізняються сумлінністю. При цьому не існує ніякого способу строго їх проконтролювати в тому, що не стосується їх безпосередніх професійних обов'язків. Тому існує ймовірність витоку конфіденційної інформації, до якої вони отримали доступ; іноді доводиться стикатися з порушенням договірних угод. Аби не стикатися з такими ситуаціями, бажано співпрацювати з організаціями, які зарекомендували себе на ринковому просторі та мають репутацію надійних фірм.

Розрізняють компанії, кожна з яких орієнтується на конкретну сферу. Однак виділяють три головних напрямки аутсорсингу:

-Виробничий. У такому випадку одна компанія передає частину виробничих функцій інший. Найпростіший приклад: рекламне агентство

співпрацює з друкарнею, яка друкує певний тираж листівок. Інший приклад — складання устаткування з наданих запчастин.

-Бізнес-процеси. Поширена передача бізнес-процесів, які не є спеціалізацією конкретної фірми. Наприклад, керівники, які не бажають утримувати великий бухгалтерський відділ, передають його завдання стороннім фахівцям. Ще один випадок — транспортування товарів (і інші логістичні завдання), для якого потрібне серйозне обладнання. Іноді також може знадобитися юридична допомога: хоча стикатися з проблемами, що стосуються правопорушень і вимагають втручання професіонала, доводиться не дуже часто, вирішити їх без людини з великим досвідом, хорошою теоретичною підготовкою неможливо.

Оскільки інформаційні технології займають все більше місця в діяльності сучасних фірм, регулярно виникає потреба в забезпеченні обладнанням, технічної підтримки, програмному забезпеченні. Наприклад, компанії часто користуються допомогою фахівців, що займаються створенням сайтів або здійснюють розробку програмного забезпечення.

Метою даної роботи є використання хмарних технологій для оптимізації роботи аутсорсингової компанії шляхом розробки її розподіленої.

Мета роботи полягає у вирішенні наступних завдань:

- Аналіз аутсорсингових компаній
- Зменшення витрат на будування інформаційно-телекомунікаційних мереж мереж завдяки віртуалізації
- Розгортання хмарних технологій у рамках аутсорсингу
- Підбір доменної служби авторизації та розподіленої баззи данних
- Використання vpn у IT-компаніях

Об’єктом дослідження виступає IT-інфраструктура аутсорсингових компаніїй.

Предметом дослідження є оптимальні рішення щодо впровадження хмарних технологій та IT-систем контролю доступу працівників аутсорсингових компаній.

Методи дослідження. Основні теоретичні та експериментальні дослідження магістерської роботи виконані із застосуванням методів теорії імовірностей, математичні статистики , теорії телетрафіку, радіо – планування, математичної статистики

Наукова новизна одержаних результатів полягає у визначенні підтвердженні гіпотези про те, що передові технології та протоколи віртуалізації та хмарних сервісів можуть дозволити аутсорсинговим компаніям збілшити працездатність та зменшити витрати на власні датацентри з великим штатом IT-фахіців.

Практична цінність отриманих результатів Полягає в майбутньому вдосконалені аутсорсингових компаній сучасними та обґрунтованими моделями віртуалізації та хмарними сервісами.

Структура та обсяг роботи. Випускна магістерська робота обсягом 91 машинописних сторінок, складається з вступу, п’яти розділів, висновків, переліка використаних джерел, що складається з 13 найменувань. Робота містить 14 рисунків,4 таблиці, 3 додатки.

1 АНАЛІЗ АУТСОРСИНГОВИХ КОМПАНІЙ

1.1 Характеристика та опис офісу аутсорсингової компанї

Офіс аутсорсингової компанї — це сучасний комплекс, який забезпечує вимоги для комфортної та ефективної роботи співробітників, для прикладу буде обраний, бізнес-центр «IQ Business Center» [14] – сучасний комплекс, який передбачає оренду 16 осклованих поверхів, 3 підвальних поверхи паркінгу та вертолітний майданчик на даху для загального користування.

Цей тип офісів відповідає найвищим стандартам міжнародної класифікації офісних центрів А+. Багато в чому це залежить від рівня технічних рішень і якості всієї системи БЦ.

Офіс аутсорсингових компаній розташован в ділових центрах міст – зручному місці для перевезення з будь-якої частини міста приватним або громадським транспортом.

В таблиці 1.1 наведена характеристика абонентського складу по кожному з поверхів.

Виходячи з таблиці 1.1 та кількості поверхів визначимо кількість абонентських пристроїв по кожному з типів поверхів та загальну можливу кількість користувачів у офісу. Результати зведені в таблиці 1.2.

Загальна кількість активних: пристроїв аутсорсингової компанії котра може розташовуватися в такому БЦ становить 4597 одиниць. До складу активних пристроїв входять різноманітні телефоні пристрої, телевізори, комп'ютери, ноутбуки та камери системи відео спостереження.

Таблиця 1.1 - Характеристика абонентського складу поверхів

Тип Поверху	Тип Приміщення	Кількість ПК	Кількість ТА	Кількість ТВ	Кількість поверхів
1	Офіс	150	17	25	5
	Конференц зал	7	7	15	
	Кухня/зона відпочинку	0	0	5	
	Проходи/ приміщення ліфту	0	0	13	
2	Офіс	193	24	25	3
	Конференц зал	5	5	13	
	Кухня/зона відпочинку	0	0	4	
	Проходи/ приміщення ліфту	0	0	15	
3	Офіс	122	12	20	4
	Конференц зал	8	8	15	
	Кухня/зона відпочинку	0	0	5	
	Проходи/ приміщення ліфту	0	0	11	
4	Інфраструктурні об’єкти	15	5	25	5
5	Офіс	73	51	21	3
	Конференц зал	5	5	17	
	Кухня/зона відпочинку	0	0	8	
	Проходи/ приміщення ліфту	0	0	14	
6	Паркінг	0	0	0	3
	Проходи/ приміщення ліфту	0	0	0	

Таблиця 1.2 - Характеристика абонентського складу бізнес-центру

Тип Поверху	Кількість ПК	Кількість ТА	Кількість ТВ	Кількість камер спостереження
1	794	130	272	193
2	713	82	161	115
3	620	73	214	130
4	175	24	122	84
5	334	160	130	156
6	0	0	0	47
Всього	2638	452	782	725

1.2 Характеристика послуг, розробка інформаційної моделі

Необхідність визначення послуг, що надаються онлайн, визначається подальшим розрахунком трафіку. Залежно від різноманітності послуг, може знадобитися використовувати певний рівень обслуговування, який визначає певні мережеві технології..

Як відомо, багато сервісних мереж призначені для доставки різних типів трафіку через один канал зв'язку. Згідно з повідомленням, очікувані канали онлайн-зв'язку забезпечать доступ до таких сервісів::

- доступ до Інтернет
- IP-телефонія з виходом до ТМЗК
- IP-телевізори.
- відео спостереження за зовнішнім та внутрішнім периметром .

На рисунку 1.1 наведена інформаційна модель мережі.

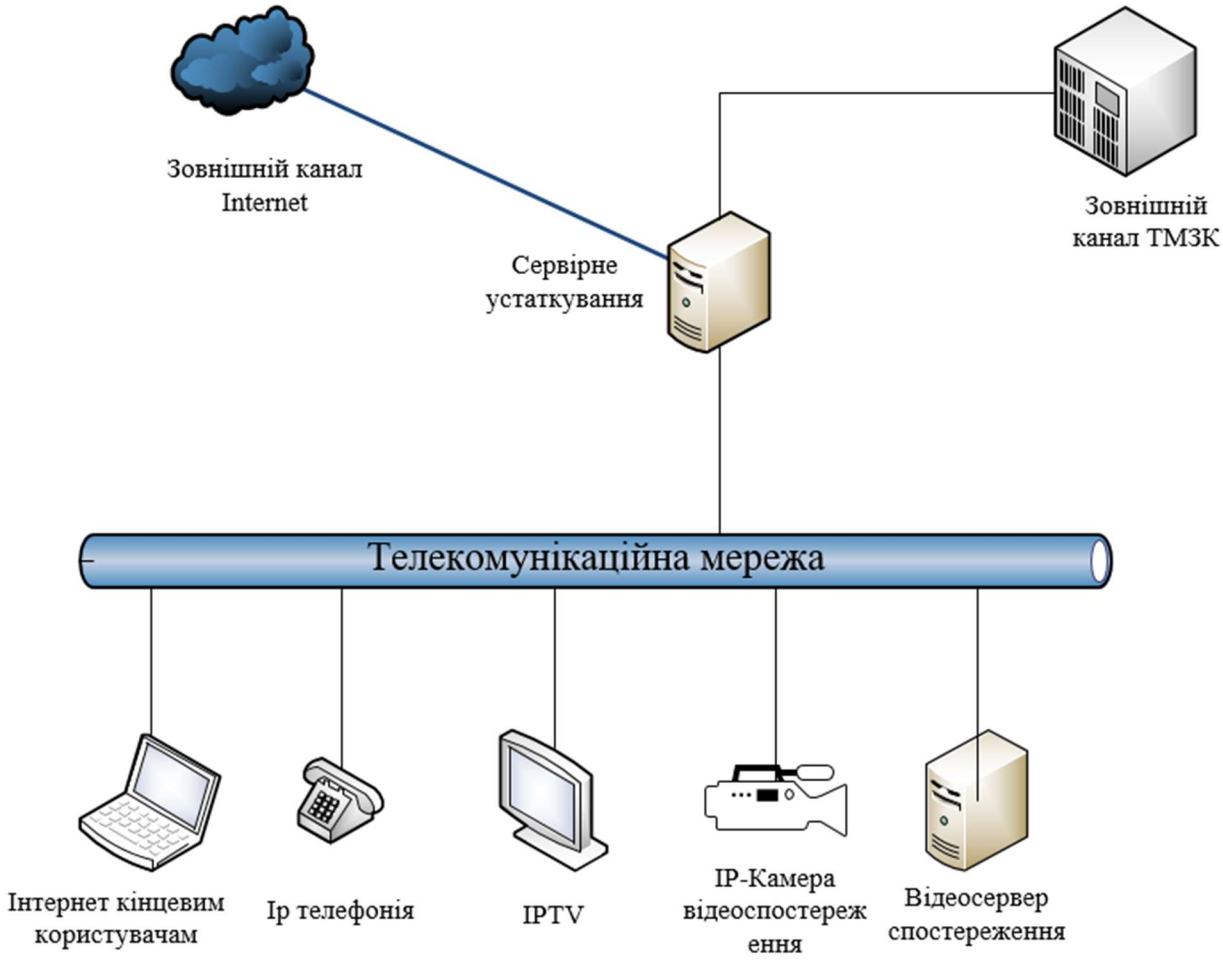


Рисунок 1.1 – Інформаційна модель мережі офісу аутсорсингової компанії

Відповідно до інформаційної моделі всі активні користувачі термінального пристрою підключені до єдиної телекомунікаційної мережі із серверним обладнанням. Комп'ютери, IP-телефони та IP-телевізори підключаються до зовнішньої мережі через сервер. Пристрої підключаються до відповідних зовнішніх каналів Розрахована на діапазон службових камер, інформація про камеру записується на спеціальний сервер відеоспостереження.

Багатофункціональна сервісна мережа передбачає надання таких послуг: Інтернет, IP-телефонія та відеосервери. Основними характеристиками послуги є швидкість, стійкість до помилок, частота, час зв'язку, максимальна погодинна телефонна частота (ARF) тощо. Буде описано кожну послугу, яку надає мережа, і визначено її основні параметри..

G. 711 - Аудіокодер представляє звуковий сигнал у вигляді потоку 64 кбіт/с (8 біт * 8000 значень в секунду). Стиснення, крім стиснення, не використовується.

Кодер G. 711 [2] використовується для розпізнавання голосу в сучасних телефонних мережах загального користування. Є дві версії: A-law і U-law. U-Laws розроблено для стандартів T1 у Північній Америці та Японії. Закон A1 застосовується до стандартів E1 в інших країнах. Різниця між двома версіями полягає в тому, як вибирається зразок коду В обох моделях сигнал дискретизується логарифмічно, а не лінійно. Закон А надає ширшу сферу дії, ніж закон Результатом є злегка спотворений звук через похибку квантування кутового сигналу. Цей код також можна використовувати на IP-телефонах-декодерах Це дуже просто і швидко, але вимагає широкої пропускної здатності.

Протокол встановлення сеансу (SIP, від англ. Session Initiation Protocol) - Протокол передачі даних, який описує, як налаштувати та завершити інтернет-сеанс користувача з обміном мультимедійним вмістом (IP-телефонія, відео-та аудіоконференції, миттєві повідомлення, онлайн-ігри). [1]

Протокол описує, як клієнт (наприклад, програмний телефон) може запитати підключення від іншого, можливо, віддаленого, клієнта до тієї ж мережі, використовуючи своє унікальне ім’я. Протокол визначає метод узгодження між клієнтами для відкриття каналів обміну на основі інших протоколів, які можна використовувати для безпосередньої передачі інформації (наприклад, RTP). Дозволяється додавати або видаляти такі канали під час стандартної сесії, а також підключати та відключати додаткових клієнтів (тобто дозволяється брати участь в обміні більш ніж двох сторін - конференц-дзвінку). Протокол також визначає порядок закінчення сеансу.

H.265/ HEVC — Сучасні стандарти стиснення відео вважаються спадкоємцями того, що зараз популярно. Кажуть, що новий стандарт покращує якість відео та вдвічі зменшує кількість біткойнів тієї ж якості, що

й H.264 / MPEG-4 AVC. Схвалений ITU кодер коду підтримує роздільну здатність 7680x4320 (8K).

Таблиця 1.3 - Характеристики послуг мережі

Служба	Максимальна Швидкість	Пачечність,P	F	Тривалість сеансу зв'язку T,C	Кодеки
Інтернет	100 Мбіт/с	5	250	5	
Інтернет	1 Гбіт/с	5	250	5	
TV	12 Мбіт/с	1	1	3600	
Відеоспостереження	4 Мбіт/с	3	1	3600	H.265+
Телефонія	64 Кбіт/с	1	1	2300	G.711,H.323, SIP
Інтернет Wi-Fi	100 Мбіт/с	10	50	15	

1.3 Розрахунок навантаження

Основне завдання, яке потрібно вирішити в цьому пункті, — розрахувати середній потік всієї мережі аутсорсинговох компанії.

Необхідно визначити параметри навантаження, яке виробляють користувачі вузла мережі, величину навантаження на магістраль, навантаження на зовнішню мережу та навантаження на комунікаційне обладнання.

Вихідними даними для розрахунку є топологія мережі, типи абонентів, види послуг, що надаються мережею та розподіл абонентів по вузлах. Виходячи з того, що топологія мережі та схема ще не визначені, розрахунок навантаження телевізійної служби буде виконано за умови її надання в режимі multicast. Загальна кількість телевізійних каналів становить 782.

Вузлами мережі в рамках об’єкту проектування виступають поверхи бізнес центру, тому розрахунок параметрів навантаження будемо проводити для кожного поверху.

Безпосередньо в основі методики розрахунку трафіку лежать імовірнісні характеристики потоку даних, які генеруються різними мережними додатками.

Трафік розраховується окремо для кожного виду послуги на кожному мережному вузлі.

Формула (1.1) дія розрахунку має вигляд:

$$\gamma_i^{(k)} = B_{ср}^{(k)} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)}, \quad (1.1)$$

.*k* - номер мережної послуги;

i- номер вузла;

$y_i^{(k)}$- математичне очікування графіка, шо генерується к-ю послугою на кцу вуалі;

$B_{\text{ср}}^{(k)}$- швидкість передачі даних (у бітах або пакетах у секунду) – середня пропускна здатність канату зв'язку, якої досить для якісної передачі графіка *k*-Ї послуги;

$N_{\text{аб}_i}^{(k)}$ - кількість абонентів на *i-му* вузлі, які користуються *k-ю* послугою;

$T_c^{(k)}$- середня тривалість сеансу зв'язку - для *k-ї* послуги;

$f_{\text{викл}_i}^{(k)}$- середня кількість викликів у годину найбільшого навантаження для користувачів *i-го* вузла, які використають *k-у* послугу.

Швидкість передачі даних $B_{\text{ср}}^{(k)}$визначається формулою (1.2):

$$B_{\text{ср}}^{(k)} = \frac{B_{max}^{(k)}}{P^{(k)}}, \quad (1.2)$$

$B_{\text{ср}}^{(k)}$- максимальна пропускна здатність каналу зв'язку:

$P^{(k)}$- пачечність одного абонента - відношення між максимальною та середньою пропускною здатністю, необхідною для забезпечення к-ї послуги.

Сумарний трафік, що генерується на *i-му* вузлі дорівнює:

$$\gamma_{\sum i} = \sum_{k=1}^{N_k} \gamma_i^{(k)}, \quad (1.3)$$

Параметри послуг, шо надаються в мережі приведені з таблиці 1.3.

На прикладі поверху типу №1 проведемо розрахунок трафіку за формулами (1.1)-(1.3):

- для доступу в Інтернет:

$$\gamma_i^{(k)} = B_{cp}^{(k)} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} = \frac{B_{max}^{(k)}}{P^{(k)}} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} =$$

$$= \frac{1000}{5} \cdot 794 \cdot 5 \cdot \frac{250}{3600} = 5513.8 \text{ Мбіт/с}$$

для доступу в Інтернет Wi-fi:

$$\gamma_i^{(k)} = B_{cp}^{(k)} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} = \frac{B_{max}^{(k)}}{P^{(k)}} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} =$$

$$= \frac{100}{1} \cdot 794 \cdot 5 \cdot \frac{100}{3600} = 1102.7 \text{ Мбіт/с}$$

- для IP-телефонії:

$$\gamma_i^{(k)} = B_{cp}^{(k)} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} = \frac{B_{max}^{(k)}}{P^{(k)}} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} =$$

$$= \frac{0.064}{1} \cdot 130 \cdot 2300 \cdot \frac{1}{3600} = 5.3 \text{ Мбіт/с}$$

- для TV:

$$\gamma_i^{(k)} = B_{cp}^{(k)} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} = \frac{B_{max}^{(k)}}{P^{(k)}} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} =$$

$$= \frac{12}{1} \cdot 272 \cdot 3600 \cdot \frac{1}{3600} = 3264 \text{ Мбіт/с}$$

- для відеоспостереження:

$$\gamma_i^{(k)} = B_{cp}^{(k)} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} = \frac{B_{max}^{(k)}}{P^{(k)}} \cdot N_{\text{аб}_i}^{(k)} \cdot T_c^{(k)} \cdot f_{\text{викл}_i}^{(k)} =$$

$$= \frac{4}{1} \cdot 193 \cdot 3600 \cdot \frac{1}{3600} = 772 \text{ Мбіт/с}$$

Підраховані всі результати навантаження. Загальне навантаження для поверху 1 типу становитиме 10657 Мбіт/с.

Результати розрахунків по кожному типу поверху окремо та мережі в цілому зведемо в таблицю 1.4.

Таблиця 1.4 - Розрахунок навантаження на мережу.

Тип поверху	Навантаження ПК. Мбіт/с	Навантаження ТА. Мбіт/с	Навантаження ТВ. Мбіт/с	Навантаження камер. Мбіт/с	Навантаження Wi-fi Мбіт/с
1	5513.8	5,3	3264	772	1102,7
2	4951.3	3,3	1932	460	990.2
3	4305.5	2,9	2568	520	861.1
4	1215.2	0.9	1464	336	243
5	2319.4	6.5	1560	624	463.8
6	0	0	0	188	0,00
Всього	18305.2	18.9	10 788	2 900	2820.1

Як виходить з наведеної таблиці, загальна величина навантаження на мережне устаткування в цілому складає більше 34,8 Гбіг/с. Зовнішній канал до мереж: Інтернет повинен становити не менш 18,4 Гбіт/с, навантаження на устаткування IP-телефонії – 19 Мбіт/с. TV – 10,8 Гбіт/с. відео спостереження – 2,9 Гбіт/с. Wi-fi – 2,8 Гбіт/с.

Висновки до розділу 1

Метою даної кваліфікаційної роботи є дослідження розподіленої інфокомунікаційної мережі аутсорсингової компанії з можливістю широкосмугового доступу, послуг високошвидкісного доступу до мережі Інтернет, IPTV та IP телефонії. Кількість поверхів становить 16. Загальна кількість поверхів під аутсорсингову компані. - 9. Окрім цього споживачами телекомунікаційних послуг виступають камери внутрішнього спостереження, загальна кількість яких становить 725.

В першій главі була розроблена інформаційна модель, надані характеристики послуг в мережі та розраховані параметри трафіку. Загальна величина навантаження на мережне устаткування в цілому складає більше 34,8 Гбіг/с. Зовнішній канал до мереж: Інтернет повинен становити не менш 18,4 Гбіт/с, навантаження на устаткування IP-телефонії – 19 Мбіт/с. TV–10,8 Гбіт/с. Відеоспостереження – 2,9Гбіт/с. Wi-fi – 2,8 Гбіт/с.к

2 ВІРТУАЛІЗАЦІЯ - ЗМЕНШЕННЯ ВИТРАТ НА БУДУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

2.1 Поняття віртуалізації

Віртуалізація - це процес запуску віртуальної комп'ютерної системи в шарі, абстрагованому (Рис. 1) від фактичного обладнання. У більшості випадків це відноситися запуску синхронно декількох операційних систем на комп'ютерній системі. Для додатків, що працюють над віртуалізованою машиною, здаватється що вони перебувають на власній спеціалізованій машині, де ОС бібліотеки та інші програми є унікальними для віртуалізованої гостьової системи та не підключені до операційної системи хоста, що знаходиться за ним логічно.

Є безліч причин, чому IT-компаніївикористовують віртуалізацію в обчислювальних технологіях. Для користувачів настільних комп’ютерів у більшості випадків використовується перспектива запускати програми, призначені для іншої операційної системи без необхідності перемикання комп'ютерів або перезавантаження в іншу систему. Для адміністраторів серверів віртуалізація у свою чергу пропонує перспективу заводити різні операційні системи, однак мабуть, що ще важливіше, вона пропонує засіб сегментувати велику систему на багато менших частин, що дозволяє більш ефективно застосовувати сервер кількома різними користувачами або програмам з різними потребами. Це також дозволяє ізолювати, захищаючи програми, що працюють у віртуальній машині, від процесів, що відбуваються в іншій віртуальній машині на цьому ж хості.

Гіпервізор - це програма для створення та роботи віртуальних машин. Гіпервізори традиційно поділяють на два класи: тип который управляє віртуальними машинами прямо у апаратному забезпеченні системи, по суті, діючи як операційна система. Другий класс гіпервізорів поводиться як

традиційні програми, котрі можливо запускати і спиняти немов звичайну програму.

Віртуальна машина - це емуляція еквівалента комп'ютерної системи, яка працює над іншою системою. Віртуальні машини можуть мати доступ до будьякої кількості ресурсів: обчислювальна сила за допомогою апаратного забезпечення, але обмежений доступ до процесора та пам'яті хост-машини; один чи кількохфізичних або віртуальних дискових пристроїв для зберігання; віртуальний чи дійсний мережевий інтерфейс; а також пристрої, як відеокарти, USB-пристрої чи інше обладнання, якими надається колективний доступ до віртуальної машини. Коли віртуальна машина зберігається на віртуальному диску, це називають образом диску. Образ диску може бути включати файли для завантаження віртуальної машини.

Рисунок 2.1 - Віртуалізація - перехід від фізичного відокремлення серверів до логічного

2.2 Типи віртуалізації[5]

Типи віртуалізації в хмарних обчисленнях:

- Віртуалізація операційної системи
  - Апаратна віртуалізація
  - Віртуалізація сервера
  - Віртуалізація зберігання

2.2.1 Віртуалізація операційної системи

Віртуалізація ОС - це тип віртуалізації в хмарних обчисленнях. Віртуалізація ОС є частиною технології віртуалізації та є різновидом віртуалізації сервера. Далі буде розглянуто використання, роботу, типи, типи дисків, переваги віртуалізації ОС.

Віртуалізація операційної системи включає змінену форму (Рис. 2), інакшу ві звичайної ОС, щоб різні користувачі могли керувати її кінцевим використанням різних програм. Весь процес має виконуватись в одному комп’ютері одночасно. У віртуалізації середовище ОС приймає команду будь-якого користувача, котрий ним керує, і виконує різні завдання в одній машині, запускаючи різні програми.

Рисинок. 2.2 - Віртуалізація операційної системи

У віртуалізації ОС, додатки не заважає один одному, хоча вони розгорнуті на одному хості. Ядро ОС дозволяє існувати більше ніж одному ізольованому екземпляру простору користувача. Такі екземпляри мають назву контейнери ПЗ, котрі є двигунами віртуалізації.

Причини, котрі вказують, чому зручно використовувати віртуалізацію ОС у хмарних обчисленнях:

– Віртуалізація ОС використовується для інтеграції апаратного забезпечення сервера шляхом переміщення служб на різнихсерверах

– Забезпечує безпеку апаратних ресурсів, котрі завдають шкоди

– Віртуалізація ОС використовується для хостингу середовища

– Може розділити додатки на контейнери

ОС комп’ютера керує усім ПЗ та АЗ комп’ютера. За допомогою ОС одночасно можуть запускатися кілька комп'ютерних додатків. Це виконується за допомогою центрального процесора комп’ютера. Через поєднання декількох компонентів комп'ютера, котрий координується ОС, кожна програма працює успішно.

Типи віртуалізації операційних систем:

– Віртуалізація ОС Linux. ПЗ VMware Workstation використовується для віртуалізації систем Linux. Крім того, для встановлення будь-якого ПЗ за допомогою віртуалізації користувачеві потрібно буде спочатку встановити ПЗ VMware. [8]

– Віртуалізація ОС Windows. Цей тип віртуалізації також подібний до вищезазначеного, щоб встановити будь-яке програмне забезпечення, потрібно спочатку встановити ПЗ VMware [10].

У віртуалізації ОС є два типи віртуального диска, щоб клієнт міг підключитися через мережу до віртуального диска:

– Технічного обслуговування буде менше, тобто, це заощадить і час, і гроші.

– Приватний диск. Приватний диск використовується одним клієнтом або однією організацією. На цьому диску компанія може зберігати інформацію на основі призначених можливостей.

– Спільний диск. Спільний диск використовує декілька клієнтів одночасно. Зміни, здійснені клієнтами, застосовуються індивідуально і не впливатимуть на налаштування іншого клієнта, коли кеш очищається під час перезавантаження системи. Він буде встановлений за замовчуванням після того, як система перезапуститься.

Переваги віртуалізації ОС:

– Віртуалізація ОС виключає використання фізичного простору, який використовує IT-система. Оскільки все є віртуальним, це вимагатиме менше місця, а значить, це заощадить гроші.

– Технічного обслуговування буде менше, тобто, це заощадить і час, і гроші.

– Кількість машин буде використовує безліч електроенергії, тому буде зменьшено споживання електроенергії, менша потреба в охолодженні, низьке обслуговування та більше економії електроенергії.

– Це також дає компаніям підвищити ефективність використання серверного обладнання, тим самим, є більша рентабельність інвестиці.

– Віртуалізація ОС має можливість швидкого розгортання.

Віртуалізація ОС дозволяє забезпечити безпеку та розташування кінцевих апаратних ресурсів серед великої кількості користувачів, котрі взаємно не довіряють. Більше того, системний адміністратор використовує його для консолідації апаратного забезпечення сервера. Це робиться шляхом переміщення служб на окремий хост у двох контейнерах, котрі знаходяться на сервері

У віртуалізації ОС може приховувати ресурси, щоб, коли комп'ютерна програма її читала, вони не відображалися в результатах перерахування. Тут також можна запустити програму в контейнерах, на котрі виділяються лише частини цих ресурсів. Частина контейнерів можуть вводити в кожну ОС, з якої виділено підмножину ресурсів комп'ютера.

Ці контейнери містять ряд комп'ютерних програм також ці програми можуть навіть взаємодіяти між собою. Виправлення та оновлення базової ОС завершуються протягом тривалого часу. Більше того, вони дуже мало чи не впливають на доступність прикладних сервісів.

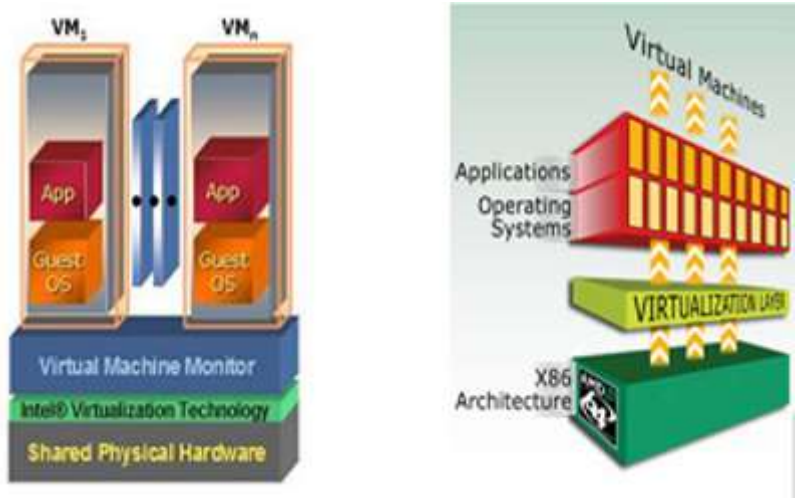
Віртуалізації ОС використовує програмне забезпечення, що дозволяє апаратному забезпеченню системи одночасно запускати кілька ОС. Більшість компаній використовують віртуалізацію ОС, оскільки вона економічна, надійна та гнучка. У віртуалізації ядро працює з єдиною ОС і забезпечує цю операційну систему з можливістю копіювання на кожній з ізольованих платформ. Віртуалізація ОС може надавати різні переваги компаніям, а також клієнтам, котрі використовують дані, оскільки вона сумісна як з невеликими компаніями, так і з масштабними організаціями.

2.2.2 Апаратна віртуалізація

Апаратна віртуалізація означає створення віртуальної платформи чогось, що буде включати апаратне забезпечення віртуального комп’ютера, віртуальні пристрої зберігання даних та віртуальну комп'ютерну мережу.

У віртуалізації апаратних засобів використовується ПЗ під назвою гіпервізор. За допомогою віртуальної машини гіпервізора ПЗ вбудовується в апаратну складову сервера. Робота гіпервізора полягає в тому, що він управляє фізичним апаратним ресурсом, який ділиться між замовником і постачальником.

Віртуальну техніку можна здійснити шляхом вилучення фізичного обладнання за допомогою монітора віртуальної машини (Рис. 2.3). У процесах є кілька розширень, котрі спомагають прискорити діяльність з віртуалізації та підвищити продуктивність гіпервізорів. Якщо ця віртуалізація виконується для серверної платформи, вона відома як соціалізація сервера.



Рисинок 2.3 - Графічне представлення апаратної віртуалізації

Гіпервізор створює шар абстракції між програмним забезпеченням та обладнанням, яке використовується. Після установки гіпервізора відбуваються віртуальні уявлення, такі як віртуальні процесори. Не можливо

використовувати фізичні процесори після встановлення. Існує кілька популярних гіпервізорів, таких як vSphere VMware на базі Microsoft Hyper-V. [6].

У цій системі одночасно можуть розміщуватися кілька віртуальних машин, але кожна віртуальна машина логічно ізольована одна від одної. Це відбувається з міркувань безпеки. Однією з причин безпеки є атака зловмисного програмного забезпечення. Через це інші віртуальні машини не постраждають. Якщо використовувати декілька віртуальних машин, ефективність системи одночасно зросте, а загальна продуктивність буде кращою. Таким чином, це призведе до того, що таке покращене використання дає різні переваги та підтримує систему, зменшуючи при цьому кількість серверів, що заощадить гроші.

Перелік віртуалізації апаратних засобів у хмарних обчисленнях:

– Повна віртуалізація. Для повної віртуалізації немає необхідності в будьяких модифікаціях для запуску будь-якої програми. Крім того, архітектура апаратури повністю імітується, що приносить користь гостьовому програмному забезпеченню. Існує середовище, досить схоже на ОС на сервері. За допомогою повних віртуалізацій адміністратори дозволяють запустити зміну віртуального середовища на його фізичний аналог. За допомогою повної віртуалізації адміністратори можуть поєднати нову та існуючу систему для ефективної роботи. Отже, вона повинна бути сумісною з новою системою.

– Емуляція віртуалізації. В емуляції віртуалізації апаратне забезпечення моделює віртуальну машину, і воно є незалежним. Тут гостьова ОС не потребує будь-яких інших модифікацій. У цій віртуалізації комп'ютерне обладнання як архітектурна підтримка будує та управляє повністю віртуалізованою машиною управління.

– Паравіртуалізація. У паравіртуалізації апаратне забезпечення не імітується, і гостьове ПЗ працює у відокремленій системі. Не потрібно імітувати апаратне забезпечення, але воно використовує прикладний

програмний інтерфейс, який модифікує гостьову ОС. Гіпервізор надає різні команди, котрі надсилаються з ОС на гіпервізор і називаються гіпервикликами. Ці гіпервиклики надалі використовують для управління пам’яттю.

Переваги апаратної віртуалізації:

– Економічна. Віртуалізація сумісна як з великими, так і з дрібними галузями. Оскільки більша частина коштів витрачається на обладнання, апаратна віртуалізація виключає цю вартість та приносить користь клієнту. Це також збільшує термін експлуатації існуючого обладнання, що зменшує енерговитрати.

– Ефективне резервне копіювання та відновлення. Оскільки поломка несподівана і дані можуть бути знищені за лічені секунди, то тут віртуалізація робить процес відновлення набагато простішим та точнішим із меншою кількістю робочої сили при використанні малих ресурсів.

– Ефективна робота. Це може забезпечити IT-працівникам більш простий спосіб встановлення та обслуговування програмного забезпечення, а не технічне обслуговування обладнання. Все можна зробити за допомогою комп’ютера, і професіонал зробить це з меншим простоєм, швидко і з мінімальною кількістю відключень.

– Відновлення поломок у апаратних віртуалізаціях. У хмарі може виникнути ситуація при котрій має бути алгоритм відновлення після аварій, який може забезпечити впевненість у тому, що продуктивність та обслуговування виконано після отримання даних. План відновлення при віртуалізації апаратних засобів передбачає захист як апаратного, так і програмного забезпечення, і це може бути виконано різними методами.

– Резервне копіювання. У цьому методі процес відновлення даних може бути складними та трудомісткими. Якщо клієнт відновлює останню копію даних, то він отримає більшу частину резервного копіювання. Існує вимога резервного пристрою та постійного зберігання матеріалів.

– Реплікація файлів та додатків. Тут реплікація даних на окремому диску та ПЗ вимагає для реплікації додатків та файлів дані, котрі можуть бути на одній стороні. Цей метод в основному використовується для додатків типу баз даних.

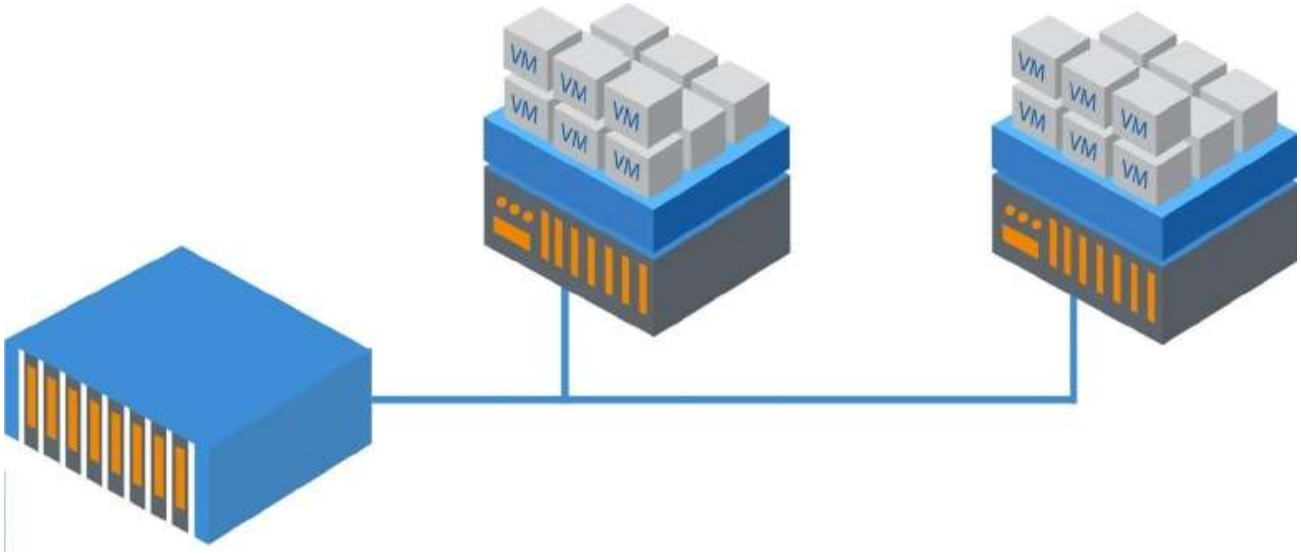
– Надлишок апаратного та програмного забезпечення. Цей метод забезпечує дублікат апаратного та програмного забезпечення, який розташований у двох різних географічних областях. Цей метод має найвищий рівень захисту від аварійних ситуацій та рішення щодо віртуалізації.

Апаратна віртуалізація стрімко розвивається і набуває популярності на серверній платформі. Основна логіка апаратної віртуалізації полягає в тому, що вона інтегрує багато невеликих служб у великі фізичні сервери для надання більш ефективних послуг. Тут операційна система, що працює на фізичному сервері, стає операційною системою, що працює на віртуальному комп’ютері. ОС, що працює на машині, складається з власного процесора, пам’яті та різних інших компонентів.

2.2.3 Віртуалізація сервера

Віртуалізація сервера розділіть фізичний сервер на кілька віртуальних серверів. Тут кожен віртуальний сервер працює на власній ОС і програмах. Можна сказати, що віртуалізація сервера хмарних обчислень маскує ресурси сервера. Сервер знайомий з окремими фізичними серверами. Один фізичний сервер програмно розділений на кілька віртуальних віртуальних серверів (рисунок 2.4).

Сьогодні компанії мають багато серверів, але не користуються ними. Це може призвести до втрати цінних серверів. Можливо віртуалізувати сервери в IT-інфраструктурі, що зменшить витрати за рахунок збільшення використання існуючих серверів. Віртуалізація серверів зазвичай приносить користь малим і середнім додаткам.



Рисинок 2.4 - Графічне зображення віртуалізації сервера

У хмарних обчисленнях існує 3 типи віртуалізації сервера:

– Гіпервізор – це рівень між ОС і пристроями. Причиною успішного запуску кількох операційних систем є гіпервізор. Він також може виконувати такі завдання, як черга, надсилання та повернення апаратних запитів. Операційна кімната працює на гіпервізоре, який використовується для керування віртуальними машинами та керування ними.

– Паравіртуалізація. Він заснований на високошвидкісному моніторі та гостьовій операційній системі та зміненому наборі записів для віртуальних машин. Після модифікації загальна функціональність збільшується, коли гість безпосередньо контактує з монітором високого артеріального тиску ОС.

– Повна віртуалізація. Повна віртуалізація може імітувати базову машину. Це абсолютно те саме, що говорити. Це використовується для керування машиною, яку ви використовуєте, а потім для виконання вводу-виводу або для зміни положення системи. Виконує незмінений гіпервізор. Це можливо, оскільки операція моделюється програмним забезпеченням, а код стану повертається разом із фактичним обладнанням.

2.2.4 Віртуалізація зберігання

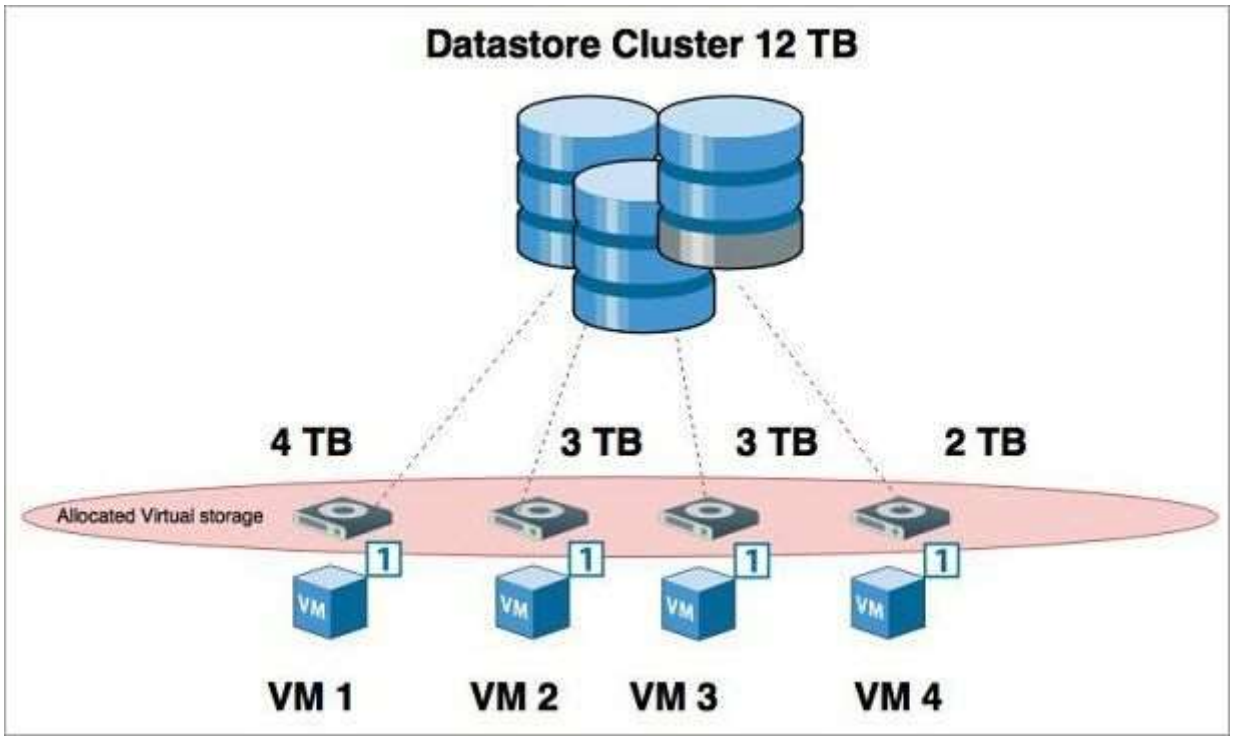
Віртуалізація пам’яті у хмарних обчисленнях - це не що інше, як спільне використання фізичного сховища на різних пристроях зберігання, це ще один пристрій зберігання даних. Можна сказати, що це група поточних пристроїв зберігання даних, які керують з центральної платформи керування. Ця віртуалізація пропонує багато переваг, таких як резервне копіювання та відновлення даних (Рисунок 2.5).

Весь цей процес займає дуже мало часу і працює ефективно. Віртуалізація сховища хмарних обчислень не відображає фактичної складності мережі зберігання даних. Ця віртуалізація застосовується до всіх рівнів мережі зберігання даних.Нижче наведено причини, котрі показують, чому потрібна віртуалізація зберігання у програмах хмарних обчислень:

– Якщо цю віртуалізацію реалізувати в IT-середовищі, це покращить управління сховищем. Оскільки все належним чином зберігатиметься, заторів не буде, і завдання буде виконано швидко.

– Буде мала кількість простоїв, оскільки доступність пам’яті краща. Всі ці проблеми усуваються за допомогою автоматизованої системи управ ління.

– Віртуалізація пам’яті забезпечує краще використання сховища, оскільки зберігання більшості інформації в певному місці може призвести до втрати даних, перевантаженості та будь-яких інших проблем. Отже, пра вильний розподіл даних для зберігання та зберігання може бути ко рисним.



Рисинок 2.5 - Віртуалізація сховища даних

Види віртуалізації зберігання:

– Апаратна віртуалізація. Цей тип віртуалізації вимагає апаратної підтримки. Саме такий стиль управління країною він використовував у Росії. Тут немодифікована ОС виступає як апаратне забезпечення віртуалізації, і можливо впоратися з нею за допомогою доступу до обладнання та вимог до захисту бізнесу.

– Віртуалізація ядра. Він працює на окремій версії ядра Linux. Ви можете запускати кілька серверів на одному ядрі. Він використовує драйвер пристрою для зв’язку між ядром Linux і віртуальною машиною. Ця віртуалізація є особливим способом віртуалізації сервера.

– Віртуалізація гіпервізора. За допомогою високого кров'яного тиску можуть працювати кілька операційних систем. Крім того, він надає функції та послуги, які допомагають операційній системі функціонувати нормально або нормально.

– Паравіртуалізація. Він заснований на супервізорі, який займається імітацією та програмним захопленням. Тут гостьова ОС

змінюється перед установкою на наступні машини. Модифікована система зв’язується безпосередньо з гіпервізором для підвищення ефективності.

– Повна віртуалізація. Ця віртуалізація схожа на віртуалізацію. У цьому випадку керівник фіксує роботу машини, яка використовується для роботи операційної системи. Після вимкнення операції він моделює програмне забезпечення та повертає код стану.

Віртуалізація хмарного сховища допомагає досягти незалежності від розташування за допомогою фізичних центрів обробки даних. Ця система надає клієнтам простір для обробки та зберігання своїх даних.

Важливість віртуалізації зберігання:

– Аварійне відновлення віртуалізації сховища в хмарних обчисленнях може збільшити використання дисків і програмних дисків. Це покращить аварійне відновлення та безперервність торгівлі.

– Рівень зберігання. Технологія рівня зберігання даних – це технологія, яка відстежує та вибирає найбільш використовувані дані та розміщує їх у найвищому порядку. Найменше використовувані дані зберігаються в мінімальній бібліотеці функцій.

Переваги віртуалізації зберігання:

– Вивантажити та завантажувати дані легко. У пам'яті дані з віртуальної пам'яті швидко відновлюються. Це так само просто, як отримати доступ до файлів на локальному комп’ютері. Зберігати дані за допомогою програми та підключення до мережі дуже просто.

– Легко керувати. Дані можна передавати на основі використання, наприклад, часто використовувані дані можна зберігати у високопродуктивній системі зберігання. Однак у дещо повільнішій системі можна зберігати дуже мало даних. Це приклад системи керування батареєю, де клієнт не має проблем зі зберіганням.

– Безпека. У віртуалізації сховище даних зберігається в іншому місці і захищається з максимальною безпекою. У разі катастрофи дані можна

отримати з іншого місця, не впливаючи на клієнта. Захист може задовольнити реальні потреби використання без надання додаткового зберігання.

Нижче наведено різні способи зберігання, що стосуються віртуалізації:

– Віртуалізація сховища на основі сервера. Вся віртуалізація та керування тут здійснюються програмним забезпеченням та фізичним сховищем у штаб-квартирі, яким може бути будь-який пристрій або група номерів. Господиня складається з кількох господинь, це віртуальні водії гостьових машин. Неважливо, корпоративна це віртуальна машина чи персональний комп'ютер.

– Віртуалізація мережевого зберігання даних. Віртуалізація веб-сховища зараз є найбільш широко використовуваною формою. Такі пристрої, як розумні комутатори або виділені сервери, підключаються до всіх пристроїв зберігання даних у оптоволоконній мережі зберігання даних і відображають сховище як віртуальний пул.

– Віртуалізація сховища на основі масивів. Тут група пам'яті має різні типи пам'яті, які використовуються як фізичні рівні та рівні зберігання.

Технологія віртуалізації сховища зараз є звичною серед користувачів через її перевагу. Завдяки віртуалізації в хмарних обчисленнях усі диски можна об'єднати з одним централізованим джерелом. Крім того, він дозволяє змінюватися і змінюватися без зміни часу. Це забезпечує гнучкість і гнучкість передачі даних.

Висновки до розділу 2

Віртуалізація — це процес віртуального вираження частини програмного забезпечення або віртуального додатка, такого як сервер, сховище та Інтернет. Це єдиний ефективний спосіб знизити витрати на IT, одночасно підвищивши ефективність і швидкість роботи всіх секторів

бізнесу.

Віртуалізація може підвищити швидкість IT, гнучкість і масштабованість, одночасно заощадивши значні витрати. Більша мобільність робочого навантаження, продуктивність і використання ресурсів, а також автоматизовані операції – це переваги віртуалізації, які спрощують управління IT та знижують витрати на володіння та експлуатацію. Включає додаткові переваги :

– Мінімізовані або зовсім усунені простої.

– Підвищена IT-продуктивність, ефективність, швидкість. • Швидше забезпечення додатків та ресурсів.

– Більша безперервність бізнесу та відновлення після аварій.

– Спрощене управління центрами обробки даних.

– Наявність справжнього центру даних, визначеного програмним забезпе ченням.

3 ХМАРНІ СЕРВІСИ

3.1 Загальний огляд

Хмарні обчислення зазвичай відноситься до надання користувачеві джерела комп’ютера та потужності у вигляді мережевої служби. Таким чином, джерело обчислень надається користувачеві «чистим» способом, і користувач не може контролювати, які комп’ютери відповідають його вимогам і яка операційна система працює. Під хмарними технологіями розуміється модель процесної системи, що забезпечує цілеспрямовану модифікацію матеріалів і віртуальних об’єктів..

Хмари мають багато спільного порівняно з більшістю базових фреймворків. Принципова відмінність між хмарою та базовою структурою полягає в тому, що її обчислювальна потужність теоретично не обмежена. Друга принципова відмінність полягає в тому, що, кажучи в двох словах, платформа термінала служить лише для взаємодії із завданнями виконання користувача. У хмарі сам термінал є потужним обчислювальним пристроєм, який може не тільки зберігати інформацію на відстані, а й безпосередньо керувати глобальною обчислювальною системою..

Серед технологій обробки даних, які з'явилися в минулому (у 90-х роках), певною популярністю набули так звані мережеві обчислення. Спочатку ця область розглядалася як можливість використовувати вільні ресурси ЦП та розробити систему оренди обчислювальної потужності. Ряд проектів (GIMPS, distribut.Net, SETI @ home) довели, що така обчислювальна модель є досить ефективною. Ця технологія використовується для вирішення науково-математичних задач, що потребують значних обчислювальних ресурсів. Відомо, що онлайн-розрахунки використовуються в бізнес-цілях. Наприклад, вони виконують деякі трудомісткі завдання, пов’язані з прогнозуванням економіки, аналізом даних про землетруси, дослідженням і

дослідженням властивостей вакцин і нових ліків. Справді, мережеві обчислення та хмара мають багато подібності в архітектурних та прикладних принципах. Однак сьогодні модель хмарних обчислень вважається більш оптимістичною, оскільки це більш гнучка платформа для роботи з віддаленими джерелами обчислень.

Зараз він складається з тисяч серверів, розташованих у центрі даних Big Cloud Computing. Вони забезпечують ресурси для десятків тисяч додатків, якими одночасно користуються мільйони користувачів. Хмарні технології є зручним інструментом для бізнесу, а підтримувати власні ERP, CRM чи інші сервери, які потребують придбання та налаштування інших пристроїв, дуже дорого..

Для зручності хмарні сервіси, такі як документи, надані Google (Документи, календарі), стають популярними серед приватних користувачів).

Причини поширення хмарних технологій очевидні: вони настільки універсальні, що можна заощадити на обслуговуванні та персоналі, а також на інфраструктурі. Апаратне забезпечення можна спростити при обробці даних і зберіганні інформації у віддаленому центрі обробки даних. Майже всі ці питання звертаються до постачальника послуг. Крім того, такий підхід дозволяє стандартизувати програмне забезпечення, і навіть комп'ютери компанії мають різні операційні системи (Windows, Linux, MacOS тощо). Хмарна технологія полегшує роботу клієнтів, які знаходяться поза офісом, але мають можливість під'єднатися до Інтернету для доступу до даних компанії.

Очевидно, що хмарні обчислення набагато простіше у використанні. Основним недоліком, який можна відразу виявити, є повна залежність від цих постачальників послуг. Фактично компанія (користувач) є заручником постачальника послуг та Інтернет-провайдера. Незважаючи на зростання надійності постачальників послуг хмарних обчислень, необхідно докласти багато зусиль, щоб забезпечити надійність і безпеку даних, наприклад, можливості резервного копіювання, а також доступність і безпеку

інформації. Крім того, хмарні обчислення не повністю сумісні з державними та військовими компаніями. Жоден комітет не сертифікує таку систему при роботі з інформацією про нерозголошення.

3.2 Моделі розгортання хмарних технологій

За моделлю розгортання хмари вони поділяються на приватні, публічні (публічні) та гібридні двигуни.

Внутрішня хмарна інфраструктура та послуги приватного хмарного підприємства. Ці хмари знаходяться в корпоративній мережі. Організація може самостійно керувати приватною хмарою або замовляти її. Інфраструктура може бути розташована в клієнтському просторі або зовнішнього оператора або частково клієнта, а з іншого боку – оператора. Ідеальна версія персональної хмари — це хмара, розміщена в організації, яка обслуговує та контролює співробітників. Приватні хмари мають ті ж привілеї, що й публічні простори, але у них є одна важлива особливість: компанія сама займається встановленням та обслуговуванням хмар. Складність і вартість створення внутрішньої хмари настільки високі, що вартість її експлуатації перевищує вартість використання загальнодоступної хмари..

Слід зазначити, що приватні хмари мають перевагу перед загальнодоступними: більш детальний контроль різноманітних хмарних ресурсів надає компанії будь-які варіанти конфігурації. Крім того, приватні хмари ідеально підходять, коли необхідно виконувати роботу, якій не можна довіряти публічні хмари з міркувань безпеки..

Хмарні послуги, що надаються постачальниками загальнодоступних хмар. Вони знаходяться поза мережею компанії. Користувачі цих хмар не мають можливості керувати або підтримувати хмарні дані, і вся відповідальність покладається на власника хмари. Постачальник хмарних

послуг відповідає за встановлення, керування, надання та підтримку програмного забезпечення, інфраструктури додатків або фізичної інфраструктури. Клієнти платять тільки за ресурси, які вони використовують. Підписатися на надані послуги може будь-яка компанія та індивідуальний користувач. Вони забезпечують зручний і недорогий спосіб розгортання великомасштабних веб-сайтів або бізнес-систем, які не можна використовувати в інших рішеннях. Наприклад: Amazon EC2 і Amazon Simple Storage Service (S3), Google Apps / Docs, Salesforce.com, Microsoft Office Web. Однак публічні хмарні послуги надаються переважно у формі стандартних конфігурацій, тобто на основі найбільш часто використовуваних умов. Це означає, що споживачі мають менший вибір щодо конфігурації користувачів у порівнянні з системами управління ресурсами. Також слід зазначити, що через поганий контроль інфраструктури жорсткі заходи безпеки та процеси, які вимагають нагляду, не завжди підходять для реалізації загальнодоступної хмари.

Шібридні хмари – це поєднання публічних і приватних хмар. Зазвичай вони створюються підприємством, а відповідальність за управління розподіляються між підприємством та постачальником загальнодоступної хмари. Mixed Cloud надає послуги, деякі з яких є загальнодоступними, а деякі приватними. Цей тип хмари зазвичай використовується, коли організація має щоквартальний час діяльності. Іншими словами, після того, як внутрішня IT-інфраструктура не виконує поточні завдання, деякі функції переносяться в загальнодоступну хмару (наприклад, багато нецінної корпоративної інформації у вигляді сировини) і надаються. Користувачі можуть отримати доступ до корпоративних ресурсів. У приватну хмару) через загальнодоступну хмару. Добре спроектована гібридна хмара може обслуговувати безпеку та важливі процеси, такі як отримання платежів від клієнтів та інших неповнолітніх. Основним недоліком такого роду хмар є те, що важко ефективно створити та керувати таким рішенням. Важливо отримувати послуги з різних джерел і організовувати їх як одне джерело.

Взаємодія індивідуального та громадського компонентів ще більше ускладнює рішення. Оскільки це відносно нова концепція архітектури в області хмарних обчислень, для цієї моделі розробляються більше практичних рекомендацій та інструментів, які можуть бути відкладені до проведення подальших досліджень. За словами Тома Бітмана, віце-президента Gartner і старшого аналітика дослідницької та консалтингової фірми Gartner, із трьох згаданих вище моделей розгортання хмари приватні хмари зараз найкраще підходять для бізнесу. Bitman виділяє п’ять ключових моментів, котрі допомагають краще зрозуміти структуру хмари.

Залежно від типу хмари послуг, ними можуть володіти й керувати постачальник і користувач або обидва. Права доступу також можуть відрізнятися.

Хмара - це не просто віртуалізація. Хоча віртуалізація серверів та інфраструктури є важливою основою для персональних хмарних обчислень, віртуалізація та управління віртуальним середовищем ще не є приватними хмарами. Віртуалізація надає кращу структуру, пул та динамічне джерело інфраструктури: сервери, настільні комп’ютери, ємність для зберігання даних, мережеве обладнання, програмне забезпечення тощо. Але для того, щоб середовище вважалося технічно хмарним, необхідні інші компоненти, такі як віртуальні машини, операційні системи або програмні контейнери, передові операційні системи, програмне забезпечення мережних обчислень, абстрактне програмне забезпечення для зберігання даних, інструменти масштабування та зберігання..

Термін «приватна хмара» не відноситься до загальнодоступних або змішаних матеріалів, до ресурсів, які використовує організація, або до повного відділення хмарних ресурсів організації від інших. Хмари не обов’язково є джерелом заощаджень. Однією з головних помилок є те, що хмара економить гроші. Збереження можливе, але не обов'язкове. Приватна хмара може допомогти ефективніше розподіляти ресурси для задоволення потреб підприємства та знизити вартість обладнання. Але приватна хмара

вимагає інвестицій в автоматизацію, а самі заощадження не окупаються. Так що зниження вартості не є основною перевагою цієї моделі. З цієї точки зору, основною рушійною силою впровадження хмарної моделі є не тільки заощадження, але й можливість виходу на ринок, здатність швидко адаптуватися та адаптуватися до попиту, а також здатність динамічно масштабуватися, що може збільшити швидкість нових послуг. Приватна хмара не завжди реалізована в клієнті. Приватна хмара відноситься до конфіденційності, а не до конкретного об'єкта, володіння ресурсом або самоуправління. Багато постачальників надають нелокальні приватні хмари, за винятком розподілу ресурсів одному клієнту. «Хмари називають приватними через їхню конфіденційність, і вони не несуть відповідальності за те, де вони розташовані, хто ними володіє і хто ними контролює», – сказав Бітмен. Наприклад, деякі можуть обмінюватися центрами обробки даних з хост-провайдерами або обмінюватися ресурсами від різних клієнтів, але використовують віртуальні приватні мережі (VPN) та подібні технології для їх розділення. Приватна хмара (як і публічна хмара) - це не тільки інфраструктурні послуги. Віртуалізація серверів є великою тенденцією, тому це потужний механізм для персональних хмарних обчислень. Але приватна хмара — це не лише інфраструктурні послуги (IaaS). Наприклад, окрім надання віртуальних машин, більш розумно розробляти та тестувати нове програмне забезпечення PaaS.

Найшвидшою платформою хмарних обчислень сьогодні є IaaS. Він забезпечує мінімальні ресурси центру обробки даних у зручній для користувача формі, але принципово не змінює принципи роботи. Програмістам зручніше використовувати PaaS для створення нових програм, спочатку розроблених для хмари, і надання абсолютно нових послуг, які відрізняються від попередніх. Приватні хмари можуть перестати бути приватними. З одного боку, приватна хмара забезпечує переваги хмари: швидкість, розширення та ефективність реконструкції, усуває деякі загрози безпеці, потенціали та реалії, характерні для публічної хмари. З іншого боку,

з часом рівень сервісу, безпеки та координації у публічних хмарних сервісах має зростати. Тому деякі приватні хмари можуть бути переведені до загальнодоступної категорії. Більшість приватних хмарних сервісів, ймовірно, перетворяться на гібридні хмарні сервіси та розширять можливості за рахунок використання загальнодоступних хмарних служб та інших сторонніх служб.

3.3 Основні властивості хмарних технологій

Документ Національного інституту стандартів і технологій (NIST) визначає такі функції хмари у «Визначеннях хмарних обчислень NIST»:

Перший — «доступ до широкосмугового доступу». Існує ряд пристроїв, до яких можна отримати доступ через хмарне джерело. Це не тільки найпоширеніші пристрої (ноутбуки, робочі станції тощо), але й мобільні телефони, тонкі клієнти. Порівняйте «широкосмуговий доступ» з основними комп'ютерними та онлайн-ресурсами. Сорок років тому оцінені ресурси були мізерними і дорогими. Їх використання обмежене через важливість і важливість робочого навантаження для збереження цих ресурсів. Аналогічно, мережа обмежена. Мережа Інтернет-протоколу (IP) була широко поширена в той час, тому не було широкосмугової мережі або мережі з низькою затримкою. Відтоді витрати, пов'язані з мережею (наприклад, витрати на обчислення та зберігання даних) були знижені завдяки масштабам виробництва та комерціалізації супутніх технологій. У міру зростання широкосмугової мережі зростають її доступ і розширення. «Широкосмуговий доступ» можна вважати особливістю хмарних обчислень, а також фактором, що сприяє їх розвитку..

"Самообслуговування на вимогу" є ключовою - дехто каже, основною - характеристикою хмарних обчислень. Якщо розглядати IT як складний ланцюжок поставок з застосунком і кінцевим користувачем в кінці

ланцюжка, здатність до самозабезпечення ресурсами в типових IT-середовищах фундаментально порушує робочий процес і процеси, котрі розвивалися як функція корпоративних IT за останні кілька десятиліть. Це включає в себе робочі процеси, пов'язані із закупівлею систем зберігання, серверів, мережевих вузлів, ліцензій на ПЗ і так далі. Самозабезпечення в не хмарних або старих архітектурах змушує традиційні процеси і функції, такі як планування пропускної здатності, управління мережею (забезпечення якості обслуговування або QOS) і безпеку (створення списків контролю доступу або ACL), зупинятися або навіть повністю руйнуватися. Добре відомий ефект в управлінні ланцюжком поставок - коли неповна або неточна інформація призводить до високої мінливості виробничих витрат - відноситься не тільки до виробничому середовищі, а й безпосередньо до виділення IT ресурсів в не хмарної середовищі (2). Хмарні архітектури, проте, проектуються і створюються з урахуванням необхідності самозабезпечення. Ця передумова має на увазі використання досить складних програмних рамок або порталів для управління функціями ініціалізації і допоміжного офісу. Історично склалося так, що відсутність комерційного готового програмного забезпечення (COTS), спеціально розробленого для автоматизації хмарних обчислень, змусило багато компаній створювати власні портали і структури для підтримки цих функцій. Пакети програмного забезпечення COTS, призначені для управління і автоматизації корпоративних робочих навантажень, в даний час складають значну частину загального потенційного ринку хмарних обчислень.

Основною передумовою розширення хмарних ресурсів є об’єднання. За відсутності обчислень інтегрованої мережі та сховища постачальник послуг повинен надавати послуги в ряді незалежних або однозначних незалежних джерел. Хмарна інфраструктура є багатокористувацьким середовищем, і багато клієнтів діляться своїми хмарними ресурсами зі своїми колегами. При найманні кількома користувачами є неминуче збільшення операційних витрат, яке можна пом’якшити конфігурацією апаратного забезпечення та

програмними рішеннями, такими як профілі програм і серверів.

«Стандартизована послуга» означає моніторинг використання цього «накопиченого ресурсу» та надання його споживачам для забезпечення точності споживання та витрат. Моніторинг використання грошей для погашення (або лише для міжвідомчої звітності та складання бюджету) давно є вимогою зацікавлених сторін IT – ще один святий погляд, але створення такої системи не є основним обов'язком більшості IT-відділів.

Останньою особливістю, втіленою у визначенні хмарних обчислень NIST, є «швидка еластичність». Еластичні розрахунки дуже важливі для зниження витрат і ринкової орієнтації (TTM). Дійсно, концепція гнучкої доставки ресурсів у ланцюжку постачання IT настільки ідеальна, що Amazon охрестила свою хмарну платформу «Elastic Computing Cloud» («EC2»). З точки зору однакових щоденних витрат, витрати на операцію розподілу ресурсів (перенесення, додавання, зміна або MAC) у ланцюжку постачання IT зазвичай є найважливішою частиною витрат, пов'язаних із розгортанням програми.

Висновки до розділу 3

У цьому розділі аналізуються сучасні хмарні технології, різні моделі хмарних сервісів, визначаються хмарні обчислення та дозволяються хмарні послуги.

Винесено рекомендації стосовно використання хмарних технологій та обчислень, завдяки чому аутсорсингові компанії можуть знизити ризики стосовно зберігання данних. Також використання хмарних технологій зменьшить витрати компанії на власний датацентр с локальними сервісами.

Також з'ясовано важливість використання хмарних технологій, що ставить під сумнів існування деяких загроз, пов'язаних із існуванням цих технологій. В четвертому розділі будуть розглянуті доменні служби авторизації та розподілені баззи данних.

4. ДОМЕННІ СЛУЖБИ АВТОРИЗАЦІЇ ТА РОЗПОДІЛЕНІ БАЗЗИ ДАННИХ

4.1 Поняття домену та його значення

Комп'ютерна мережа – необхідність у будь-якій компанії, де встановлено 2 та більше ПК. Цей спосіб організації бізнес-взаємодії дозволяє

- обмінюватися інформацією,
- користуватися Інтернетом,
- мати спільний доступ до різних мережевих ресурсів, серверів та програм

Комп'ютер, підключений до мережі, стає частиною робочої групи або домену. ПК з'єднують між собою за допомогою кабелю, телефонного дроту, супутникового зв'язку або бездротового пристрою. IT-структура може бути як локальною, так і великою мережею, де клієнти знаходяться в сотнях і тисячах кілометрів один від одного.

Використання домену значно спрощує автоматизацію процесів і підвищує безпеку даних. Завдяки створеній мережі, можна контролювати всю IT-сферу фірми.

Під час організації єдиної структури необхідно вибрати головний комп'ютер. Саме він оброблятиме запити, що надходять. Також можна використовувати роутер. З його допомогою спрощується не лише робота в мережі, а й підключення до інтернет-провайдера. Від настроювань DNS-сервера залежить швидкість обробки інформації.

Доменна система імен (DNS) – розподілена база даних із загальними політиками безпеки, що містить різноманітну інформацію про підключені комп'ютери. Як правило, це імена машин, IP-адреси та відомості для маршрутизації пошти.

Створення корпоративної доменної мережі на базі 1-рангової включає

кілька етапів:

– встановлення та попереднє налаштування серверної операційної системи,
– встановлення та налаштування служби Active Directory,
– встановлення та налаштування DNS,
– встановлення та налаштування DHCP,
– підключення комп'ютерів до домену,
– налаштування груп доменної мережі та прав її користувачів.

Домен - єдиний керований об'єкт. Він має щонайменше 1 сервер, який здійснює функцію контролю. Завдяки такій схемі підключення можна проводити моніторинг мережі та конфігурувати комп'ютери.

Усі пристрої, пов'язані з доменом, підпорядковані контролеру. Для зміни налаштувань та оновлення програмного забезпечення не потрібно працювати індивідуально з кожним ПК. Все це може зробити контролер.

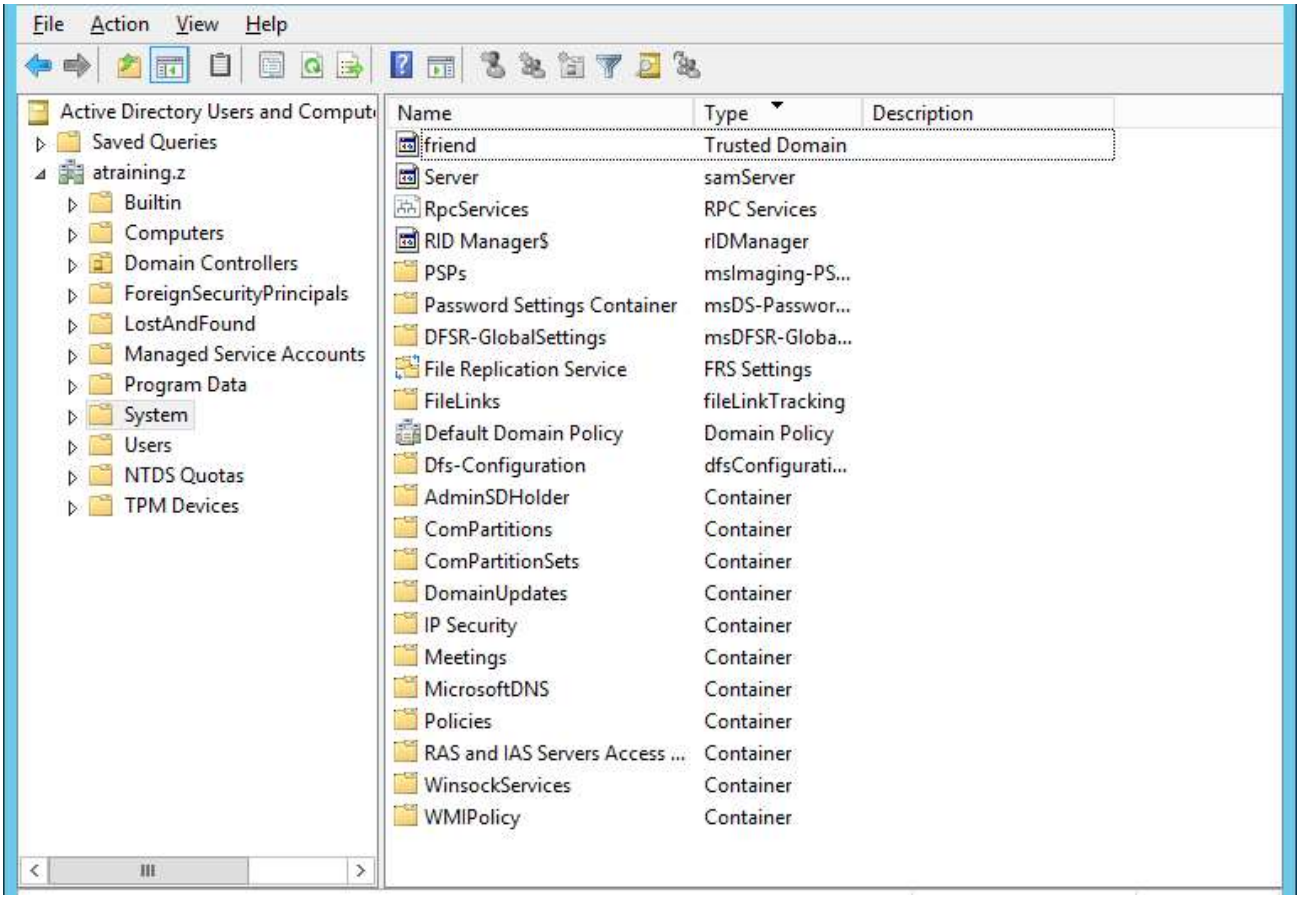
Служба каталогів Active Directory – це загальна база даних для всіх доменів. Об'єднання комп'ютерів у єдину систему здійснюється за допомогою протоколів мережі TCP/IP. Необхідна умова для їхньої роботи – наявність індивідуальних IP-адрес кожного ПК. [12]

Під час виконання спільних завдань різними комп'ютерами використовують систему контролю DNS. Також вона дозволяє переводити доменне ім'я в IP-адресу і навпаки. Якщо на ПК немає інформації про відповідність IP-адрес та імен, можна отримати відомості від DNS-сервера.

4.2 Служба каталогів Active Directory

Служби Active Directory (служби активного каталогу) є розподіленою базою даних, яка містить всі об'єкти домену. Доменне середовище Active Directory є єдиною точкою автентифікації та авторизації користувачів та

програм у масштабах підприємства. Саме з організації домену та розгортання служб Active Directory починається побудова IT-інфраструктури підприємства.



Рисинок 4.1 - Дерево домену Active Directory

База даних Active Directory зберігається на виділених серверах-Контролерів домену. Служби Active Directory є участю серверних операційних систем Microsoft Windows Server. Служби Active Directory мають широкі можливості масштабування. У лісі Active Directory може бути створено понад 2 мільярди об'єктів, що дозволяє впроваджувати службу каталогів у компаніях із сотнями тисяч комп'ютерів та користувачів. Ієрархічна структура доменів дозволяє гнучко масштабувати IT-інфраструктуру на всі філії та регіональні підрозділи компаній. Для кожної філії або підрозділу компанії може бути створений окремий домен зі своїми політиками, своїми користувачами та групами. До кожного

дочірнього домену можуть бути делеговані адміністративні повноваження місцевим системним адміністраторам. При цьому дочірні домени підпорядковуються батьківським.

Крім того, служби Active Directory дозволяють налаштовувати довірчі стосунки між доменними лісами. Кожна компанія має власний ліс доменів, кожен із яких має власні ресурси. Але іноді буває потрібно надати доступ до своїх корпоративних ресурсів співробітникам іншої компанії – робота із загальними документами та програмами в рамках спільного проекту. Для цього між лісами організацій можна налаштувати довірчі стосунки, що дозволить співробітникам однієї організації авторизуватись у домені іншої.

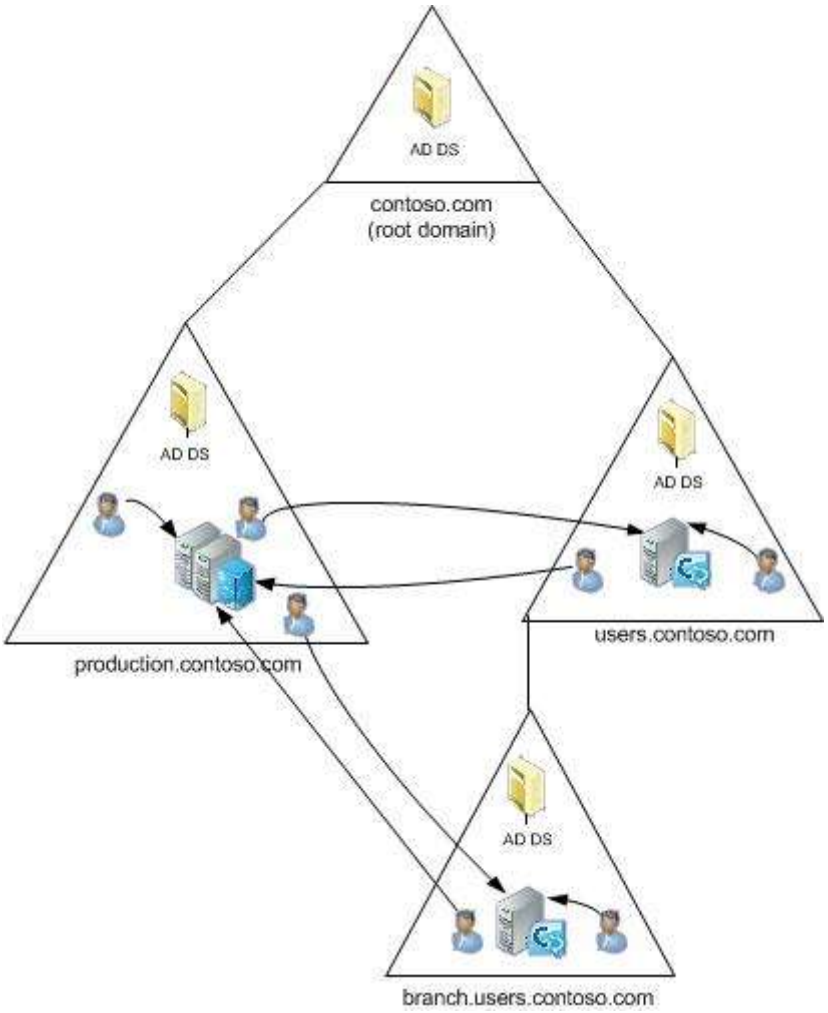


Рисунок 4.2 - Схематичне зображення лісу доменів

Для забеспечення відказостійкості у службі Active Directory, необхідно

розгорнути два або більше контролерів домену в кожному домені. Між контролерами домену забезпечується автоматична реплікація всіх змін. У разі виходу з ладу одного з контролерів домену працездатність мережі не порушується, адже продовжують працювати. Додатковий рівень відмови стійкості забезпечує розміщення серверів DNS на контролерах домену в Active Directory, що дозволяє в кожному домені отримати кілька серверів DNS, що обслуговують основну зону домену. І у разі відмови одного із DNS серверів, продовжать працювати інші.

4.2.1 Переваги служби каталогів Active Directory.

Єдина точка автентифікації

У робочій групі на кожному комп'ютері або сервері доведеться вручну додавати повний список користувачів, яким потрібний доступ до мережі. Якщо раптом один із співробітників захоче змінити свій пароль, його потрібно буде поміняти на всіх комп'ютерах і серверах. Добре, якщо мережа складається із 10 комп'ютерів, але якщо їх більше? При використанні домену Active Directory всі облікові записи користувачів зберігаються в одній базі даних і всі комп'ютери звертаються до неї за авторизацією. Усі користувачі домену включаються до відповідних груп, наприклад, «Бухгалтерія», «Фінансовий відділ». Достатньо один раз задати дозволи для тих чи інших груп, і всі користувачі отримають відповідний доступ до документів та програм. Якщо в компанію приходить новий співробітник, для нього створюється обліковий запис, що входить до відповідної групи, – співробітник отримує доступ до всіх ресурсів мережі, до яких йому має бути дозволено доступ. Якщо працівник звільняється, то достатньо заблокувати – і він одразу втратить доступ до всіх ресурсів (комп'ютерів, документів, додатків).

Єдина точка управління політиками

У робочій групі всі комп'ютери є рівноправними. Жоден з комп'ютерів неспроможна керувати іншим, неможливо проконтролювати дотримання єдиних політик, правил безпеки. При використанні єдиного каталогу Active Directory всі користувачі та комп'ютери ієрархічно розподіляються по організаційних підрозділах, до кожного з яких застосовуються єдині групові політики. Політики дають змогу встановити єдині налаштування та параметри безпеки для групи комп'ютерів та користувачів. При додаванні в домен нового комп'ютера або користувача він автоматично отримує настройки, що відповідають прийнятим корпоративним стандартам. За допомогою політик можна централізовано призначити користувачам мережні принтери, встановити необхідні програми, встановити параметри безпеки браузера, налаштувати програми Microsoft Office.

Підвищений рівень інформаційної безпеки

Використання служб Active Directory значно підвищує рівень безпеки мережі. По-перше – це єдине та захищене сховище облікових записів. У доменному середовищі всі паролі доменних користувачів зберігаються на виділених серверах контролерах домену, які зазвичай захищені від зовнішнього доступу. По-друге, при використанні доменного середовища для аутентифікації використовується протокол Kerberos, який є значно безпечнішим, ніж NTLM, що використовується в робочих групах.

Інтеграція з корпоративними додатками та обладнанням

Великою перевагою Active Directory є відповідність стандарту LDAP, який підтримується іншими системами, наприклад, поштовими серверами (Exchange Server), проксі-серверами (ISA Server, TMG). Причому це не обов'язково лише продукти Microsoft. Перевага такої інтеграції полягає в тому, що користувачеві не потрібно пам'ятати велику кількість логінів і паролів для доступу до тієї чи іншої програми, у всіх додатках користувач має одні й ті самі облікові дані – його автентифікація відбувається в єдиному каталозі Active Directory. Windows Server для інтеграції з Active Directory надає протокол RADIUS, який підтримується великою кількістю мережного

обладнання. Таким чином, можна, наприклад, забезпечити автентифікацію доменних користувачів при підключенні з VPN ззовні.

Єдине сховище конфігурації програм

Деякі програми зберігають свою конфігурацію в Active Directory, наприклад, Exchange Server. Розгортання служби каталогів Active Directory є обов'язковою умовою для роботи цих програм. Зберігання конфігурації програм у службі каталогів є вигідним з точки зору гнучкості та надійності. Наприклад, у разі повної відмови сервера Exchange, вся його конфігурація залишиться недоторканою. Для відновлення працездатності корпоративної пошти достатньо буде інсталювати Exchange Server в режимі відновлення.

Підбиваючи підсумки, хочеться ще раз акцентувати увагу на тому, що служби Active Directory є серцем IT-інфраструктури підприємства. У разі відмови вся мережа, всі сервери, робота всіх користувачів будуть паралізовані. Ніхто не зможе увійти до комп'ютера, отримати доступ до своїх документів та програм. Тому служба каталогів повинна бути ретельно спроектована і розгорнута, з урахуванням всіх можливих нюансів, наприклад, пропускної спроможності каналів між філією або офісами компанії (від цього залежить швидкість входу користувачів в систему, а також обмін даними між контролерами домену).

4.3 Аналоги Active Directory

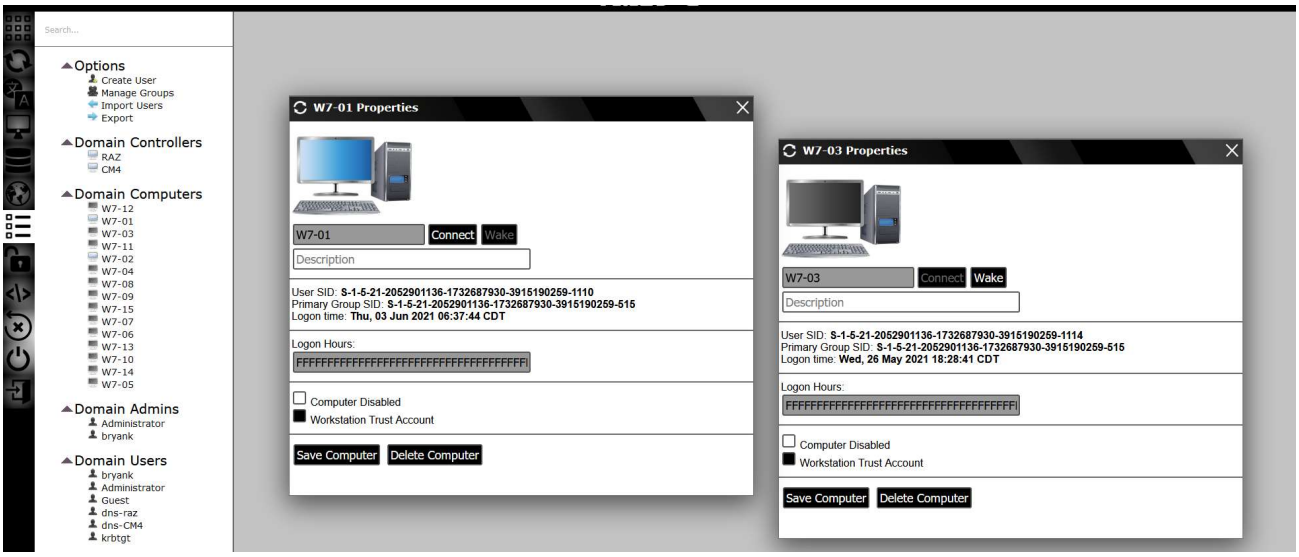
Є багато можливостей щодо забезпечення конфіденційності в операційній системі Windows. Однак якщо ви хочете домогтися того, щоб ваш сервер був надійно захищений від сторонніх людей, потрібно застосовувати Microsoft AD - принаймні, у більшості фірм вибирають саме цей варіант. Її наявність дозволяє зробити так, що система буде доступна лише співробітникам IT-підрозділу та працівникам компанії.

MAD є базою даних, розробленою компанією Microsoft. IT-підрозділу необхідно отримати доступ до Microsoft Active Directory на комп'ютері, керованому Windows Server, і вона виконуватиме функції доменного контролера. Всім мережевим користувачам доведеться звертатися до цього контролера для отримання входу до системи.

У цьому розділі будуть описані та порівняні 3 найпопулярніші альєрнативи, які розробники надають безкоштовно.

RazDC- Це активна заміна каталогів, створена CentOS + Samaba4. Включає до себе підтримку сервісів Directory, DNS, DCHP і NTP. ПЗ інтегрується з MAD і має нескладний інтерфейс, що підлаштовується під всі розміри екранів. Мінусом програми є те, що вона поступається в потужності іншим програмним забезпеченням з цієї добірки. Проте якщо компанія зацікавлена у легковажній альтернативі MAD, то рекомендується використовувати саме RazDC Особливості:

– Контролер домену Active Directory, сумісний з MS
– Внутрішній сервер доменних імен
– Перенаправлення DNS
– DHCP
– Веб-інтерфейс користувача
– Ведення журналу
– Звітність



Рисинок 4.3 - інтерфейс RazDC

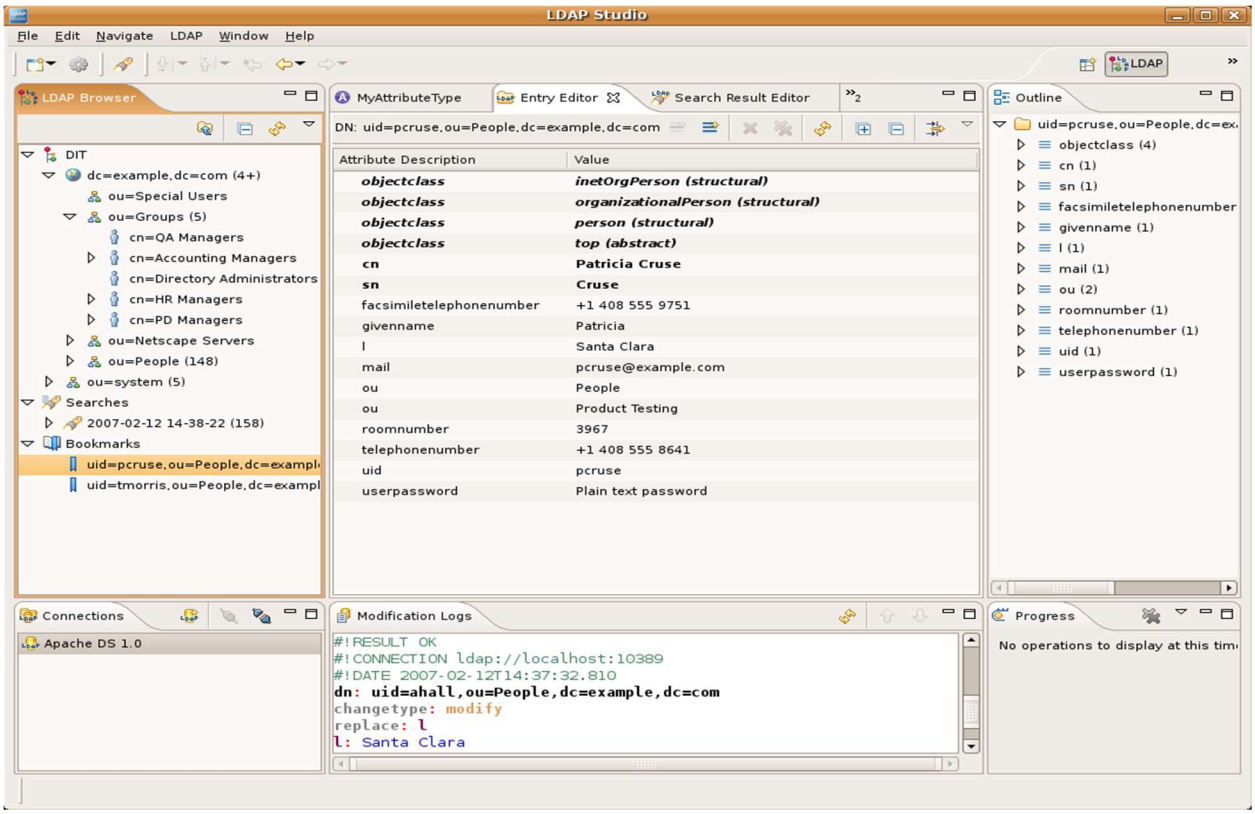


Рисунок 4.4 - Інтерфейс ApacheDS

ApacheDS ™ - це сервер, що розширюється і вбудовується каталогів, повністю написаний на Java, який був сертифікований LDAPv3 сумісним з Open Group. Крім LDAP, він підтримує Kerberos 5 і протокол зміни пароля. Він був розроблений для впровадження тригерів, збережених процедур, черг та уявлень у світ LDAP, якому не вистачало цих багатих конструкцій.

Samba – це стандартний пакет сумісності Windows для програм для Linux та Unix. З 1992 року Samba надає безпечні, стабільні та швидкі служби друку та друку для всіх клієнтів, які використовують протокол SMB/CIFS, такі як усі версії DOS та Windows, OS/2, Linux та багато інших. Samba є важливим компонентом для безшовної інтеграції Linux / Unix-серверів та настільних комп'ютерів у середовищі Active Directory з використанням демона winbind.

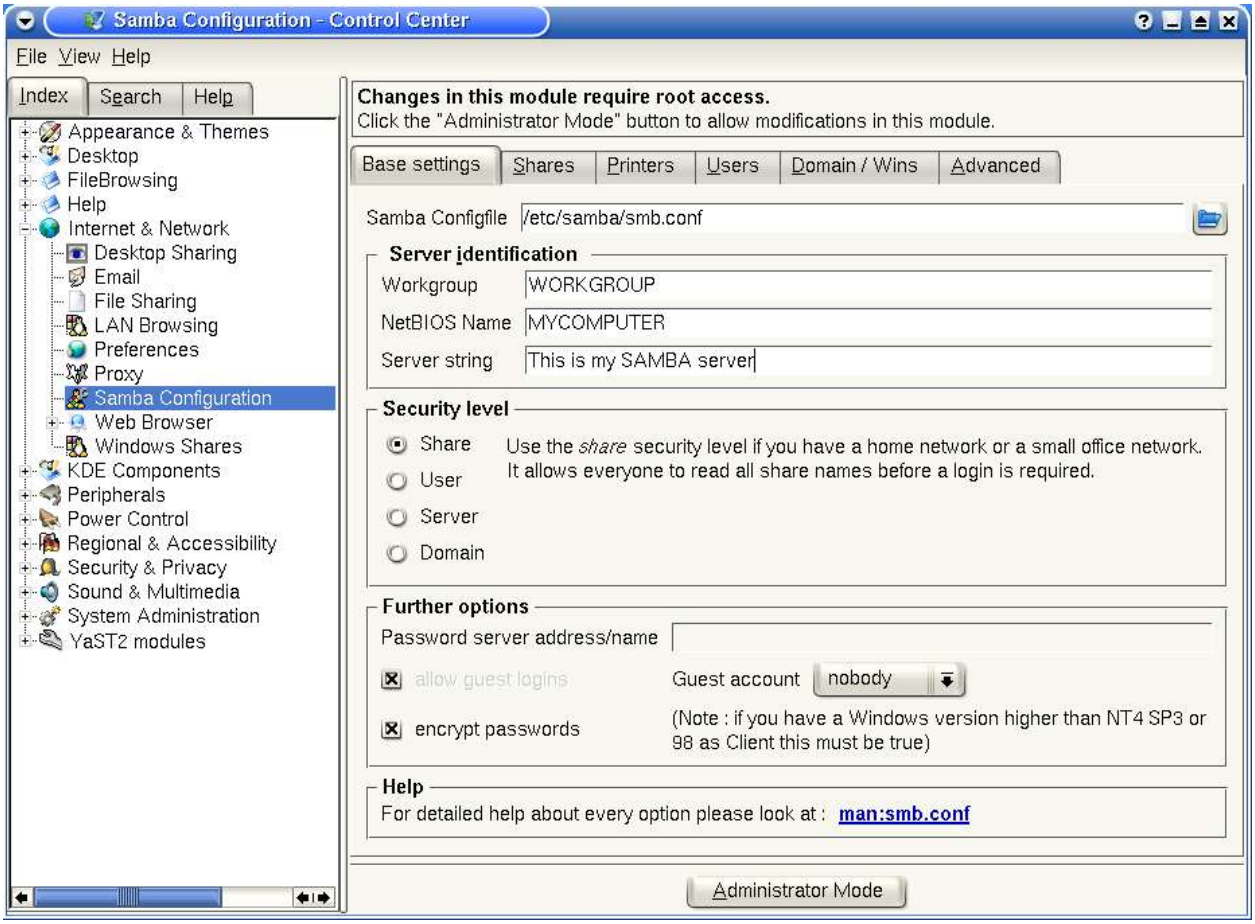


Рисунок 4.5 – Інтерфейс Samba

4.4 RADIUS сервер

Протокол служби дистанційної аутентифікації користувачів по комутов аних лініях (RADIUS) був розроблений корпорацією Livingston Enterprises як протокол аутентифікації та обліку для сервера доступу. Специфікація RADIU S RFC 2865 замінює RFC 2138. Стандарт обліку RADIUS RFC 2866 замінює RFC 2139 [9].

З'єднання між сервером доступу до мережі (NAS) та сервером RADIUS засноване напротоколі UDP (User Datagram Protocol). У загальному вигляді п

ротокол RADIUS представляєсобою службу без встановлення з'єднання. Пит ання, пов'язані з доступністю сервера,повторною передачею та часом очікува ння, вирішуються пристроями з підтримкою RADIUSкраще, ніж протоколом передачі.

RADIUS – протокол типу клієнт-сервер. Клієнт RADIUS зазвичай є

сервер NAS, а сервер RADIUS – процес демон на комп'ютері з ОС Windows NT або UNIX.Клієнт передає відомості про користувача зазначеним серверам RADIUS та виконує різні дії в залежності від поверненої відповіді. Сервери RADIUS приймають запити підключення користувачів, виконують автентифікацію користувачів та повертають дані про конфігурацію, необхідні для обслуговування користувачаклієнтом. Сервер RADIUS може діяти як проміжний для інших серверів RADIUS або сервери автентифікації іншого типу.

Користувач ініціалізує автентифікацію PPP із сервером NAS. NAS запитує ім'я користувача та пароль (для протоколу аутентифікації пароля [PAP]) або хеш-рядок (для протоколу аутентифікації з непрямим погодженням [CHAP]). Користувач надсилає відповідь.

Клієнт RADIUS надсилає серверу RADIUS ім'я користувача та зашифрований пароль.

Сервер RADIUS видає одну з відповідей: Accept (прийнято), Reject (відхилено) або Challenge (потрібна вторинна автентифікація).

Клієнт RADIUS вибирає дію залежно від служб та їх параметрів, об'єднаних із повідомленнями Accept або Reject.

Аутентифікація та авторизація

Сервер RADIUS може підтримувати багато методів автентифікації користувача. Для автентифікації імені користувача та пароля, що надаються серверу, можуть використовуватись протоколи PPP, PAP, CHAP, вхід UNIX та інші механізми автентифікації.

Зазвичай процес входу користувача складається з передачі запиту (Access-Request) сервера NAS на сервер RADIUS та отримання відповідної

відповіді з сервера (AccessAccept або Access-Reject). Пакет Access-Request містить ім'я користувача, зашифрований пароль, IP-адреса сервера NAS та порт. Спочатку сервери RADIUS розміщувалися на UDP-порту 1645, що створювало конфлікт зі службою datametrics. За цей конфлікт документ RFC 2865 офіційно закріпив за протоколом RADIUS порт 1812. Більшість пристроїв та програм Cisco підтримують обидва набори номерів. Формат запиту також містить інформацію про тип сеансу, який збирається ініціювати користувач. Наприклад, якщо запит подано в символьному режимі, то висновок повинен виглядати як Service-Type = Exec-User, але якщо запит представлений у пакетному режимі PPP, то висновок виглядає як Service Type = Framed User та Framed Type =PPP.

Після отримання від NAS запиту Acceess-Request сервер RADIUS здійснює пошук вказаного імені користувача у базі даних. Якщо ім'я користувача не знайдено в базі даних, це означає, що завантажено профіль за промовчанням, або сервер RADIUS негайно надсилає повідомлення Access-Reject. Це повідомлення Access-Reject може супроводжуватись текстовим повідомленням, у якому вказується причина відмови у доступі.

У RADIUS автентифікація та авторизація об'єднані. Якщо ім'я користувача знайдено та пароль правильний, сервер RADIUS повертає підтвердження доступу, включаючи список пар "атрибут-значення", які описують параметри, необхідні для цього сеансу.

Серед типових параметрів: тип служби (сеанс інтерпретатора чи кадрування), тип протоколу, призначений користувачеві IP-адреса (статична або динамічна), Список доступу, що застосовується, або статичний маршрут для установки в таблицю маршрутизація NAS. Дані конфігурації на сервері RADIUS визначають компоненти, які будуть встановлені на сервер NAS. Рисунок нижче показує автентифікацію RADIUS та послідовність авторизації.

Функції обліку протоколу RADIUS можуть використовуватись незалежно від функцій автентифікації чи авторизації RADIUS. Облікова

функція RADIUS дозволяє надсилати дані на початку та в кінці сеансів, відображаючи ресурси (такі як час, пакети, байти тощо). використані під час сеансу. Для задоволення потреб безпеки та білінгу постачальник послуг Інтернету (ISP) може використовувати ПЗ RADIUS з управління доступом та обліку. У більшості пристроїв Cisco як порт RADIUS використовується порт 1646, але також може бути обраний номер 1813 (по причини зміни номерів портів, закріпленого документом RFC 2139).

Справжність транзакцій між клієнтом та сервером RADIUS підтверджується за допомогою загального секретного ключа, що ніколи не пересилається по мережі. Крім того, обмін паролями користувачів між клієнтом та сервером RADIUS виконується у зашифрованому вигляді для виключення ймовірності перехоплення пароля користувача зловмисниками через прослуховування незахищеної мережі.

4.5 Порівняння сучасних RADIUS серверів

Щоб вибрати оптимальний за всіма параметрами RADIUS-сервер, необхідно розглянути та порівняти існуючі сервери. Оскільки RADIUS сервером є прикладне програмне забезпечення, необхідно розглянути найбільш популярні з них: Radiator steal belt radius server, Softpi radius, Cisco ISE.

Radiator Steal Belt Сервер RADIUS.

Радіатор підтримує широкий спектр функцій, яких немає в інших серверах RADIUS:

− максимальна гнучкість та можливість налаштування з веб-графічного інтерфейсу та моніторингу;

− підтримується понад шістдесят різних методів аутентифікації, які можуть бути змішаними, щоб задовольнити майже будь-яку вимогу аутентифікації;

− необмежену кількість користувачів;

− продуктивність та масштабованість для великих систем;

− підтримка IPv4 та IPv6 на RADIUS, проксі-сервер, TACACS+, SNMP;

− підтримка VOIP аутентифікації: сумісна з Asterisk, SIP Express.

Підтримує кілька методів автентифікації EAP, які використовуються у бездротових локальних мережах 802.1X. Це означає, що можна легко настроїти безпечну автентифікацію бездротового зв'язку. Може виступати як шлюз між клієнтами PEAP-mschapv2 і не-EAP серверів RADIUS. Підтримує Novell Edirectory із універсальними паролями. Універсальні паролі можна використовувати з PAP, CHAP, MSCHAP, mschapv2, TLS, TTLS-*, PEAP, EAP-MD5 і т.д.

Підтримує кілька методів автентифікації EAP, які використовуються у бездротових локальних мережах 802.1X. Це означає, що можна легко настроїти безпечну автентифікацію бездротового зв'язку. Може виступати як шлюз між клієнтами PEAP-mschapv2 і не-EAP серверів RADIUS. Підтримує Novell Edirectory із універсальними паролями. Універсальні паролі можна використовувати з PAP, CHAP, MSCHAP, mschapv2, TLS, TTLS-*, PEAP, EAP-MD5 і т.д.

Простий у створенні веб-звітів для аналізу сесій. Підтримує SNMP Radius IETF MIB Сервера: збирає статистику із сервера за SNMP. Повний набір алгоритмів балансування навантаження для проксі-серверів RADIUS. Автоматично розподіляє IP-адреси з бази даних SQL і DHCP. Підтримує ADSL. Підтримує GPRS.

Цей продукт є кросплатформним, що дає можливість розгортати сервер практично на будь-якій операційній системі:

− будь-який Unix, включаючи Linux (Red Hat, Debian, Mandrake, SuSE, Lindows, Slackware, Ubuntu тощо на Intel, Sparc, PPC, HP-PA тощо), FreeBSD, NetBSD, SunOS, AIX, IRIX, SCO Open Server, Digital, HP-UX тощо;

− solaris 8, 9, 10. 32-bit або 64-bit. SPARC або Intel;

− windows 95, 98, NT, 2000, ME, XP, 2003, 2008 тощо;

− mac OS9, Mac OS X;

Radiator працює з будь-якою базою даних SQL, яка має Perl DBD підтримку:

− informix;

− Sybase;

− MySQL;

− Microsoft SQL, включаючи версії 6.5, 7, 2000 та 2005;

− ODBC;

− SAP;

− PostgreSQL;

− SQLite.

Radiator підтримує багато систем білінгу, включаючи:

− enableIP (раніше Hawk-i);

- billmax;

− ISPBill;

− розширений білінг ISP;

- опера micros-fidelio;

− система управління майном;

− виставлення рахунків провайдером реактивного Інтернету.

SoftPI RADIUS.

Система SoftPI RADIUS є RADIUS-сервером, що працює під операційними системами Windows і призначений для виконання функцій аутентифікації, авторизації та обліку користувачів при підключенні та використанні ресурсів інтернет/інтранет відповідно до RFC 2865, 2866, 2868, 2869, 2548, 57 SoftPI RADIUS сервер може використовуватися для провідних та бездротових (Wi-Fi) користувачів, для користувачів VPN мереж та інших мережевих ресурсів.

SoftPI RADIUS сервер є реалізацією сервера RADIUS для операційних систем сімейства Windows 2000/XP/2003/Vista/2008/7. Підтримуються

основні функції сервера RADIUS: автентифікація (Authentication), авторизація (Authorization) та облік використовуваних ресурсів (Accounting).

Підтримуються наступні протоколи аутентифікації користувачів:

− PAP;

− CHAP;

− MS CHAP v2;

− EAP-MD5;

− EAP-MS-CHAP v2;

− PEAP MS CHAP v2.

Гнучке настроювання параметрів автентифікації та авторизації користувачів:

− значення атрибутів користувача прив'язуються до пристрою доступу;

− можливість завдання правила для перевірки значення атрибута;

− підтримуються специфічні атрибути производителя (Vendor-Specific attributes). Система містить понад 30 атрибутів шаблонів різних виробників: 3COM, Alcatel, Cisco, Juniper, HP, Microsoft, Avaya-Nortel.

У SoftPI RADIUS сервер реалізовано облік використовуваних користувачами ресурсів відповідно до RFC 2866, що може використовуватися при взаємодії з системами білінгу. Ця функція інтегрована із білінговим комплексом Tariscope 3.5 (SoftPI).

Усі налаштування параметрів SoftPI RADIUS здійснюються у зручному графічному інтерфейсі. Існує можливість контролювати сесії користувачів: можливість розриву сесії користувача шляхом завдання її тривалості.

Є можливість створення груп користувачів, які мають однакові атрибути. При цьому конкретному користувачеві, який входить до якоїсь групи, можна додати додаткові атрибути, не включені до списку атрибутів групи.

SoftPI RADIUS підтримує можливість синхронізації користувачів та їх атрибутів, використовуючи протокол LDAP, наприклад з Active Directory.

SoftPI RADIUS містить режим, що забезпечує отримання інформації щодо його роботи. При цьому адміністратор SoftPI RADIUS може за допомогою фільтра встановити будь-які умови фільтрації інформації та застосувати складні умови сортування інформації.

Звіт може бути експортований в один із таких форматів: PDF, Excel (Microsoft), HTML, текстовий. Є можливість попереднього перегляду звіту та його роздруківки.

З міркувань безпеки сервер SoftPI RADIUS адмініструється за допомогою протоколу SSL. Дія цього протоколу заснована на сертифікаті. Використання такого сертифіката дозволяє аутентифікувати сервер і зашифрувати обмін даними під час адміністрування. Ви можете придбати сертифікат у центрі сертифікації, використовувати корпоративний сертифікат, підписаний довіреним центром сертифікації, або використовувати самопідписаний сертифікат.

З метою захисту від атак на SoftPI RADIUS сервер у ньому передбачено можливість блокування користувача у разі багаторазових невдалих спроб аутентифікації.

Cisco ISE

Cisco Identity Services Engine (Cisco ISE)— це багатофункціональне рішення, що закриває повний спектр питань контролю доступу до корпоративної мережі [КД]. Централізація політик доступу до мережі та автоматизація безлічі рутинних завдань – основні переваги рішення Cisco ISE. [13]

Більшість організацій мають корпоративний каталог — єдине місце зберігання даних про користувачів. Найчастіше це Microsoft Active Directory (MS AD), але можливо і LDAP сервер. Зручно заводити користувачів в одному місці та керувати більшістю налаштувань їхнього робочого оточення. Багато систем можуть отримувати дані з активного каталогу: поштовий сервер, CRM та ін. Проблема в тому, що "мережа", як сутність, в

активному каталозі проводити аутентифікацію не вміє. Має бути проміжний пристрій, який розуміє, наприклад, MS AD і мережу.

RADIUS — один із найстаріших та найпоширеніших протоколів мережної автентифікації. Для аутентифікації користувачів у мережі повинен бути розгорнутий сервер RADIUS.

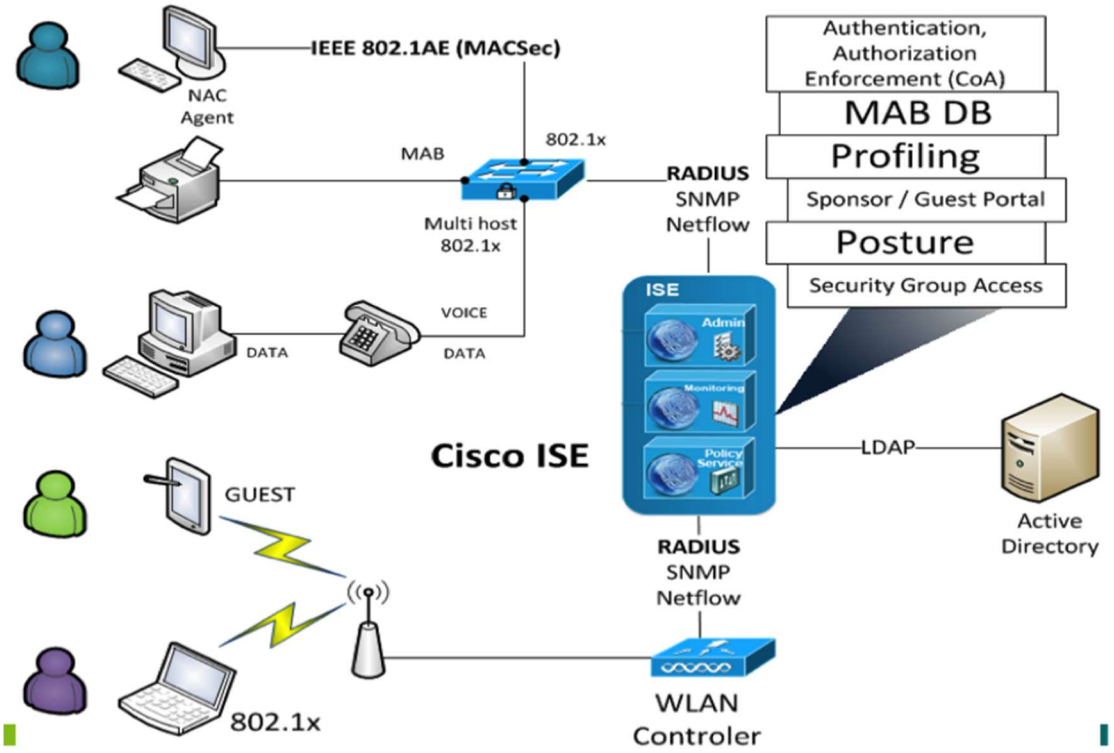


Рисунок 4.6 - Приклад архітектури рішення КД на базі Cisco ISE

У сучасних дизайнах мереж Cisco роль такого сервера RADIUS виконує Cisco ISE. Крім цього, Cisco ISE дозволяє автоматизувати безліч завдань, які неминуче виникають спільно з проектами впровадження сервера RADIUS для контролю доступу до мережі.

Cisco ISE дозволить вирішити цілий комплекс завдань, пов'язаних із КД.

Підвищення спостерігальності та швидкості реакції мережі Для підвищення спостерігальності та швидкості вирішення проблем доцільно впровадити єдине рішення, глибоко інтегроване в існуючу інфраструктуру і

що пов'язує усі політики доступу на мережевому обладнанні. Таке завдання для IT-підрозділів вирішує Cisco ISE.

Централізація та спрощення управління КД

Cisco ISE дозволяє досягти спрощення та централізація політики мережного доступу.

Корпоративна інформація має власну цінність. Контроль доступу до мережі – один із засобів захисту інформації. За такого різноманіття варіантів підключень ручне управління політиками стає трудомістким. Це робить значні затримки на швидкість реакції мережі на зміни. Деякі завдання, такі як моніторинг стану підключень до мережі в реальному часі і ретроспективі, не здійсненні вручну і однозначно вимагають розробки будь-яких скриптів і зведення всіх їх функцій в одну систему управління. Підтримка таких рішень стає з часом непосильною ношею для IT. Щоб мати впевненість у тому, що у мережі підприємства лише довірені пристрої потрібна централізація управління політиками мережі та глибока інтеграція коїться з іншими мережевими сервісами.

Автоматизація рутинних завдань

Значно скоротивши операційні витрати, можна підвищити ефективність роботи IT та підприємства загалом. Впровадження засобів автоматизації мережевих політик доступу дозволить розділити завдання та зони відповідальності IT та ІБ. Витрати часу на внутрішні та зовнішні аудити також можуть бути зведені до мінімуму. Вся облікова інформація зберігається одному місці. Завжди можна оцінити поточний стан.Використання рішення автоматизації контролю доступу Cisco ISE дозволить зменшити операційні витрати на супровід всіх мережевих сервісів.

Варто відмітити щовикористання Cisco ISE дозволить значно знизити витрати на ЦОД за рахунок застосування нових архітектур та технологій (TrustSec/SGT). Важливо мати єдине рішення, що пов'язують політики доступу різних пристроях: свічі доступу, фаєрволли, інфраструктура ЦОД.

Завдяки Cisco ISE є можливість розмежувати доступ за багатьма критеріями:

– хто повинен мати доступ;

– з яких пристроїв;

– у який час доби;

– через які мережеві пристрої;

– який рівень доступу потрібний.

Все це визначає контекст доступу до мережі.

Cisco ISE робить можливим глибоко інтегрувати поняття контексту мережного доступу (хто? як? звідки? з якого пристрою?) у широкий набір мережевих рішень та рішень інформаційної безпеки.

Рисунок 4.7 - Приклад політики з урахуванням контексту доступу до мережі

Також слід відмітит що Cisco ISE у порівнянні з Radiator steal belt radius server та Softpi radius є копмлексним рішенням та надає й інші переваги компанії Cisco, як постійне оновлення, швидкий відклик від технічної підтримки та вісоку відказустійкість. Також ключевим у виборі Cisco ISE є єдина екосистема котру не можуть надати інщі вендори. Однією з переваг Cisco ISE є можливість перевіриння підлінності софту перед наданням йому доступу до мережі. Перевірка виконується за допомогую VPN клієнту на пристрої також від вендора Cisco а самє Anyconnect у котрому модуль Posture check, який можливо настроїти на перевірку різноманітних пунктів.

Висновки до розділу 4

В четвертій главі кваліфікаційної роботи були розглянуті та описані принципи роботи доменних служби авторизації та розподілених баззи данних.

Було надано поняття домену та служби каталогів Active Directory

Розглянуті принципи роботи служби каталогів Active Directory перелiковані її переваги, та розглянуті можливості роботи у дереві домену та у лісі домену. Були наданя аналоги служби каталогів Active Directory, а саме: RazDC, ApacheDS ™,Samba. Перечислені їх основні фонкції.

В порівнянні за іншими службами каталогів для аутсорсингових компаній в IT-інфраструктурі яких використовується більше 30% компьютерів за опереційною системою Windows рекомендовано використовувати служби каталогів Active Directory.

Якщо аутсорсингова компанія базуеється на використанні операційних систем на базі Unix слід використовувати служби каталогів за можливістю ввдоу до домену Unix систем на приклад Samba.

Був описан протокол RADIUS та сфера його застосування було наведено прицип роботи RADIUS серверу за базою данних служби каталогів Active Directory. Були порівняні між собою RADIUS сервери: Radiator steal

belt radius server, Softpi radius, Cisco ISE. Описані їх ключеві відмінності та переваги з недоліками. Основючись на перевагах Cisco ISE він рекомендован для використання для аутсорсингових компаній за свою гнучкість там більший спектр мережевих конфігурацій. В 5 главі квалікафіційної роботи буде розглянут VPN кліенє від вендора Cisco основючись на рекомендованому RADIUS сервері Cisco ISE.

5 ВИКОРИСТАННЯ VPN У ІТ КОМПАНІЯХ

5.1 Поняття VPN

VPN – Virtual Private Network – віртуальна приватна мережа це сукупність технологій, що дозволяють забезпечити одне або кілька мережевих з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет). [4].

Розшифровка назви: мережа – об'єднання кількох пристроїв будь-яким видом зв'язку, що дозволяє обмінюватися інформацією. Віртуальна – невловима, не фізична, тобто не важливо, якими саме каналами зв'язку вона прокладена. Фізична та логічна топології можуть як збігатися, так і відрізнятися. Приватна - в цю мережу не може увійти сторонній користувач, там знаходяться ті, кому дозволили доступ. У приватній мережі треба маркувати учасників та їх трафік, щоб відрізнити його від решти чужої інформації. Також у такій мережі забезпечується захист даних криптографічними засобами, простіше кажучи, шифрується.

Наведемо ще одне визначення: VPN – це сервіс, що дозволяє захистити приватні дані під час користування Інтернетом.

Навіщо потрібний VPN:

– Для віддаленої роботи. Наприклад, ви працюєте з дому. За VPN ви можете отримати доступ до сервісів та документації своєї організації, при цьому з'єднання буде безпечнішим, дані буде складно перехопити та розшифрувати.

– Щоб поєднати різні частини однієї компанії. Офіси можуть бути віддалені один від одного на будь-яку відстань.

– Усередині компаній – для об'єднання та ізоляції відділів.

– При підключенні до Wi-fi у кафе, метро тощо, щоб хакери не могли вкрасти копроративні дані. При користуванні публічною мережею

безпечно, хіба переглядати сайти в браузері. А ось якщо використовувати соц.мережі, зловмисник може не тільки перехопити вашу конфіденційну інформацію, але й використовувати її у своїх цілях, авторизувавшись у цій соцмережі від Вашого імені. Ще гірше, якщо йому вдасться зламати пошту. Тоді атаці піддадуться всі програми, прив'язані до цієї поштової скриньки. Але найнеприємнішим може виявитися витік даних вашої банківської картки, якщо ви вирішили перевести комусь гроші, підключившись до безкоштовного Wi-fi.

З'єднання VPN – це так званий “тунель” між комп'ютером користувача та комп'ютером-сервером. Кожен вузол шифрує дані до їхнього потрапляння в “тунель”

Ви підключаєтеся до VPN, система ідентифікує вашу мережу і починає автентифікацію (порівняє введений пароль із паролем у своїй базі даних).

Далі сервер Вас авторизує, тобто надає право виконання певних дій: читання пошти, інтернет-серфінг тощо. Після встановлення з'єднання весь трафік передається між вашим ПК та сервером у зашифрованому вигляді. Ваш ПК має IP-адресу, надану інтернет-провайдером. Цей IP блокує доступ до деяких сайтів. VPN сервер змінює ваш IP на свій. Вже з VPN-сервера всі дані передаються до зовнішніх ресурсів, які ви запитуєте. Тепер можна переглядати будь-які ресурси та не бути відстеженим.

Проте слід пам'ятати, що не вся інформація шифрується. У різних VPN-провайдерів можуть відрізнятися такі характеристики як ступінь шифрування, приховування факту підключення до сервера, зберігання логів (журнал, в якому зберігається інформація про сайти, реальні IP адреси тощо) і співробітництво при видачі інформації третім особам.

Якщо VPN-провайдер взагалі не записує логи, то передавати третім особам нічого. А приховування факту підключення до сервера – вже рідкісна послуга. При некоректному підключенні або різкому розриві з'єднання може статися витік частини даних. Вирішити проблему допоможе технологія

Multihop VPN, яка передбачає з'єднання із сайтом одразу через кілька серверів.

Розглянемо популярні VPN**:**

PPTP – протокол тунелювання «точка-точка». Використовується, коли захист даних не дуже важливий або немає інших варіантів.

Переваги:

– Підтримується усіма ОС

– Не вимагає багато обчислювальних потужностей

Недоліки:

– Погана захищеність. Методи шифрування застаріли, погана архітектура, є помилки у реалізації протоколу від Microsoft. За замовчуванням немає шифрування, на злом потрібно менше доби.

L2TP – протокол тунелювання рівня 2. Працює спільно з іншими протоколами, найчастіше IPSec. Використовується інтернет-провайдерами та корпоративними користувачами.

Переваги:

– Ефективніший для побудови віртуальних мереж

Недоліки:

– Більш вимогливий до обчислювальних ресурсів

– Не передбачає шифрування за умовчанням

IPSec – Internet Protocol Security – група протоколів та стандартів для безпечних з'єднань. Часто використовується разом із іншими технологіями.

Переваги:

– Хороша архітектура

– Надійність алгоритмів

– Прискорення алгоритму шифрування AEC

Недоліки:

– Складений у налаштуванні (отже, зниження захисту, якщо налаштувати неправильно)

– Вимагає багато обчислювальних ресурсів

SSL - Secure Sockets Layer & TLS - Transport Layer Security - група методів, що включає протоколи SSL і TLS та інші методи захисту. Використовується на веб-сайтах, URL яких починається з https деякі реалізації: OpenVPN, Microsoft SSTP.

Переваги:

– Безперешкодно пропускаються більшістю публічних мереж

– OpenVPN має відкритий код, реалізований практично для всіх платформ, вважається дуже надійним.

Недоліки:

– Досить низька продуктивність

– Складність у налаштуванні, необхідність встановлення додаткового ПЗ

VPN – комплекс технологій, що дозволяють створити логічну мережу поверх фізичної. Використовується для захисту трафіку від перехоплення зловмисниками та безпечної діяльності в Інтернеті. VPN відкриває доступ до заблокованих ресурсів, так що багато хто готовий миритися з нижчою швидкістю інтернету та можливими логами програм. Хоча VPN використовує досить надійні алгоритми шифрування, включення VPN-клієнта на ПК не гарантує 100% збереження конфіденційної інформації, тому слід уважно поставитися до вибору VPN-провайдера.

5.2 VPN клієнт Cisco AnyConnect

Cisco AnyConnect є логічним розвитком Cisco VPN Client, який за багато років не тільки був русифікований, але й збагатився безліччю різних функцій та можливостей для захищеного віддаленого доступу до корпоративної або хмарної інфраструктури за допомогою одного з трьох протоколів – TLS, DTLS та IPSec (підтримується також FlexVPN). Перший є

досить традиційним для VPN-клієнтів і використовує TCP як транспортний для своєї роботи. Проте тунелювання через TLS означає, що програми, засновані на TCP, дублюватимуть його (один раз для організації TLS, другий — для своєї роботи вже всередині TLS). А протоколи на базі UDP... все одно використовуватиме TCP. Це може призвести до певних затримок, наприклад, для мультимедіа-програм, які є дуже популярними при віддаленій роботі. Вирішенням цієї проблеми стала розробка протоколу DTLS, який замість TCP використовує UDP для роботи TLS. AnyConnect підтримує обидві реалізації TLS — на базі TCP та UDP, що дозволяє гнучко використовувати їх залежно від умов віддаленої роботи. Зазвичай TCP/443 або UDP/443 дозволені на міжмережевих екранах або проксі і тому використання TLS та DTLS не є великою проблемою. Але часом може знадобитися застосування протоколу IPSec, який також підтримується AnyConnect'ом (IPSec/IKEv2).

Пристрої на котрих може термінуватися VPN-тунель:

- Міжмережеві екрани Cisco ASA 5500 та Cisco ASA 5500-X
- Багатофункціональні захисні пристрої Cisco Firepower
- Віртуальні MCE Cisco ASAv та Cisco ASAv в AWS та Azure
- Маршрутизатори Cisco ISR 800/1000/4000 та ASR 1000 с мережної ОС Cisco IOS або Cisco IOS XE
- Віртуальні маршрутизатори Cisco CSR 1000v [3].

Цікаво, що, на відміну від багатьох інших VPN-клієнтів, існує безліч варіантів інсталяції Cisco AnyConnect на персональний комп'ютер або мобільний пристрій ваших працівників. Якщо ви видаєте їм такі пристрої з власних запасів або спеціально купуєте для співробітників ноутбуки, то ви можете просто встановити захисного клієнта замість іншого програмного забезпечення, необхідного для віддаленої роботи. Але що робити для користувачів, які знаходяться далеко від корпоративних IT-фахівців та не можуть надати їм свій ноутбук для встановлення потрібного програмного забезпечення? Можна, звичайно, задіяти і спеціалізоване ПЗ типу SMS, SCCM або Microsoft Installer, але у Cisco AnyConnect є і інший спосіб

установки - при зверненні до згаданого VPN-шлюзу клієнт сам завантажується на комп'ютер користувача, який працює під керуванням Windows, Linux або macOS. Це дозволяє швидко розвернути VPN-мережу навіть на особистих пристроях працівників, надісланих на віддалену роботу. Мобільні користувачі можуть просто завантажити Cisco AnyConnect з Apple AppStore або Google Play.

У AnyConnect є така функція — Always-On VPN, яка запобігає прямому доступу до Інтернету, якщо користувач не знаходиться в так званій довіреній мережі, якою може бути ваша корпоративна інфраструктура. Але зверніть увагу, що ця функція працює дуже гнучко. Якщо користувач знаходиться в корпоративній мережі, VPN автоматично вимикається, а при її залишанні (наприклад, якщо користувач працює з ноутбука, планшета або смартфона), VPN знову вмикається; причому прозоро та непомітно для користувача. Тим самим користувач завжди перебуватиме під захистом корпоративних засобів захисту, встановлених на периметрі, — міжмережевого екрану, системи запобігання вторгненням, системи аналізу аномалій, проксі тощо. Багато компаній, видаючи віддаленим працівникам корпоративні пристрої, ставлять умову використання їх лише з службових цілей. А щоб контролювати виконання цієї вимоги, включають в AnyConnect налаштування, що забороняють користувачеві ходити в Інтернет безпосередньо.

Функція Always-On VPN дуже корисна для захисту віддаленого доступу з виданих пристроїв, але далеко не завжди можливо змусити користувача робити те, що необхідно адміністраторам, особливо якщо йдеться про його особистий комп'ютер, на якому не можливо встановлювати свої правила. І користувач не захоче, щоб особистий трафік проходив через корпоративний периметр і ваші адміністратори стежили за тим, які сайти користувач відвідує під час надомної роботи.

У цьому випадку на Cisco AnyConnect можна увімкнути функцію split tunneling, тобто розділення тунелів. Одні види трафіку, наприклад, до

корпоративної інфраструктури та робочих хмар трафік шифруватиметься, а трафік до соцмереж або онлайн-кінотеатрів йтиме у звичайному режимі, без захисту з боку AnyConnect. Це дозволяє врахувати інтереси компанії та її працівників, змушених ділити персональний комп'ютер співробітника між двома областями життя — особистим та службовим. Але варто пам'ятати, що функція split tunneling може знизити захищеність вашої мережі, тому що користувач може підчепити якусь заразу в Інтернет, а потім вже захищеним каналом вона потрапить усередину компанії.

Окрім розділення трафіку за принципом «довірений/недовірений», Cisco AnyConnect підтримує функцію Per App VPN, яка дозволяє шифрувати трафік окремих програм (навіть на мобільних пристроях). Це дозволяє шифрувати (читай, пускати в корпоративну мережу) лише певні програми, наприклад, 1С, SAP, Sharepoint, Oracle, а той самий Facebook, LinkedIn або персональний Office365 пускати в обхід корпоративного периметра. При цьому для різних груп віддалених пристроїв або користувачів можуть бути правила безпеки.

З одного боку, Cisco AnyConnect може перевіряти наявність у вас системи захисту Cisco AMP for Endpoints і встановлювати її за відсутності. Але можливо, у користувача вже встановлено власний антивірус або цей антивірус вже був встановлений при перекладі працівників на віддалену роботу. Проте антивірус сьогодні ловить дуже мало серйозних загроз і непогано доповнити його більш просунутими рішеннями з виявлення шкідливих програм, аномалій та інших атак. Якщо у вашій корпоративній інфраструктурі розгорнуто рішення Cisco Stealthwatch, можна легко інтегрувати з ним і агенти Cisco AnyConnect, встановлені на домашніх комп'ютерах ваших працівників. В AnyConnect вбудований спеціальний модуль Network Visibility Module (NVM), який транслює активність вузла спеціально розроблений для цього завдання протокол nvzFlow,Netflow-колектор , яким може бути як Cisco Stealthwatch Enterprise , так і будь-який SIEM, наприклад, Splunk. Серед іншого NVM-модуль може передавати таку

інформацію, на базі якої можна виявляти аномальну та шкідливу активність на домашньому комп'ютері, яка залишилася непомітною для встановленого антивірусу:

– Дані мережевої активності у схожому з IPFIX форматі
– Ідентифікатор, адреса та ім'я пристрою
– Ім'я користувача
– Тип облікового запису користувача
– Імена та ідентифікатори процесів і додатків, що запускаються, включаючи і дані щодо їх «батьків».

Даний функціонал по суті є полегшеною UEBA (User Entity Behaviour Analytics), новою технологією аналізу поведінки користувачів і додатків/процесів, що запускаються від їхнього імені.

Коли користувачі працюють на корпоративних комп'ютерах, вони проходять автентифікацію зазвичай в Active Directory або іншому LDAP-довіднику. Хочеться отримати таку ж можливість і при віддаленому доступі і Cisco AnyConnect дозволяє її реалізувати за рахунок підтримки автентифікації за логіном/паролем, включаючи і одноразові паролі (наприклад, LinOTP), користувальницьким або машинним сертифікатам, апаратним токенам (наприклад, смарт-карт або Yubikey) , і навіть біометрії та іншим методам багатофакторної аутентифікації. Всі ці варіанти можуть бути легко інтегровані з вашими рішеннями щодо управління ідентифікацією та автентифікацією за допомогою протоколів RADIUS, RSA SecurID, SAML, Kerberos тощо.

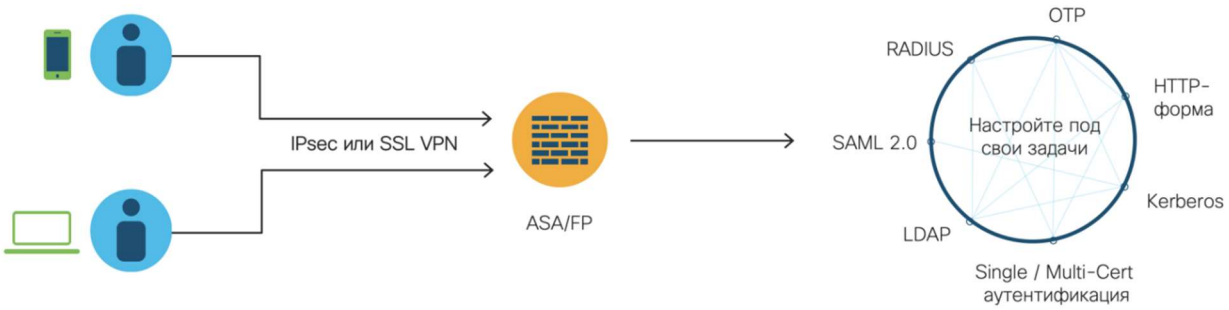


Рисунок 5.1 - Авторизація юзера за допомогою AnyConnect

У Cisco існує віртуальний маршрутизатор Cisco CSR 1000, який може бути розгорнутий у хмарному середовищі, наприклад, в Amazon AWS або MS Azure, і який може термінувати на собі VPN-тунелі, створювані Cisco AnyConnect.

Насправді Cisco AnyConnect має значно більшу кількість можливостей. Він може працювати у прихованому режимі, динамічно вибирати найбільш оптимальний шлюз віддаленого доступу, підтримує IPv6, має вбудований персональний міжмережевий екран, моніториться віддалено, забезпечує контроль доступу, підтримує RDP тощо. А ще він русифікований, щоб у користувачів не виникало питань щодо рідкісних повідомлень, які Cisco AnyConnect може видавати. Так що Cisco AnyConnect – це не просто VPN-клієнт, але набагато цікавіше рішення для забезпечення захищеного віддаленого доступу, який останніми тижнями починає набирати популярність через пандемію коронавірусу, що змушує роботодавців переводити окремі категорії своїх працівників на віддалення.

Висновки до розділу 5

В п’ятій главі кваліфікаційної роботи було надано поняття VPN та його значення для IT-компаній. Надані технології використання та відмічені можливості шифрування трафіку для забеспечення безпеки данних компаній.

Булао надо порівняння сучасних VPN: PPTP, L2TP, IPSec, SSL з переліком їх переваг та недоліків.

Був розглянут один з популярніших VPN клієнтів від вендора Cisco, а саме AnyConnect. Перелікована та пояснені його можливості необхідні для IT-компаній. Наданий переклік пристроїв на котрих може термінуватися VPN-тунель. Пояснені функції Always-On VPN Per App VPN.

Вхраховуючи переваги AnyConnect такі як можливість перевірки підліності ОС та блокування доступу до мережі у випадку відсутності певних крітерій як навність дозволеного антивіруси чи необхідного патч менеджера. Винесено рекомендації стосовно використання VPN клієнта Cisco AnyConnect для аутсорсингових компаній котрі мають достатньій обсяг користовачів та фінансування IT-підрозділу щоб використовувати AnyConnect безпосередньо в поєднанні з RADIUS сервером Cisco ISE.

ВИСНОВКИ

Метою даної кваліфікаційної роботи є розробити та дослідження розподіленої інфокомунікаційної мережі аутсорсингової компанії з можливістю широкосмугового доступу, послуг високошвидкісного доступу до мережі Інтернет, IPTV та IP телефонії.

Результатом кваліфікаційної роботи є інфокомунікаційна мережа аутсорсингової компанії, техніко-економічного обґрунтування обраних проектних рішень та компонентів мережі. Вибір ключових проектних рішень, а саме розробка топології, вибір технологій та протоколів, зменшення витрат на будування інформаційно-телекомунікаційних мереж за рахунок віртуалізації. Проведений аналіз сучасних рішень хмарних технологій. Вибір доменні служби авторизації та розподіленої баззи данних. Вибір VPN клієнту. Їх вибір проводився з урахуоїанням даних вимог.

В першому розділі кваліфікаційної роботи виконаний аналіз об’єкту проектування. Загальна кількість точок доступу до ресурсів телекомунікаційної мережі становить 4597 портів. Мережа, що проектується, надає послуги Інтернету, файлового обміну, телефонного зв’язку, відеоспостереження. На підставі загальної кількості користувачів та послуг мережі був розрахований трафік мережу в цілому та на окремі послуги. Загальне можливе навантаження на мережу складає понад 34,8 Гбіг/с. Зовнішній канал до мереж Інтернет повинен становити не менш 18,4 Гбіт/с, навантаження на устаткування IP-телефонії – 19 Мбіт/с. TV–10,8 Гбіт/с. Відеоспостереження – 2,9Гбіт/с. Wi-fi – 2,8 Гбіт/с.

В другому розділі кваліфікаційної роботи надано поняття віртуалізації. Було надо пояснення до кожного типу віртуалізації та його практичне використання для аутсорсингових компаній. Віртуалізація може підвищити швидкість IT, гнучкість і масштабованість, одночасно заощадивши значні витрати. Більша мобільність робочого навантаження, продуктивність і використання ресурсів, а також автоматизовані операції – це переваги

віртуалізації, які спрощують управління IT та знижують витрати на володіння та експлуатацію.

В третій главі кваліфікаційної роботи надано поняття хмарних сервисів. Були надані моделі розгортання хмарних технологій. Перелiковані основні властивості хмарних технологій котрі використовються у аутсорсингових компаній.Зз'ясовано важливість використання хмарних технологій, що ставить під сумнів існування деяких загроз, пов'язаних із існуванням цих технологій. Винесено рекомендації стосовно використання хмарних технологій та обчислень, завдяки чому аутсорсингові компанії можуть знизити ризики стосовно зберігання данних. Також використання хмарних технологій зменьшить витрати компанії на власний датацентр с локальними сервісами.

В четвертій главі кваліфікаційної були розглянуті та описані принципи роботи доменних служби авторизації та розподілених баззи данних. Було надано поняття домену та служби каталогів Active Directory Розглянуті принципи роботи служби каталогів Active Directory перелiковані її переваги, та розглянуті можливості роботи у дереві домену та у лісі домену. Були наданя аналоги служби каталогів Active Directory, а саме: RazDC, ApacheDS ™,Samba. Перечислені їх основні фонкції. Був описан протокол RADIUS та сфера його застосування було наведено прицип роботи RADIUS серверу за базою данних служби каталогів Active Directory. Були порівняні між собою RADIUS сервери: Radiator steal belt radius server, Softpi radius, Cisco ISE. Описані їх ключеві відмінності та переваги з недоліками. Основючись на перевагах Cisco ISE. В порівнянні за іншими службами каталогів для аутсорсингових компаній в IT-інфраструктурі яких використовується більше 30% компьютерів за опереційною системою Windows рекомендовано використовувати служби каталогів Active Directory для Unix слід використовувати служби каталогів за можливістю ввдоу до домену Unix систем на приклад Samba. Був рекомендован RADIUS сервер Cisco ISE

основючись на його перевагах для аутсорсингових компаній за свою гнучкість там білший спектр мережевих конфігурацій.

В п’ятій главі кваліфікаційної винесено рекомендації стосовно використання VPN клієнта Cisco AnyConnect для аутсорсингових компаній котрі мають достатньій обсяг користовачів та фінансування IT-підрозділу щоб використовувати AnyConnect безпосередньо в поєднанні з RADIUS сервером Cisco ISE. Було надано поняття VPN та його значення для IT-компаній. Порівняні технології використання та відмічені можливості шифрування трафіку для забеспечення безпеки данних компаній. Булао надо порівняння сучасних VPN: PPTP, L2TP, IPSec, SSL з переліком їх переваг та недоліків. Був обран один VPN клієнтів від вендора, а саме AnyConnect. Перелікованні та пояснені його можливості необхідні для IT-компаній. Наданий переклік пристроїв на котрих може термінуватися VPN-тунель. Пояснені функції Always-On VPN Per App VPN

В заключному розділі дипломного проекту були надані інструкції з охорони та безпеки життя в рамках побудови телекомунікаційної мережі офісної будівлі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. А.Ретана, Д.Слайс, Р.Уайт. Принципи проектування корпоративних IP-мереж. "Вільямс", 2002. – 368 с.

2. Семенов А.В., «Проектирование и расчет структурированных кабельных систем и их компонентов»; ДМК – 2003.;416 стр.; ISBN: 5940742106

3. А. Леінвальд. Б. Пінські. Конфігурування маршрутизаторів CISCO. "Вільямс", 2001. – 386 с.

4. В.Боллапрагада, К Мерфі, Р.Уайт. Структура операційної системи CISCO IOS. "Вільямс", 2002. – 208 с.

5. Олифер Б.В., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы (4-е издание) / Учебное пособие. Питер.: 2010г., 943с.

6. "Проектирование и внедрение компьютерных сетей. Учебный курс" Палмер, Питер-Пресс, 2004.

8. Стаття «Как работает виртуализация VMware: платформа vSphere, приложение vCenter Server и гипервизоры ESX и ESXi» [Електронний ресурс]: «market.cnews.ru». – Режим доступа: https://market.cnews.ru/news/top/2020-06-3_gipervizory_vmware_vspherevcenter – Дата доступа: грудень 2021.

9. Форум стосовно порівняння радіус серверів

[Електронний ресурс]: «opennet.ru». – Режим доступа: https://www.opennet.ru/base/cisco/radiuses.txt.html– Дата доступа: грудень 2021.

10. Сайт «lostapp.ru» з порівнянням аналогів для xen-orchestra [Електронний ресурс]: «lostapp.ru». – Режим доступа: http://lostapp.ru/soft/xen-orchestra – Дата доступа: грудень 2021

11. Стандарти Ethernet мережі [Електронний ресурс]: «wikipedia.org» - Режим доступу: https://ru.wikipedia.org/wiki/Ethernet - Дата доступу: грудень 2021.

12. Стаття «Пять проблем Active Directory» [Електронний ресурс]: «www.osp.ru» - Режим доступу: https://www.osp.ru/winitpro/2010/07/13004675 - Дата доступу: грудень 2021.

13. Стаття «Cisco Identity Services Engine» [Електронний ресурс]: «habr.com» - Режим доступу: https://habr.com/ru/company/cisco/blog/229525/ - Дата доступу: грудень 2021

14. Офіційний сайт «IQ Business Center» [Електронний ресурс]: «http://iqbc.ua/» - Режим доступу: http://iqbc.ua/ru/ - Дата доступу: грудень 2021

ДОДАТОК А

Охорона праці та безпека при надзвичайнихситуаціях на підприємстві

А.1 Характеристика умов праці науково-дослідного відділу аутсорсингової компанії

Робочим приміщенням, у якому розташовано науково-дослідний відділ, є кімната розмірами 10 метрів на 4,5 метрів. У приміщенні розташовані 1 комп’ютер потужністю 0,5 кВт/год., 2 монітор потужністю 0,1 кВт/год., 1 ноутбук потужністю 0,09 кВт/год, 1 принтер потужністю 0,4 кВт/год., генератор сигналів потужністю 0,06 кВт/год., осцилограф потужністю 0,05 кВт/год., паяльна станція потужністю 0,6 кВт/год, 4 лабораторні блоки живлення потужністю 0,20 кВт/год., 1 кондиціонер потужністю 4 кВт/год.

Приміщення знаходиться на 3-ому поверсі адміністративного будинку цегельної будівлі та за своїх характеристикам цілком відповідає вимогам СІ І і П 2.09.04 – 87 «Адміністративні і побутові будинки виробничих підприємств», а також СП 512 – 78 «Інструкція з проектування будинків і приміщень ЕОМ».

Основними шкідливими факторами, зв'язаними з роботою на ПК є:

– напруга зорових органів та пов’язане з цим стомлення, захворювання і побічні ефекти;

– значне навантаження на пальці та кисті рук, що при відсутності профілактики та медичного контролю можуть викликати професійні захворювання;

– тривале перебування в одній і тій самій позі, що викликає застійні явища в організмі, та може сприяти різним захворюванням;

– випромінювання різного виду при використанні відеомоніторів на електронно-променевих грубках (м'яке рентгенівське випромінювання, ультрафіолетове випромінювання, видиме випромінювання, інфрачервоне

випромінювання, низько і високочастотне електромагнітне випромінювання, електростатичні полючи);

– механічні шуми, що пов'язані з роботою електронно-механічного друкуючою пристрою (принтера), вентиляторів системи охолодження, приводів читання CD-дисків та вібрація; іонізація повітря;

– наявність шкідливих хімічних речовин.

Дослідження науково-дослідного інституту гігієни праці і профзахворювань вказали на зміни у функціональному стані зорового аналізатора в ході виробничої діяльності фахівців, що працюють з відеотерміналами, наприкінці 4 години роботи.

Професійні захворювання при роботі з персональним комп’ютером:

– комп'ютерний зоровий синдром. Вплив роботи з монітором зазвичай залежить від віку користувача, від стану зору, а також від інтенсивності роботи з дисплеєм та організації робочого місця. В результаті тривалої роботи дуже великий ризик появи, або прогресивності вже наявною, короткозорості.

– проблеми, що пов'язані з м'язами і суглобами. Нерухома напружена поза оператора, протягом тривалого часу прикутого до екрану монітора, призводить до втоми і виникнення болю в хребті, шиї, плечових суглобах, а також розвивається м'язова слабкість і відбувається зміна форми хребта. Інтенсивна робота з клавіатурою викликає больові відчуття в ліктьових суглобах, передпліччях, зап'ястях, в кистях і пальцях рук. Зазвичай присутні скарги на оніміння шиї, біль у плечах і попереку або поколювання в ногах. Але бувають, проте, і більш серйозні захворювання. Найбільш поширений кистьовий тунельний синдром, при якому нерви руки пошкоджуються внаслідок частої і тривалої роботи на комп'ютері. У найбільш важкій формі цей синдром проявляється у вигляді болісних відчуттів, що позбавляють людину працездатності.

– синдром комп'ютерного стресу. Постійні користувачі ПК зазвичай піддаються психологічним стресам, функціональних порушень центральної

нервової системи, хвороб серцево-судинної системи.

– вплив на імунну систему. При впливі електро-магнітного випромінювання (ЕМВ) порушуються процеси імуногенезу, опромінених ЕМВ, змінюється характер інфекційного процесу – протягом інфекційного процесу обтяжується. ЕМВ можуть сприяти неспецифічному пригнічення імуногенезу, посилення утворення антитіл до тканин плоду і стимуляції аутоімунної реакції в організмі вагітної самки.

– вплив на ендокринну систему і нейрогуморальну реакцію. При дії ЕМВ, як правило, відбувається стимуляція гіпофізарно-адреналінової системи, що супроводжується збільшенням вмісту адреналолина в крові, активацією процесів згортання крові.

– вплив на статеву функцію. Порушення статевої функції зазвичай пов'язані зі зміною її регуляції з боку нервової та нейроендокринної систем.

Симптоми захворювання різноманітні і численні. Зазвичай, на-відмінність єдиного симптому малоймовірно, оскільки всі функціональні органи людини взаємопов'язані.

1. Фізичні нездужання: сонливість, непроходяча втома; головний біль після роботи; болі в нижній частині спини, в ногах, відчуття поколювання, оніміння, болі в руках; напруженість м'язів верхньої частини тулуба.

2. Захворювання очей: відчуття гострого болю, печіння, свербіння.

3. Порушення візуального сприйняття: неясність зору, яка збільшується протягом дня; виникнення подвійного зору.

4. Погіршення зосередженості і працездатності: зосередженість досягається за працею; дратівливість під час і після роботи; повітря робочої точки на екрані; помилки при друкуванні.

А.2 Заходи щодо поліпшення умов праці

До приміщення науково-дослідного відділу й організації робочого

місця з обліком шкідливих виробничих факторів пред'являється ряд вимог. Приміщення в якому знаходиться робоче місце з ПК повинно мати природне освітлення, бажано з однобічним розміщенням світопрорізів, площа осклянілості яких не повинна перевищувати 25 % від площі стіни світопрорізами. Віконні прорізи в приміщенні з ПК повинні мати регульовані жалюзі чи занавеси або інші сонцезахисні пристрої. Не допускається розташування робочих місць із ПК у підвальних і цокольних поверхах. Робочі місця з ПК рекомендується розміщати в окремих приміщеннях. Площа на одного працюючого з ПК повинна складати 6 м^2, об’єм – 20 м^3. Неприпустиме розташування ПК, при якому працюючий звернений обличчям, або спиною до вікон чи кімнати задньої частини ПК, у яку монтуються вентилятори.

Забороняється застосовувати для обробки інтер'єра приміщень із ПК полімерні матеріали (дерев’ястружечні плити, шпалери що миються, плівкові та рулоні синтетичні матеріали, шаруватий паперовий пластик та ін.), що виділяються в повітря шкідливі хімічні речовини, що перевищують гранично допустимі концентрації, не включені в «Перелік дозволених , МЗ» 1977-1985 р.

В лабораторії вимірювальної техніки та науково-дослідної роботи робочі місця з ПК розташовані від стіни з вікнами на відстані 1 м, відстань між столами складає 3 м. Екрани відеомоніторів ПК знаходяться від очей користувача на відстані 700 мм відповідно до СН 512-78, приміщення (S=21 м^2, V=73,5 м^3) дозволяє розташовувати більше 3 робочих місця.

Робочі місця в положенні сидячі відповідають вимогам ДСТ 12.2.032 – 78 та ДСТ 12.2.029 – 77. Поверхня робочого столу знаходиться на висоті 0,75 метрів від підлоги, розміри робочої поверхні стільниці складають 1050х590 міліметрів, розміри вільного простору для ніг під столом складає висота 650, глибина 550, ширина 450 міліметрів відповідно. Робочий стілець оснащений підйомно-поворотнім пристроєм, що забезпечує регуляцію висоти сидіння і спинки, пневматичним і гідравлічними амортизаторами та обладнанні

підлокітниками.

Мікроклімат робочого місця. У приміщенні науково-дослідного відділу є джерела тепловиділення, тому необхідно визначити необхідні умови його вентилювання. Витрату повітря в приміщенні з додатковим тепловиділенням визначаємо за формулою:

$$L = \frac{Q_{НАД}}{c \cdot p \cdot (t_B - t_H)}, \quad \text{(А.1)}$$

де $Q_{НАД}$ – надлишкове виділення тепла в робочому приміщенні, ккал/год.; c – теплоємкість повітря (0,249 ккал/кг); p – обсягова вага повітря (1,346 кг/м^3); t_B – температура витяжного повітря (30°С); t_H – температура приточного повітря (20°С).

Розрахуємо надлишкове надходження тепла за наступною формулою:

$$Q_{НАД} = Q_{УСТ} + Q_{ПЕР} + Q_{ОСВ} + Q_{СР}, \quad \text{(А.2)}$$

де $Q_{УСТ}$ – виділення тепла від устаткування; $Q_{ПЕР}$ – виділення тепла робітниками; $Q_{ОСВ}$ – надходження тепла від електричного освітлення; $Q_{СР}$ – надходження тепла від сонячної радіації через вікна.

Визначимо виділення тепла від устаткування за формулою:

$$Q_{УСТ} = P \cdot K_a \cdot K_б \cdot 860, \quad \text{(А.3)}$$

P – сумарна потужність устаткування, кВт/год; K_a – коефіцієнт установленої потужності (0,95); $K_б$ – коефіцієнт одночасної роботи (1,0).

$$Q_{УСТ} = [x_1 \cdot k_1 + x_2 \cdot k_2 + x_3 \cdot k_3 + x_4 \cdot k_4 + x_5 \cdot k_5 + x_6 \cdot k_6 + x_7 \cdot k_7 +$$

$$+x_8 \cdot k_8 + x_9 \cdot k_9] \cdot K_a \cdot K_б \cdot 860 =$$
$$= [2 \cdot 0{,}5 + 1 \cdot 0{,}1 + 1 \cdot 0{,}07 + 0{,}4 + 1 \cdot 0{,}06 + 1 \cdot 0{,}05 + 1 \cdot 0{,}6 + 4 \cdot 0{,}15 +$$
$$+1 \cdot 4] \cdot 0{,}95 \cdot 1 \cdot 860 = 5620 \text{ ккал/год.}$$

Визначимо виділення тепла від обслуговуючого персоналу за допомогою наступної формули:

$$Q_{ПЕР} = n \cdot g = 2 \cdot 100 = 200 \text{ ккал/год,} \qquad (А.4)$$

де n – кількість працюючих; g – кількість тепла, що виділяє один працівник за годину (100 ккал/год.).

Визначимо надходження тепла від електричного освітлення за формулою:

$$Q_{ОСВ} = E_M \cdot g_1 \cdot S = 300 \cdot 0{,}05 \cdot 21 = 315 \text{ ккал/год,} \qquad (А.5)$$

де E_M – нормована освітленість для цієї зорової роботи, величина якої дорівнює 300 лк; g_1 – питоме тепловиділення на 1 м^2 підлоги при 1 лк освітленості (для / люмінесцентних ламп – 0,05 ккал/год.) S – площа приміщення, м^2.

Визначимо надходження тепла від сонячної радіації через вікна за наступною формулою:

$$Q_{СР} = F \cdot g_2 \cdot K_{ОСЛ} = 7{,}5 \cdot 65 \cdot 0{,}4 = 195 \text{ ккал/год,} \qquad (А.6)$$

де F – площа віконних прорізів (3х2,5=7,5 м^2); g_2 – кількість тепла, що надходить через 1 м^2 віконного прорізу (65 ккал/год.); $K_{ОСЛ}$ – коефіцієнт ослаблення, приймаємо 0,4.

Визначимо кількість надлишкового тепла:

$$Q_{НАД} = Q_{УСТ} + Q_{ПЕР} + Q_{ОСВ} + Q_{СР} = 5620 + 200 + 315 + 195$$
$$= 6330 \text{ ккал/год.}$$

Визначимо витрати повітря в приміщенні:

$$L = \frac{Q_{НАД}}{c \cdot p \cdot (t_B - t_H)} = \frac{6330}{0{,}237 \cdot 1{,}226 \cdot (30 - 20)} = 2178 \text{ } м^3/\text{ год.}$$

Існуюча в наявності система кондиціонування і вентилювання має продуктивність 2200 куб. м./годину, що задовольняє необхідним нормативам.

Параметри мікроклімату на робочих місцях регламентуються ДНАОІІ 0.03.3.15 – 86 «Санітарні норми мікроклімату виробничих приміщень № 4088–86». Відповідно доданих санітарних норм температура повітря, швидкість руху повітря та відносна вологість у холодні періоди року повинна складати

(22 – 24) градуса за Цельсієм, 0,1 метра в секунду та 40-60 % відповідно. При збереженні всім параметрів можливе коливання температури від 21 до 25 градусів Цельсія. У теплі періоди року температура повітря повинна складати (23 – 25) градусів Цельсія, рухливість повітря (0,1 – 0,2) метрів секунду, вологість (40 – 60) %. Температура може коливатися від 22 до 26 градусів Цельсія при збереженні всіх інших параметрів мікроклімату. Вище зазначені норми цілком відповідають фактичним даним приміщення лабораторії вимірювальної техніки та науково-дослідним відділом.

Розрахунок системи загального рівномірного освітлення з лампами розжарювання для приміщення, в якому використовуються зорові роботи високої точності. Розміри приміщення: довжина (a=6 м), ширина (b=3,5 м), висота (h=3,5 м). Приміщення має світлу побілку: коефіцієнт відбиття $P_{стелі}$ = 70 %, $P_{стін}$ = 50 %. Висота робочих поверхонь (столів) h_p = 0,7 м. Для освітленняприйнято світильники типуУПМ-15, які підвищуються до стелі,

відстаньвід світильника до стелі h_c=0,4 м.. Мінімальна освітленість за нормами E=200 лк.

1) Визначимо висоту підвісу світильників над підлогою

$$h_0 = H - h_c = 3{,}5 - 0{,}4 = 3{,}1 \text{ м.}$$

Для світильників загального освітлення з лампами розжарювання потужністю до 200 Вт мінімальна висота підвісу над підлогою відповідно до СНІП П-4-79 повинна бути у межах (2,5 –4,0) м, залежно від характеристики світильника. В лабораторії вимірювальної техніки та науково-дослідному відділу відповідає цій вимозі.

2) Визначимо висоту підвісу світильника над робочою поверхнею:

$$h = h_0 - h_p = 4{,}5 - 0{,}4 = 4{,}1 \text{ м.}$$

Рівномірність освітлення досягається при відповідному співвідношенні відстані між світильниками (L) та висоти їх підвісу (h).

3) Визначимо рекомендовану відстань між світильниками

$$L = 0{,}7 \cdot h = 0{,}7 \cdot 2{,}8 = 2{,}0 \text{ м.}$$

4) Розрахуємо необхідну кількість світильників

$$N = \frac{a \cdot b}{L^2} = \frac{10 \cdot 4{,}5}{2^2} = 11.25.$$

Приймаємо 6 світильників, враховуючи розміри приміщення розміщуємо їх у два ряди по 3 штуки.

5) Світловий потік лампи світильника $(\Phi_Л)$ визначається за формулою:

$$\Phi_{Л} = \frac{E \cdot K_{З} \cdot S \cdot Z}{N \cdot n \cdot \eta},$$

де E – нормативна освітленість, лк; $K_{З}$ – коефіцієнт запасу, який враховує зниження освітленості в результаті забруднення та старіння ламп; S – площа приміщення, що освітлюється, м^2; Z – коефіцієнт нерівномірності освітлення для ламп розширювання (1,15); N – кількість світильників; n – кількість ламп у світильнику; η – коефіцієнт використання світового потоку, який визначається за світлотехнічними таблицями залежно від показника приміщення (i) та коефіцієнтів відбиття стін та стелі.

6) Визначимо показник приміщення:

$$i = \frac{a \cdot b}{h \cdot (a + b)} = \frac{10 \cdot 4{,}5}{4{,}5 \cdot (10 + 4{,}5)} = 4{,}71.$$

Коефіцієнт використання η = 0,48 для світильника УПМ-15 (при і= 2,5, $Р_{стелі}$=70%, $Р_{стін}$ = 50 %)

Світловий потік одного світильника, а значить і лампи, оскільки за конструктивним виконанням у світильнику цього типу встановлена лише одна лампа, дорівнює:

$$\Phi_{Л} = \frac{E \cdot S \cdot Z}{N \cdot n \cdot \eta} = \frac{200 \cdot 21 \cdot 1{,}15}{6 \cdot 1 \cdot 0{,}48} = 1677 \text{ лм.}$$

9) обираємо лампу Б-150 потужністю 150 Вт, світловий потік якої становить 2100 лм. Хоча це значення на 18% більше розрахованого, однак не перевищує встановлену норму (– 0 %<$\Phi_{Л}$<+20 %). Сумарна електрична потужність усіх світильників, встановлених у приміщенні становить:

$$P_{СВ} = P \cdot N = 150 \cdot 6 = 900 \text{ Вт.}$$

А.3 Пожежна безпека

Найважливішою умовою роботи будь-якого підприємства є дотримання правил пожежної охорони. У приміщені лабораторії вимірювальної техніки та науково-дослідному відділу основні міри для забезпечення пожежної безпеки визначає «Інструкція про заходи пожежної безпеки для службових приміщень (офісів)». Вона є обов'язковою для використання всіма співробітниками відділу. У згідності з цією інструкцією, у кожному приміщенні повинний бути призначений відповідальний за пожежну безпеку, вивішена на видному місці табличка з указівкою його посади та прізвища.

Меблі й устаткування повинні розміщатися таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (шириною не менше 1 м). Евакуаційні шляхи та виходи необхідно постійно держати вільними, нічим не захаращувати. По мірі нагромадження та закінчення роботи пальні відходи варто збирати в спеціально відведених сміттєзбиральників.

Електромережі, електроприлади й апаратура повинна експлуатуватися тільки в справному стані, з урахуванням рекомендацій підприємства-виготовлювачів. У випадку виявлення ушкоджень електромереж, вимикачів, розеток та інших електровиробів варто негайно відключи їх та вжити необхідних заходів до приведення в пожежобезпечний стан. Документи папір та інші горючі матеріали варто зберігати на відстані не менш 1 м від електрощитів, електрозбірок та електрокабелів, 0,5 м від світильників та 0,25 м від приладів опалення.

Засоби протипожежного захисту (пожежні крани, пожежна й охоронно-пожежна сигналізація, первинні засоби пожежогасіння і т.п.), що маються в приміщеннях, варто тримати в справному стані.

Усі працівники повинні пройти протипожежний інструктаж, уміти

користатися наявними вогнегасниками, іншими первинними засобами пожежогасіння та знати місце їхнього перебування. Відстань від найбільш віддаленого місця приміщення до місця розміщення вогнегасника не повинне перевищувати 20 м.

А.4 Безпека при надзвичайних ситуаціях на підприємстві

Об’єктом розгляду на предмет визначення надзвичайних небезпек та їх наслідків є науково-дослідний відділ. Однією із вірогідних загроз може бути раптове виникнення пожару внаслідок короткого замикання в електромережах або розрядів статистичної електрики, що може привести до пошкодження і руйнування будівлі, устаткування, комунікацій, виділення токсичних продуктів горіння.

Тому в науково-дослідному відділі розроблено оперативний план гасіння пожежі, який визначає порядок дії персоналу при пожежі, порядок її гасіння в електроустановках, взаємодію з власним складом пожежних підрозділів, а
також застосування схем и засобів пожежогасіння з урахуванням заходів безпеки.

Будівля повинна бути обладнана мережею протипожежного водозабезпечення, установками виявлення та гасіння пожеж відповідно вимогам нормативно-технічних документів. Кожний працівник повинен чітко знати та виконувати вимоги ППБ та протиаварійний режим на об’єкті, уміти користуватися наявними вогнегасниками, іншими первинними засобами пожежогасіння і знати місце їхнього перебування.

Меблі й устаткування повинні розміщатися таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (шириною не менше 1 м). Евакуаційні шляхи і виходи необхідно постійно держати вільними, нічим не захаращувати. Засоби протипожежного захисту в приміщеннях потрібні триматися у справному стані.

У випадку виявлення пожежі слід: негайно повідомити державну пожежну охорону за телефоном «101», вказати при цьому адресу, кількість поверхів, місце виникнення пожежі, наявність людей, своє прізвище; повідомити про пожежу керівництву, а в нічний час черговому охоронцю; у разі можливості почати гасіння пожежі наявними засобами, організувати зустріч пожежних підрозділів.

При виникненні пожежі у початковій стадії його розвитку випромінюється тепло, накопичуються токсичні продукти згоряння, імовірні руйнування будівельних споруд. Тому слід як можна швидше провести евакуацію людей із палаючої будівлі. Показником ефективності евакуації є час, протягом якого працівники можуть при потрібності залишити окремі приміщення і будівлю в цілому. Безпека евакуації досягається тоді, коли час евакуації не перевищує час настання критичної фази розвитку пожежі, тобто часу від початку пожежі до досягнення граничних для людини впливів факторі пожежі (критичних температур, ступені задимлення, зниження концентрації кисню и т.п.). Число евакуаційних виходів повинно бути не менш двох. Вони повинні розташовуватися розосереджено. Мінімальна відстань між найбільш віддаленими один від одного евакуаційними виходами із приміщення визначається за формулою:

$$l = 1{,}5 \cdot \sqrt{P} = 1{,}5 \cdot \sqrt{19} = 6{,}5 \text{ м}, \qquad \text{(А.7)}$$

де P – периметр приміщення, м.

Двері на шляхах евакуації повинні відкриватися у напрямку виходу із будівлі. У кожному приміщенні на видному місці повинен бути вивішений план евакуації при пожежі.

При пожежі обов'язково необхідно враховувати небезпечні чинники і механізм їх дії на людину. При виникненні пожежі, після виклику пожежної охорони, необхідно попередити про це усіх, хто знаходиться поруч, після чого евакуюватися самому і по можливості допомогти евакуюватися іншим,

особливо особам літнього віку і дітям, попереджаючи при цьому виникнення паніки. З метою обмеження циркуляції повітря, яке здатне збільшувати швидкість горіння, покидаючи приміщення, закрийте за собою усі двері, якщо це можливо. Якщо пожежа виникла в приміщенні над вами і безпосередньої загрози для вас не спостерігається, то бажано виконати заходи по зниженню можливих втрат від води яку проливають при гасінні пожежі. Для цього необхідно відключити всі електроприводи та прикрити їх поліетиленовою плівкою. Значно гірше, якщо пожежа виникла в приміщенні під вами – потрібно оцінити обстановку и якщо є впевненість, що ще не має сильної задимленості з високою температурою, потрібно негайно покинути приміщення, рухаючись до виходу по коридорам і сходовим кліткам. Користуватися ліфтом категорично забороняється, за винятком ліфтів, які спеціально призначені для транспортування пожежної охорони. Шахта ліфта є шляхом для поширення диму і отруйних продуктів горіння, до того ж при пожежі ліфт часто відключають і можна опинитися в пастці при пожежі.

Якщо ви знаходитеся в приміщенні де немає пожежі, але відрізани вогнем, димом, високою температурою від головних шляхів евакуації, то в першу чергу необхідно заважити доступу диму и продуктів горіння в це приміщення. Для чого необхідно негайно закрити усі щілини у дверях та під ними змоченими водою ганчірками, рушниками, робочими халатами та ін. Якщо приміщення все ж заповнено димом, необхідно підповзти до вікна, закрити при цьому рот та ніс змоченою тканиною, яка грає роль фільтру та в певної мірі захищає від продуктів горіння.

ДОДАТОК Б

Типовий офіс аутсорсингової компанії

Рисунок Б.1 - План офісного центру

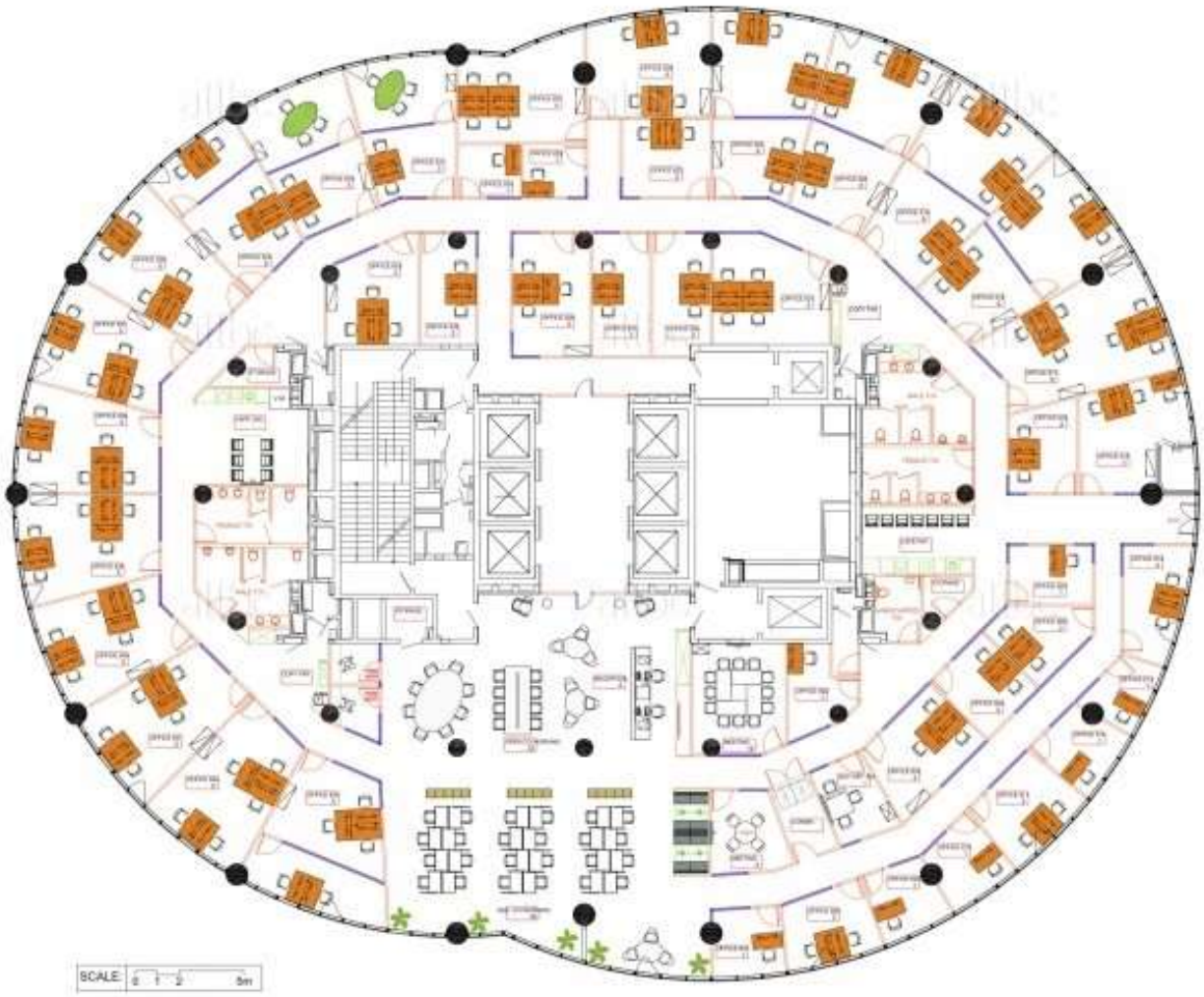


Рисунок Б.2 - План поверху 1 типу

ДОДАТОК В
Струкртурна схема мережі

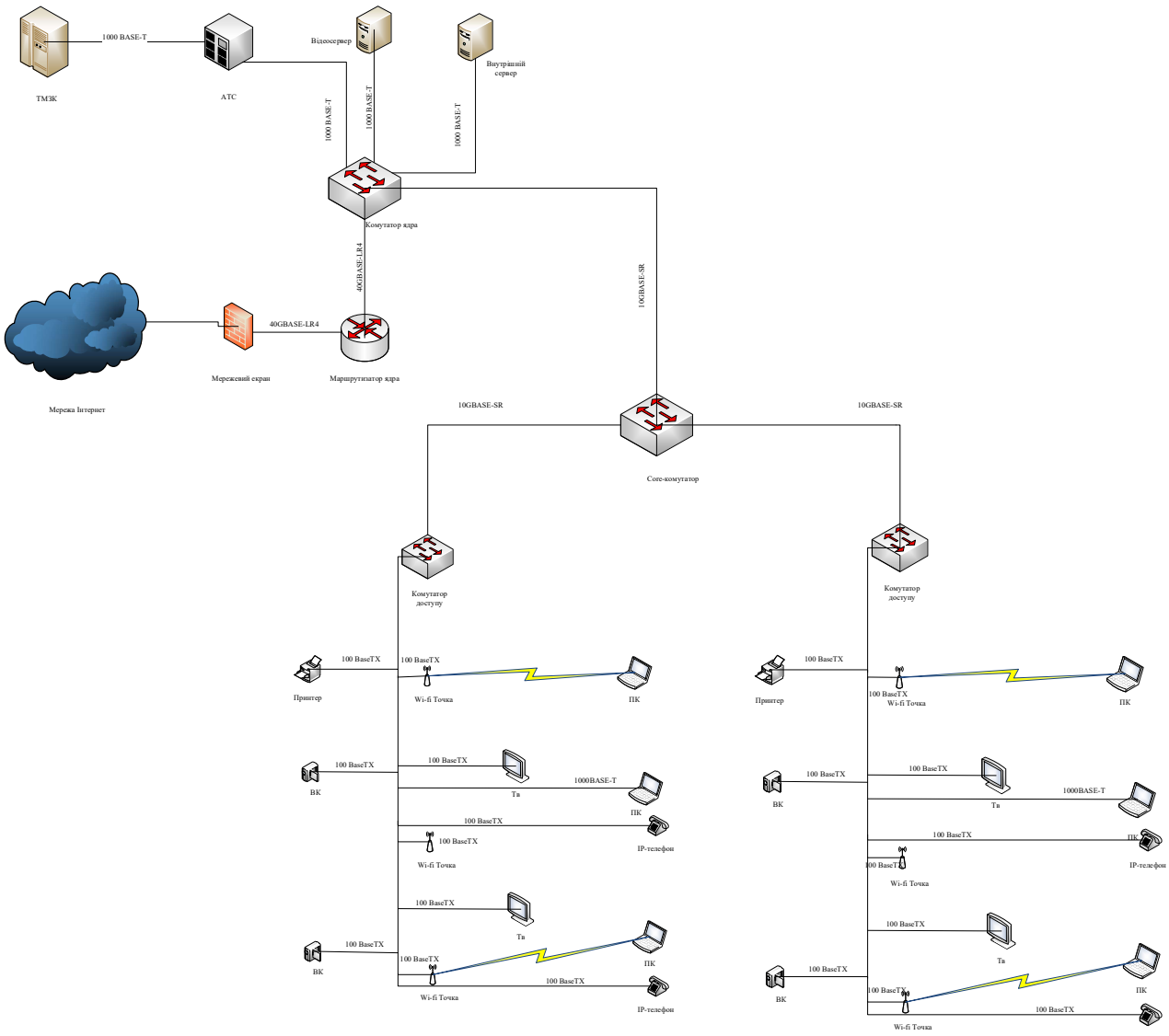


Рисунок В.1 - Структурна схема мережі