

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Навчально-науковий інститут телекомунікаційних систем

Кафедра телекомунікацій

«На правах рукопису»

УДК _____

«До захисту допущено»

Завідувач кафедри

_____ Сергій КРАВЧУК

«___» _____ 2024 р.

Магістерська дисертація

на здобуття ступеня магістра

**за освітньо-професійною програмою «Інженерія та програмування
інфокомунікацій»**

зі спеціальності 172 «Телекомунікації та радіотехніка»

**на тему: «Використання хмарних середовищ для забезпечення надійності
даних мобільних операторів»**

Виконала:

студентка ІІ курсу, групи ТЗ-з21мп

Світельська Марія Вікторівна _____

Керівник:

Доцент кафедри ТК НН ІТС, к.т.н., с.н.с.

Міночкін Д.А. _____

Рецензент:

Доцент кафедри ІТТ НН ІТС, к.т.н., доцент

Новогрудська Р.Л. _____

Засвідчую, що у цій магістерській
дисертації немає запозичень з праць
інших авторів без відповідних
посилань.

Студентка _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Сергій КРАВЧУК

«___» _____ 2023 р.

ЗАВДАННЯ
на магістерську дисертацію студентці
Світельській Марії Вікторівні

1. Тема дисертації «Використання хмарних середовищ для забезпечення надійності даних мобільних операторів», науковий керівник дисертації доцент кафедри ТК НН ІТС, к.т.н., Міночкін Дмитро Анатолієвич, затверджені наказом по університету від «31» жовтня 2023 р. № 5067-с.
2. Термін подання студентом дисертації 05.01.2024 р.
3. Об'єкт дослідження: «Процеси збереження, обробки та забезпечення надійності даних в системах мобільних операторів».
4. Предмет дослідження: «Використання хмарних середовищ для оптимізації процесів збереження та забезпечення надійності даних мобільних операторів».
5. Перелік завдань, які потрібно розробити:
 - Вивчити досвід побудови інфраструктури мобільних операторів.
 - Розібратися в основних характеристиках інфраструктури хмарних середовищ.
 - Розглянути та порівняти різні архітектурні підходи до використання хмар для забезпечення надійності.
 - Розробити математичну модель використання хмарних середовищ у мобільних операторів.
 - Оцінити ефективність використання хмарних середовищ для

- забезпечення надійності даних мобільних операторів.
- Розробити ринкову стратегію розгортання стартап-проекту.

6. Орієнтовний перелік ілюстративного матеріалу:

- Хронологію розвитку стандартів мобільних мереж.
- Архітектура GSM-мережі.
- Архітектура GSM-мережі із додаванням технологій покращення передачі даних GPRS.
- Архітектура 3G-мережі.
- Архітектура 4G-мережі.
- Архітектура 5G-мережі.
- Приклад використовуваного фізичного обладнання для побудови датацентру для побудови хмарного рішення аварійного відновлення.
- Приклад використання технології Oracle Data Guard для забезпечення реплікації між основним та DR сайтом.
- Приклад операційної інфраструктури мобільного оператора, де переключення трафіку здійснюється шляхом зміни DNS-записів основних сервісів.
- Приклад коду terraform, який дозволяє перемикати DNS-A записи для зміни відповідності IP-адреси і доменних імен.

7. Орієнтовний перелік публікацій

8. Дата видачі завдання “ 15 ” вересня 2022 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Узгодження теми	15.09.2022	виконано
2	Написання першого розділу магістерської дисертації	15.12.2022	виконано
3	Написання другого розділу магістерської дисертації	23.03.2023	виконано
4	Написання третього розділу магістерської дисертації	25.05.2023	виконано
5	Написання четвертого розділу магістерської дисертації	11.11.2023	виконано

Студент

Марія, СВІТЕЛЬСЬКА

Науковий керівник дисертації

Дмитро, МІНОЧКІН

РЕФЕРАТ

Робота містить 93 сторінок, 9 рисунків, 15 таблиць та використовує посилання на 50 джерел. Актуальність дослідження полягає в зростаючій важливості мобільного зв'язку у сучасному суспільстві та необхідності забезпечення надійності даних в цій галузі.

Мета роботи полягає в розробці та впровадженні стратегій для підвищення надійності зберігання та доступу до даних мобільних операторів в хмарних середовищах. Для досягнення цієї мети були виконані наступні завдання: аналіз існуючих рішень, розробка стратегій забезпечення надійності, експериментальне впровадження, аналіз результатів та формування рекомендацій.

Наукова новизна дослідження полягає у комплексному підході до забезпечення надійності даних мобільних операторів в хмарних середовищах.

Практичне значення результатів включає підвищення надійності та безпеки даних мобільних операторів та зменшення витрат на обслуговування.

Ключові слова: мобільний зв'язок, хмарні середовища, надійність даних, стратегії, безпека, ефективність, дослідження.

ABSTRACT

The paper consists of 93 pages, 9 figures, 15 tables, and references to 50 sources. The relevance of the research lies in the increasing importance of mobile communication in modern society and the need to ensure data reliability in this field.

The aim of the study is to develop and implement strategies to enhance the reliability of data storage and access for mobile operators in cloud environments. To achieve this goal, the following tasks were performed: analysis of existing solutions, development of reliability assurance strategies, experimental implementation, analysis of results, and formulation of recommendations.

The scientific novelty of the research lies in a comprehensive approach to ensuring data reliability for mobile operators in cloud environments.

The practical significance of the results includes improving the reliability and security of data for mobile operators and reducing maintenance costs.

Keywords: mobile communication, cloud environments, data reliability, strategies, security, efficiency, research.

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1.....	12
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТА РОЗВИТОК СТАНДАРТІВ МОБІЛЬНОГО ЗВ'ЯЗКУ.....	12
1.2. Архітектура та особливості роботи мереж типу 2G.....	15
1.3. Архітектура та особливості роботи мереж типу 3G.....	22
1.4. Архітектура та особливості роботи мереж типу 4G.....	25
1.5. Архітектура та особливості роботи мереж типу 5G.....	27
Висновки.....	31
РОЗДІЛ 2.....	33
ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ НАДІЙНОСТІ ІНФРАСТРУКТУРИ.....	33
2.1 Загальна характеристика доступних хмарних сервісів.....	33
2.2. Хмарні служби для забезпечення надійності.....	36
2.3. Географічна розподіленість.....	37
2.4. Автоматичне масштабування.....	38
2.5. Системи моніторингу та управління.....	40
2.6. Автоматизована система управління.....	42
2.7. Кібербезпека хмарних середовищ.....	44
Висновки.....	46
РОЗДІЛ 3.....	49
ПІДВИЩЕННЯ НАДІЙНОСТІ ІНФРАСТРУКТУРИ ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ ШЛЯХОМ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ АВАРІЙНОГО ВІДНОВЛЕННЯ.....	49
3.1. Характеристика поняття аварійного відновлення (disaster recovery).....	49
3.2. Створення стартапу для надання аварійного відновлення як сервіс (DRaaS)	

операторам мобільного зв'язку.....	55
3.3. Забезпечення переключення кінцевих користувачів між основною та DR платформами.....	63
Висновки.....	66
РОЗДІЛ 4.....	70
РОЗРОБКА СТАРТАП ПРОЕКТУ.....	70
4.1. Опис ідеї проекту.....	70
4.2. Технологічний аудит ідеї проекту.....	71
4.3. Аналіз ринкових можливостей запуску стартап-проекту.....	72
Продовження таблиці 4.10.....	80
4.4. Розроблення ринкової стратегії проекту.....	80
4.5. Розроблення маркетингової програми стартап-проекту.....	82
ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ.....	83
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	87

ПЕРЕЛІК СКОРОЧЕНЬ

MSC	Mobile Switching Centre
BSS	Base Station Subsystem
BSC	Base Station Controller
BTS	Base Transceiver Station
MS	Mobile Station
GPRS	General Packet Radio Service
SGSN	Serving GPRS Support Node
GGSN	Gateway GPRS Support Node
EPC	Evolved Packet Core
MME	Mobility Management Entity
S-GW	Serving Gateway
P-GW	PDN Gateway
PDN	Packet Data Network
BaaS	Backup as a service
DRaaS	Disaster recovery as a service
RTO	Recovery time objective
RPO	Recovery point objective

ВСТУП

В сучасному світі, де висока доступність та надійність інформації стають ключовими факторами успіху для різноманітних галузей, мобільні оператори встають перед викликом забезпечення стабільної та безперебійної роботи своїх мереж та зберігання величезного обсягу даних.

Актуальність обраної теми необхідно розглядати у контексті сучасних викликів та тенденцій розвитку технологій. Сучасне суспільство виявляє зростаючу залежність від мобільного зв'язку, який став не лише комунікаційним інструментом, але й невід'ємною частиною подання та отримання послуг, проведення фінансових операцій, навчання та багатьох інших аспектів повсякденного життя. З цим ростом значущості мобільного зв'язку зростає і вимога до його надійності та стабільності. [1,2]

Водночас, масштабні обсяги даних, що генеруються та обробляються мобільними операторами, викликають необхідність удосконалення технічних та організаційних аспектів управління цією інформацією. Збереження, захист та доступ до цих даних стають критично важливими завданнями, оскільки будь-який збій у цьому процесі може призвести до серйозних порушень в обслуговуванні абонентів та великих економічних втрат [1].

Одним із ключових інструментів для вирішення цих проблем є використання хмарних середовищ, що визначається їхньою гнучкістю, масштабованістю та здатністю забезпечити високу надійність систем збереження та обробки даних. Особливо важливим стає це в контексті мобільних операторів, де величезний потік даних обробляється в реальному часі, а доступність послуг є ключовим фактором для задоволення потреб сучасного суспільства [3,4].

Таким чином, враховуючи зростаючу важливість мобільного зв'язку та величезні обсяги даних, що обробляються, дослідження використання хмарних середовищ для забезпечення надійності даних мобільних операторів є актуальним завданням, яке напряду впливає на сталість та ефективність функціонування цієї ключової галузі інформаційних технологій. З урахуванням

цих вимог, використання хмарних середовищ стає актуальною стратегією для оптимізації інфраструктури та забезпечення надійності систем [4].

Метою даного дослідження є вивчення та аналіз можливостей використання хмарних середовищ для забезпечення надійності даних мобільних операторів.

Сучасні реалії висувають перед мобільними операторами особливі завдання та виклики, врахування яких стає стратегічно важливим у контексті їхньої діяльності. Зростання залежності суспільства від мобільного зв'язку визначає його критичну роль у щоденному функціонуванні та розвитку різних галузей. Відтак, забезпечення надійності інфраструктури мобільних операторів стає не тільки завданням внутрішнього планування, але й стратегічною необхідністю для суспільства загалом.

Діяльність мобільних операторів напряду пов'язана із забезпеченням надійного та стабільного мобільного зв'язку, що є важливою складовою для безперервного доступу до інформації, електронного взаємодії та послуг для мільйонів користувачів. Коли кожен аспект нашого життя, починаючи від комунікації та завершуючи операційними процедурами, обробкою фінансових транзакцій і роботою віддалених систем, втручається у цифровий простір, важливість надійного мобільного зв'язку стає надзвичайною [1].

Однак ця критичність мобільного зв'язку також робить його схильним до різних викликів і загроз, починаючи від технічних неполадок та закінчуючи кібератаками та природними катастрофами. Такі випадки можуть призвести до великих перерв у наданні послуг, що безпосередньо впливає на зручність та безпеку користувачів, а також може призвести до серйозних економічних та соціальних наслідків [3].

Враховуючи ці реалії, дослідження використання хмарних середовищ для забезпечення надійності даних мобільних операторів виявляється не тільки важливим науковим завданням, але й ключовим кроком у напрямку забезпечення стабільності та безпеки мобільного зв'язку, який став невід'ємною частиною нашого сучасного життя.

Мета даного дослідження полягає в аналізі та вивченні можливостей використання хмарних середовищ для забезпечення надійності даних мобільних операторів. З урахуванням швидкого технологічного розвитку і поширення мобільних технологій, важливо розуміти, як нові підходи можуть покращити якість обслуговування та знизити ризики втрати даних.

Дослідження включає в себе аналіз хмарних технологій у різних галузях та аспекти надійності даних. Після цього буде проведено аналіз технологій хмарних середовищ та їх потенційний вплив на надійність інфраструктури мобільних мереж. Необхідно також детально розглянути інтеграцію хмарних середовищ в інфраструктуру мобільних операторів, визначити переваги та обмеження цього процесу та визначити ключові аспекти успішного впровадження [4].

Загальна мета дипломної роботи полягає в розробці практичних рекомендацій щодо ефективного використання хмарних середовищ для забезпечення надійності даних мобільних операторів. Це дослідження може слугувати основою для подальших покращень в області зберігання та обробки інформації, що, в свою чергу, сприятиме підвищенню конкурентоспроможності мобільних операторів та задоволенню потреб споживачів.

Об'єктом даного дослідження є процеси збереження, обробки та забезпечення надійності даних в системах мобільних операторів. **Предметом** – використання хмарних середовищ для оптимізації процесів збереження та забезпечення надійності даних мобільних операторів.

У кінці дослідження буде здійснено аналіз отриманих результатів, сформульовані висновки та вказані напрямки подальших досліджень у даній області.

РОЗДІЛ 1

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТА РОЗВИТОК СТАНДАРТІВ МОБІЛЬНОГО ЗВ'ЯЗКУ

1. Зародження та розвиток мобільних мереж зв'язку. Коротка характеристика основних особливостей стандартів мобільного зв'язку

Мережі 1G (першої генерації) є піонерськими мобільними телефонними системами, розгорнутими у 1980-1990 роках [5]. На рис. 1.1. зображено хронологію розвитку стандартів мобільних мереж [47].

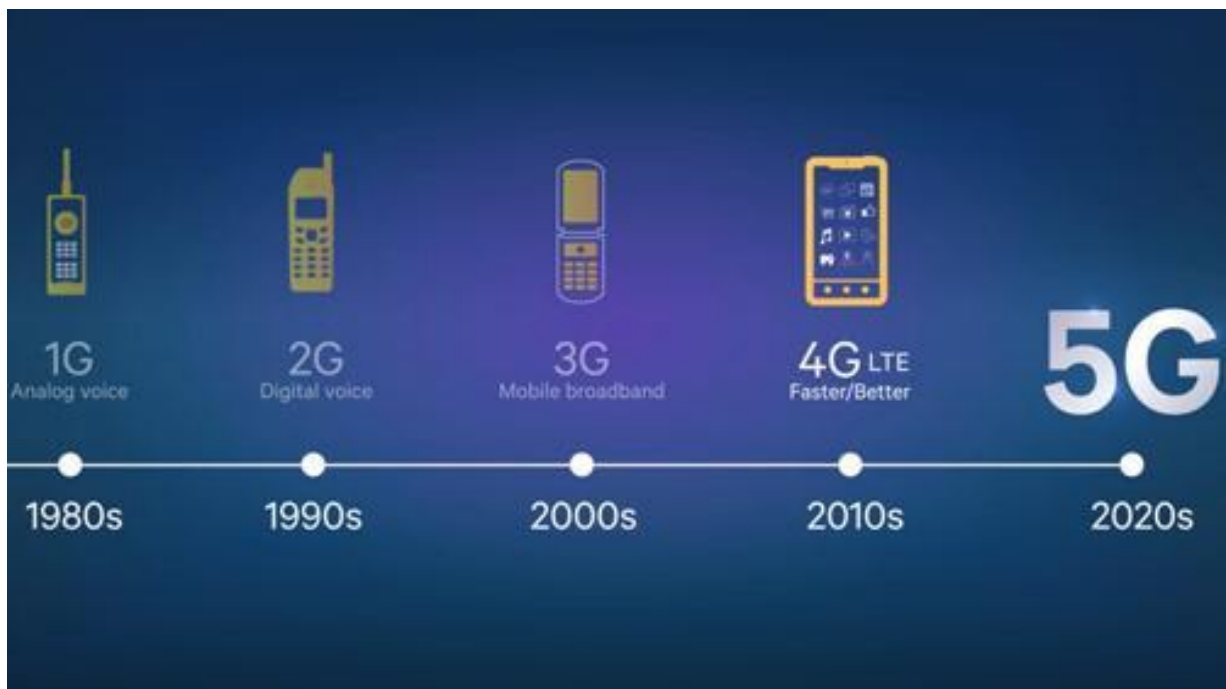


Рис. 1.1. Хронологію розвитку стандартів мобільних мереж

Мобільна мережа 1G орієнтована на передачу аналогового звукового сигналу. Вона з'явилася в далекому 1980 році та функціонувала на базі новаторського винаходу AMPS (США) та TACS, NMT (Європа) [6].

Основні характеристики 1G включають:

1. **Аналогова технологія:** мережі 1G використовували аналогові сигнали для передачі голосу і були більш схильний до шуму і спотворень; прослуховування розмови іншими абонентами.
2. **Низька ємність:** обмежена кількість абонентів, обслуговуваних однією станцією базового зв'язку.
3. **Низька якість звуку:** голосовий зв'язок був часто нестійким, і якість звуку могла коливатися, оскільки для передачі застосовувалася частотна модуляція.
4. **Проблеми із терміналами:** мобільні телефони були великими і важкими порівняно з сучасними стандартами; висока потужність рухомої станції 1G — 3-5 Вт.
5. **Обмежена покриття та роумінг:** мережі мали обмежений радіус покриття, і роумінг був обмеженим.
6. **Нестандартизовані системи:** різні країни використовували різні технології, що ускладнювало міжнародну комунікацію.

Основний недолік функціонування мережі пов'язаний із низькою ємністю через нераціональне використання виділеної смуги частот [6]. Цей недолік було визначено у середині 80-х. Розробники почали замислюватися над існуванням нової мережі. Хоча мережі 1G мали обмеження та недоліки, вони виступили важливим етапом у розвитку мобільних зв'язків та визначили основу для подальшого розвитку стандартів більш високого покоління. Наразі технологія 1G не використовується і відійшла в історію, поступившись більш сучасним.

Наразі існують кілька основних стандартів мобільного зв'язку, які використовуються у різних регіонах світу. Кожен із них має свої унікальні особливості та застосування, і вони співіснують, доповнюючи один одного в різних сегментах ринку та регіонах. На сьогоднішній день найбільш поширеними стандартами є:

1. **2G (Друга генерація):**

- **Характеристики:** Цифровий голосовий зв'язок, можливість відправки SMS, низька швидкість передачі даних (до 64 Кбіт/сек) [5].
- **Застосування:** Основно голосовий зв'язок, SMS, початкові послуги передачі даних.
- **Впроваджено:** Перші системи 2G були впроваджені у 1991 році [6].

2. 3G (Третя генерація):

- **Характеристики:** Передача даних зі швидкістю до 2 Мбіт/сек, можливість використання для широкомасштабних послуг передачі даних, підтримка відеодзвінків [5].
- **Застосування:** Інтернет-серфінг, електронна пошта, відеодзвінки.
- **Впроваджено:** Перші комерційні мережі 3G були впроваджені на початку 2000-х років.

3. 4G LTE (Четверта генерація - Long-Term Evolution):

- **Характеристики:** Швидкість передачі даних до 100 Мбіт/сек та вище, низька затримка, вдосконалена ефективність мережі [8].
- **Застосування:** Широкомасштабний Інтернет, стрімінг відео, високоякісний голосовий зв'язок.
- **Впроваджено:** Перші мережі 4G LTE були впроваджені наприкінці 2000-х років.

4. 5G (П'ята генерація):

- **Характеристики:** Висока швидкість передачі даних (до 10 Гбіт/сек), низька затримка, підтримка великої кількості пристроїв (IoT), висока надійність [7].
- **Застосування:** Високошвидкісний Інтернет, розширені можливості для віртуальної реальності, інноваційні послуги для промисловості та автономних автомобілів.
- **Впроваджено:** Перші мережі 5G почали впроваджуватися в 2019 році, і розвиток продовжується на сучасний час.

Ці стандарти існують паралельно, оскільки різні покоління задовольняють різні потреби користувачів та розвиток мобільних технологій. Поступово відбувається відмова від застарілих стандартів, і нові мережі в основному розгортаються з використанням 4G LTE та 5G технологій. У майбутньому, розвиток та розгортання технологій 5G буде продовжувати набирати оберти.

Дані мережі мережеві стандарти застосовують у різних регіонах та контекстах. Кожен з цих мобільних стандартів представляє різні покоління технологій і надає певні переваги в швидкості передачі даних, функціональності та витраті енергії. На практиці сьогодні мережі розгортають у такий спосіб:

- **2G:** Цей стандарт все ще використовується для голосового зв'язку та текстових повідомлень, але дедалі менше, оскільки новіше обладнання в основному підтримує 3G та 4G.
- **3G:** Забезпечує передачу даних, голосовий зв'язок та можливість відеодзвінків. Зазвичай використовується для обслуговування старших телефонів та в регіонах, де ще не розгорнуті більш швидкі мережі.
- **4G LTE:** Основний стандарт для широкомасштабного бездротового Інтернету, стрімінгу відео, онлайн-ігор та інших високошвидкісних послуг.
- **5G:** Знаходиться в стадії впровадження і надає найвищу швидкість передачі даних, низьку затримку та підтримку великої кількості пристроїв, що підключені до Інтернету речей (IoT).

Далі ми розглянемо більш детально особливості та характеристики згаданих вище стандартів мобільного зв'язку.

1.2. Архітектура та особливості роботи мереж типу 2G.

Мережі 2G стали першим великим кроком у розвитку мобільних технологій, надаючи базові функції голосового та текстового зв'язку, які стали масовими і використовуються дотепер. GSM (Глобальна система мобільних зв'язків) – це набір стандартів та протоколів мобільних комунікацій, які

регулюють мережі другого покоління або 2G, спочатку розроблені та впроваджені в Європі.

GSM – це цифровий стандарт для мобільних комунікацій, який є універсально визнаним. Європейський інститут стандартів телекомунікацій створив стандарт GSM для визначення процедур цифрових мобільних мереж другого покоління, які використовуються пристроями, такими як мобільні телефони [20]. Це технологічна програма для широкомасштабних комунікацій, яка використовує цифрове радіочастотне каналювання для надання аудіо-, інформаційних та мультимедійних систем зв'язку.

GSM – це мобільна мережа, а не комп'ютерна мережа в класичному розумінні – це означає, що пристрої взаємодіють із нею, шукаючи найближчі стільниці. GSM, разом із іншими технологічними досягненнями, вплинув на еволюцію послуг мобільного бездротового зв'язку. Система GSM керує комунікацією між мобільними станціями, базовими станціями та перемикаючими системами. Кожен радіоканал GSM шириною 200 кГц та додатково розділяється на фрейми з 8 часовими інтервалами. Глобальна система мобільного зв'язку (GSM) спочатку була відома як Groupe Special Mobile, що є походженням аббревіатури. Система GSM включає мобільні станції, базові станції та взаємодіючі перемикаючі системи [5, 20]. Програма GSM дозволяє 8-16 абонентів одночасно використовувати кожен радіоканал, а кожна радіостанція може мати кілька радіоканалів.

Частотні діапазони GSM загалом розділяються на два: 900/1800 МГц та 850/1900 МГц. Більшість Європи, Азії, Африки, Близького Сходу та Австралії використовують діапазон 900 МГц / 1800 МГц. Північна і Південна Америка, а також Сполучені Штати, Канада, Мексика та інші країни використовують діапазон 850 МГц / 1900 МГц. У системі глобального мобільного зв'язку частотний діапазон 900 МГц охоплює від 880 до 960 МГц, тоді як діапазон 1800 МГц охоплює від 1710 до 1880 МГц [5].

Діапазон частот 850 МГц, з іншого боку, охоплює від 824 до 894 МГц, тоді як діапазон 1900 МГц охоплює від 1850 до 1990 МГц. Мобільні системи на

основі GSM використовують серію номерів або унікальних кодів для розпізнавання абонентів мобільних телефонів та надання їм відповідної допомоги.

IMSI (Міжнародний ідентифікаційний номер абонента мобільного зв'язку) - це унікальний серійний код для кожної SIM-карти. Щоб приховати постійний ідентифікатор, мережа телефонів може створювати тимчасовий код, названий “тимчасовий ідентифікаційний номер абонента”, для кожного IMSI.

Міжнародний номер телефонного абонента мобільної станції - це повний номер телефону для певної SIM-карти, включаючи всі префікси. Нарешті, MSRN - аббревіатура від Мобільний номер роумінгу абонента, і це тимчасовий номер мобільного телефону, наданий мобільній станції, якщо вона не знаходиться в локальній мережі (роумінг). Таким чином, будь-які дзвінки чи системи зв'язку можуть бути пов'язані з ним.

Два ключові підходи, які використовує GSM, - це частотне розділення багатоканального доступу (FDMA) та багатоканальний часовий доступ (TDMA) [20]:

- **FDMA** - це техніка розбиття частотних діапазонів на багато діапазонів, кожен з яких призначений конкретним користувачам. У GSM FDMA розбиває 25 МГц ширину діапазону на 124 несучі частоти по 200 кГц. Кожній базовій станції призначається одна чи кілька несучих частот.
- **TDMA** - це практика призначення однієї і тієї ж частоти для декількох користувачів за допомогою розбиття ширин діапазонів на різні часові інтервали. Кожному абоненту призначається часовий інтервал, що дозволяє різним станціям ділити одну і ту ж область передачі.

TDMA використовується для розділення кожного розділеного несучого частоти на різні часові інтервали для GSM. Кожен TDMA-фрейм має 8 часових інтервалів і триває 4,164 мілісекунди (мс). Це означає, що кожний часовий інтервал чи фізичний канал у цій структурі повинен займати 577 мікросекунд, і інформація передається порціями протягом цього часу. У системі GSM існують

різні розміри клітин, включаючи макро-, мікро-, піко- та зонтові клітини. Кожна клітина відрізняється в залежності від діапазону виконання.

Мережа GSM має п'ять розмірів сот: макро, мікро, піко та зонт. Залежно від наданої опції з'єднання кожної клітини відрізняється. Метод багатоканального часового доступу (TDMA) працює за принципом надання кожному клієнту різного часового інтервалу на тому ж частотному діапазоні. Це легко адаптується для відправлення та отримання даних і голосового зв'язку, і воно може утримувати діапазони від 64 кбіт/с до 120 Мбіт/с.

Архітектура мережі 2G включає три основні компоненти [5]:

- Мобільна станція (MS): Це включає в себе мобільний телефон та SIM-карту.
- Підсистема базової станції (BSS): Це включає в себе базову трансиверну станцію (BTS), яка взаємодіє з мобільним телефоном, та контролер базової станції (BSC), який керує розподілом радіоканалів.
- Підсистема перемикання мережі (NSS): Це включає в себе центр перемикання мобільних дзвінків (MSC), який керує перемиканням дзвінків між різними мережами, та реєстр місця проживання (HLR), який зберігає дані користувача.

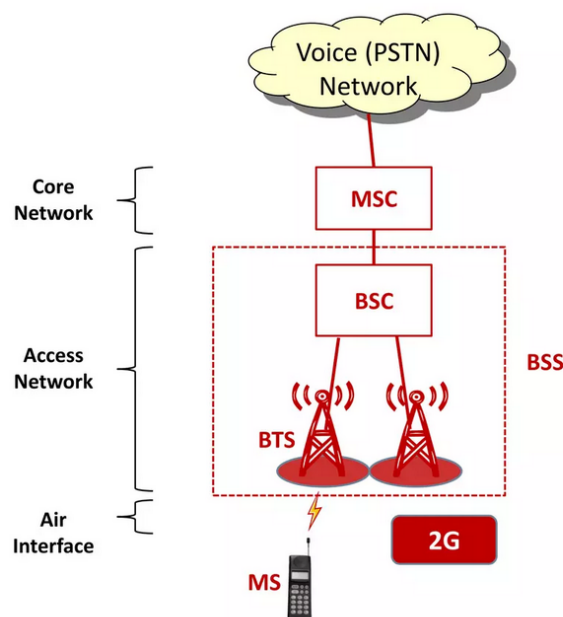


Рис. 1.2. Архітектура GSM-мережі.

У більш детальній формі можна функціонально виділити наступні елементи архітектури мережі 2G [20, 21]:

- **Базові станції (BTS):** Основні елементи, які взаємодіють із мобільними телефонами в конкретних стільниках.
- **Базовий контролер (BSC):** Керує групою BTS та здійснює управління ресурсами, які включають в себе частоти та часові інтервали.
- **Центральний вузол керування (MSC):** Відповідає за керування викликами та комутацію великої кількості базових станцій.
- **Вузол підключення до головної мережі (GMSC):** Забезпечує комутацію для вхідних та вихідних дзвінків між мережею 2G та іншими мережами.
- **Вузол керування рухом (MSC/VLR):** Відповідає за ведення бази даних абонентів та їхніх місцезнаходжень.
- **Вузол аутентифікації та авторизації (AUC):** Відповідає за захист від несанкціонованого доступу до мережі.
- **Вузол передачі SMS (SMS-C):** Відповідає за обробку та передачу текстових коротких повідомлень.
- **Вузол передачі даних (GPRS):** Забезпечує передачу даних в мережі 2G за допомогою GPRS (General Packet Radio Service).

Важливо також зауважити на етапі переходу від 2G до 2.5G, який відбувався приблизно у кінці 1990-х - початку 2000-х років. Точні дати можуть відрізнятися в різних регіонах світу, оскільки впровадження нових технологій часто відбувається етапами та може залежати від рішень окремих операторів мобільного зв'язку та ринкових умов. Головною технологією 2.5G є GPRS (General Packet Radio Service), яка надавала можливість передачі даних через пакетну комутацію.

Перехід від 2G (другого покоління) до 2.5G позначає певний етап розвитку мобільних телефонних мереж і технологій передачі даних. Основна характеристика переходу від 2G до 2.5G - це вдосконалення передачі даних та

можливість використання інтернет-схожих послуг, але це ще не є повноцінною 3G (третім поколінням) технологією [18].

Основні риси переходу від 2G до 2.5G включають:

- **GPRS (General Packet Radio Service):** GPRS вперше впроваджено у мережах 2.5G. Він забезпечує покращену передачу даних, дозволяючи використовувати інтернет-схожі послуги, такі як електронна пошта та доступ до веб-сайтів, через пакетну передачу даних.
- **Покращена передача даних:** 2.5G покращила швидкість передачі даних порівняно з технологією 2G, що забезпечило кращу продуктивність для користувачів при використанні послуг, які вимагають передачу даних.
- **Підтримка мультимедіа:** хоча 2.5G не має всіх можливостей мультимедійних послуг 3G, вона вже вносить певні поліпшення у плані передачі мультимедійних даних, таких як картинки та звук.
- **Підтримка більш швидкісних послуг:** 2.5G відкриває можливість для більш швидкісних послуг порівняно із звичайними мобільними службами 2G.

Однак, важливо відзначити, що 2.5G все ще заснована на основі технології 2G, і це не є повноцінною технологією 3G. 2.5G є проміжним етапом у вдосконаленні мобільних мереж перед введенням більш розвинутих технологій 3G та 4G. Нижче представлена діаграма, яка акцентує наявність GPRS у 2G.

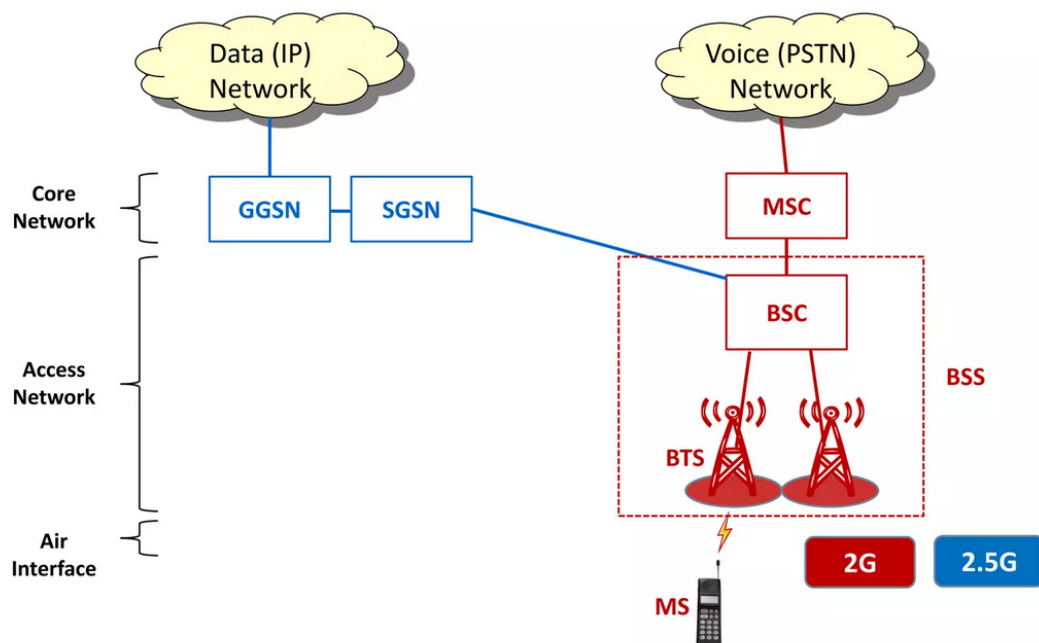


Рис. 1.3. Архітектура GSM-мережі із додаванням технологій покращення передачі даних GPRS.

Перехід від 2G до 2.5G відбувався приблизно у кінці 1990-х - початку 2000-х років. Точні дати можуть відрізнятися в різних регіонах світу, оскільки впровадження нових технологій часто відбувається етапами та може залежати від рішень окремих операторів мобільного зв'язку та ринкових умов. Головною технологією 2.5G є GPRS. Для її реалізації необхідно було розширити поточну інфраструктуру наступними елементами [6]:

1. **GPRS (General Packet Radio Service):** GPRS є аббревіатурою від "General Packet Radio Service" і представляє собою технологію передачі даних у мобільних мережах. Це розширення стандарту GSM, яке вперше впроваджено в системах 2.5G. GPRS дозволяє передавати дані в пакетному режимі, що означає, що інформація розбивається на пакети та передається по мережі, коли це необхідно. Це дозволяє ефективніше використовувати ресурси мережі та підтримує послуги, такі як доступ до Інтернету, електронна пошта та інші мультимедійні додатки.

2. **SGSN (Serving GPRS Support Node):** SGSN є скороченням від "Serving GPRS Support Node" і представляє собою вузол, який забезпечує обслуговування абонентів GPRS в мобільній мережі. SGSN відповідає за керування сесіями передачі даних, ведення статистики та вирішення питань, пов'язаних з безпекою в контексті GPRS.
3. **GGSN (Gateway GPRS Support Node):** GGSN є аббревіатурою від "Gateway GPRS Support Node" і виконує роль шлюзу між мобільною мережею та зовнішніми пакетними мережами, такими як Інтернет або корпоративні мережі. GGSN відповідає за маршрутизацію трафіку GPRS між абонентами і зовнішніми мережами, а також за взаємодію з іншими GPRS-мережами. Цей вузол відіграє ключову роль у забезпеченні з'єднання між мобільними абонентами та іншими мережами.

1.3. Архітектура та особливості роботи мереж типу 3G.

3G або мобільна технологія третього покоління була впроваджена на початку 2000-х років. Вона використовує мережеву архітектуру з комутацією пакетів, що дозволяє досягати вищих швидкостей передачі даних та підтримує мультимедійні застосунки. Еволюція від 2G до 3G представляє собою значущий стрибок у розвитку мобільних технологій, із збільшенням швидкості передачі даних, розширенням спектра послуг та покращенням якості зв'язку [17]. Нижче наведено деякі ключові аспекти еволюції:

1. Швидкість передачі даних:

- **2G (GPRS/EDGE):** Введення GPRS (General Packet Radio Service) та EDGE (Enhanced Data Rates for GSM Evolution) дозволило значно поліпшити швидкість передачі даних у порівнянні з традиційним 2G. GPRS забезпечував пакетну передачу даних, що дозволяло завантажувати інтернет-сторінки та використовувати послуги електронної пошти.

- **3G (UMTS/HSPA):** В стандарті 3G (Universal Mobile Telecommunications System), а також його покращенні HSPA (High-Speed Packet Access), була додана підтримка високошвидкісної передачі даних, що дозволило використовувати більш різноманітні мультимедійні послуги, такі як відеозв'язок та стрімінгове відео [14].

2. Розширення послуг:

- **2G:** Основною функцією 2G було забезпечення голосового зв'язку, але впровадження GPRS/EDGE дозволило використовувати послуги передачі даних.
- **3G:** Стандарт 3G відкрив нові можливості для багатогранних послуг, включаючи високошвидкісний доступ до Інтернету, відеозв'язок, мультимедійні потокові послуги та інші передові додатки.

3. Технологічні вдосконалення:

- **2G:** В 2G використовувалися технології, такі як GSM, CDMA, GPRS, EDGE.
- **3G:** Технології 3G включають UMTS (Universal Mobile Telecommunications System) та HSPA (High-Speed Packet Access), які забезпечують високошвидкісну передачу даних та покращену якість голосу [24].

4. Покращена якість обслуговування:

- **2G:** Головний фокус був на голосовому зв'язку.
- **3G:** Забезпечена вища якість обслуговування як для голосового, так і для даних, зокрема завдяки високій швидкості передачі даних та покращеним технологіям компресії аудіо та відео.

На рис. 1.4. представлено еволюцію мережі стільникового зв'язку, де різними кольорами відмічено еволюційний розвиток [24].

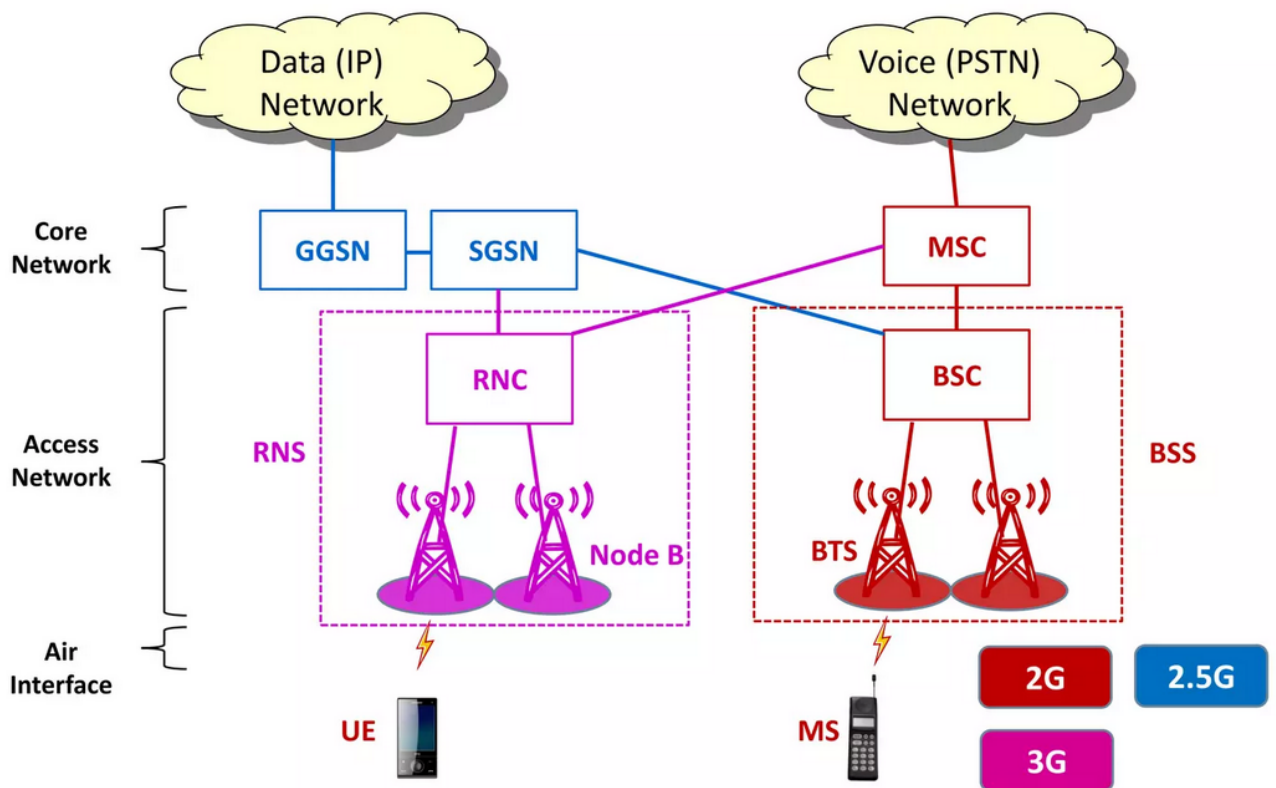


Рис. 1.4. Архітектура 3G-мережі.

До попереднього набору технологій із функціональної точки зору було додано наступні елементи [22]:

- **RNC:** Radio Network Controller (контролер радіомережі) - елемент архітектури мобільної мережі UMTS, відповідальний за керування радіоресурсами та управління базовими станціями (Node B).
- **RNS:** Radio Network Subsystem (підсистема радіомережі) - складова частина архітектури UMTS, яка включає в себе RNC та базові станції (NodeB), відповідні за обробку та передачу радіосигналів.
- **UE:** User Equipment (користувацьке обладнання) - термін, що використовується для позначення обладнання, яке використовує користувач для доступу до мобільної мережі, таке як смартфон, телефон, планшет або інші пристрої.

1.4. Архітектура та особливості роботи мереж типу 4G.

4G або мобільна технологія четвертого покоління була впроваджена наприкінці 2000-х років. Вона використовує мережеву архітектуру з використанням протоколу Internet Protocol (IP), що дозволяє досягати вищих швидкостей передачі даних та підтримує застосунки з великою пропускнуою здатністю, такі як стрімінг відео та онлайн-геймінг [11]. Основні функціональні відмінності між 3G та 4G включають:

1. Швидкість передачі даних:

- **3G:** Зазвичай досягає максимальної швидкості передачі даних приблизно 384 kbps для рухомих користувачів та до 2 Mbps для стаціонарних.
- **4G:** Забезпечує набагато вищі швидкості, зазвичай в діапазоні від 20 Mbps до сотень Mbps, з можливістю перевищення 1 Gbps у певних умовах [10].

2. Технологія передачі даних:

- **3G:** Використовує CDMA (Code Division Multiple Access) або WCDMA (Wideband Code Division Multiple Access) для передачі даних.
- **4G:** Використовує OFDMA (Orthogonal Frequency Division Multiple Access) або LTE (Long-Term Evolution), як правило, для ефективної передачі даних [8].

3. Якість зв'язку та покриття:

- **3G:** Забезпечує прийнятну якість зв'язку та покриття, але може виникати перенавантаження у місцях з великою кількістю користувачів.
- **4G:** Забезпечує вищу якість зв'язку та ширше покриття, зменшуючи перенавантаження мережі [9]

4. Затримка (Lag):

- **3G:** Має відносно велику затримку при передачі даних.
- **4G:** Забезпечує меншу затримку, що робить його більш ефективним для реального часу та інтерактивних додатків.

5. Технології та додатки:

- **3G:** Стандартно підтримує основні послуги передачі даних та мультимедіа.
- **4G:** Спрямований на високошвидкісний доступ до Інтернету, підтримку великих обсягів даних, стрімінг відео в високій роздільності та інші високопродуктивні застосунки.

6. Технології зв'язку:

- **3G:** Використовує CDMA, UMTS, HSPA.
- **4G:** Використовує LTE, WiMAX.

Загалом, 4G забезпечує значно кращі швидкості передачі даних та покращені можливості для використання великих обсягів даних та високоякісних мультимедійних застосунків порівняно з 3G.

Архітектура мережі 4G включає в себе [11]:

- **EPC:** Evolved Packet Core (покращене ядро пакетного з'єднання) - це центральна частина архітектури мережі 4G, відповідальна за обробку та передачу IP-пакетів у мережі.
- **MME:** Mobility Management Entity (система управління мобільністю) - це елемент EPC, який відповідає за управління сигналізацією та здійсненням реєстрації пристроїв в мережі.
- **S-GW:** Serving Gateway (службовий шлюз) - це елемент EPC, який управляє потоком даних між мобільним пристроєм (UE) та мережею.
- **P-GW:** PDN Gateway (шлюз мережі пакетних даних) - це елемент EPC, який забезпечує доступ мобільного пристрою до Інтернету та інших мереж.
- **PDN:** Packet Data Network (мережа пакетних даних) - це загальна термінологія, яка вказує на мережу, яка передає дані у формі пакетів.
- **eNodeB:** Evolved NodeB (покращена базова станція) - це частина мережі 4G, яка взаємодіє з мобільними пристроями (UE) та відповідає за управління радіоресурсами.

Нижче представлена діаграма, яка ілюструє додавання 4G до існуючого набору технологій [10, 5, 21].

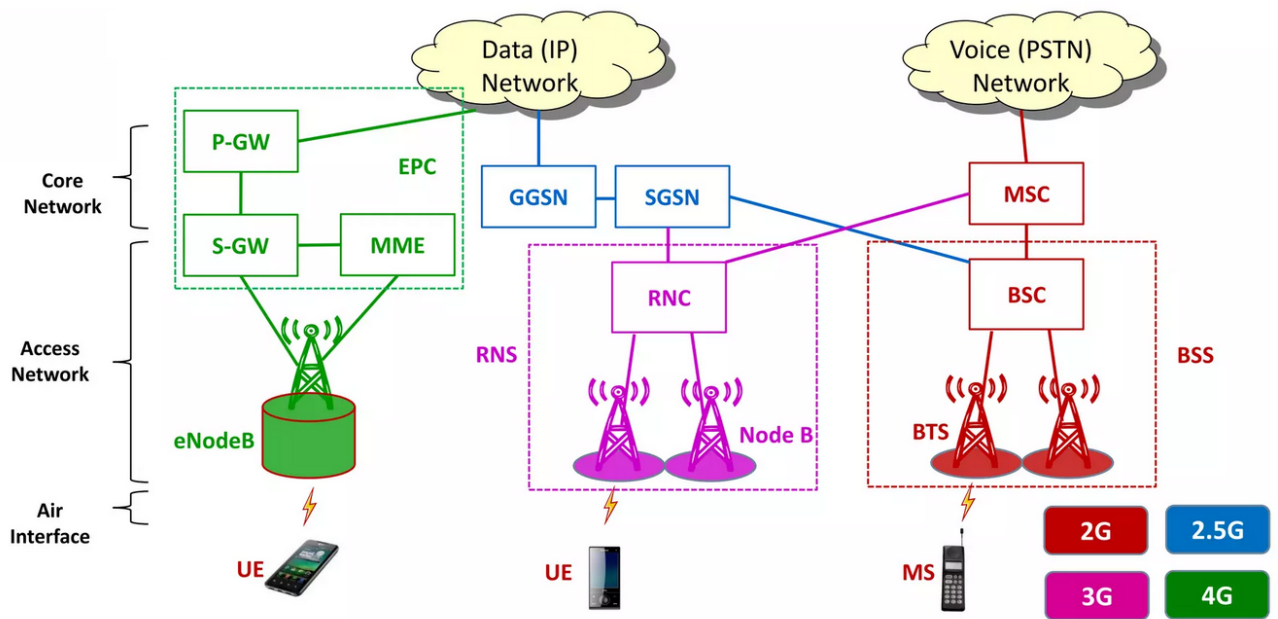


Рис. 1.5. Архітектура 4G-мережі.

1.5. Архітектура та особливості роботи мереж типу 5G.

Основні відмінності між 4G та 5G включають [7, 21]:

1. Швидкість передачі даних:

- **4G:** Забезпечує швидкості від декількох Мбіт/с до кількох сотень Мбіт/с.
- **5G:** Передбачає набагато вищі швидкості, включаючи кілька Гбіт/с, навіть до 10 Гбіт/с та більше.

2. Затримка (Lag):

- **4G:** Має прийнятну, але відносно велику затримку.
- **5G:** Зменшує затримку до кількох мілісекунд, що робить його ідеальним для реального часу та інтерактивних додатків.

3. Ємність мережі:

- **4G:** Має обмежену ємність, особливо в областях з великою кількістю підключених пристроїв.
- **5G:** Забезпечує високу ємність мережі та можливість підключення великої кількості пристроїв на квадратний кілометр.

4. Частоти та діапазони:

- **4G:** Використовує низькі, середні та високі частоти (600 MHz - 2.5 GHz).
- **5G:** Розширює спектр використовуваних частот, включаючи високочастотні міліметрові хвилі (24 GHz та вище).

5. Технології та архітектура:

- **4G:** Використовує технології, такі як LTE.
- **5G:** Використовує нові технології, такі як NR (New Radio), та має різні архітектурні зміни.

6. Підтримка IoT та масштабування:

- **4G:** Забезпечує обмежену підтримку для великої кількості підключених пристроїв.
- **5G:** Орієнтований на велике масштабування IoT та підтримує велику кількість одночасно підключених пристроїв.

7. Застосунки:

- **4G:** Зосереджений на швидкісному доступі до даних.
- **5G:** Враховує високий обсяг даних, реальний час, велику кількість підключених пристроїв, AR (розширена реальність), VR (віртуальна реальність) та інші високотехнологічні застосунки.

8. Безпека:

- **5G:** Має покращені заходи безпеки порівняно з 4G.

5G призначений для забезпечення вищої швидкості передачі даних, зменшення затримки та розширення можливостей для нових технологій та застосунків [25]. Перехід від 4G до 5G вимагає значних архітектурних змін, оскільки включає розгортання нових базових станцій, обладнання ядра мережі, волоконно-оптичних ліній та інших компонентів 5G:

1. **NGCN:** Next Generation Core Network (мережа наступного покоління) —термін вказує на майбутню архітектуру ядра мобільної мережі, яка використовується для обробки та передачі даних в мережі наступного покоління 5G.

2. **gNodeB:** Next Generation NodeB (вузол наступного покоління) – вузол базової станції, який використовується в мережі наступного покоління (наприклад, 5G). gNodeB забезпечує безпосередній зв'язок між мобільними пристроями та мережею.
3. **NR:** New Radio (новий радіоінтерфейс) – стандарт радіоінтерфейсу, який використовується в мережах наступного покоління 5G. NR розроблений для забезпечення високошвидкісного бездротового зв'язку та підтримки різноманітних послуг, включаючи широкосмуговий інтернет, масштабовану віртуальну реальність та інші додатки нового покоління.

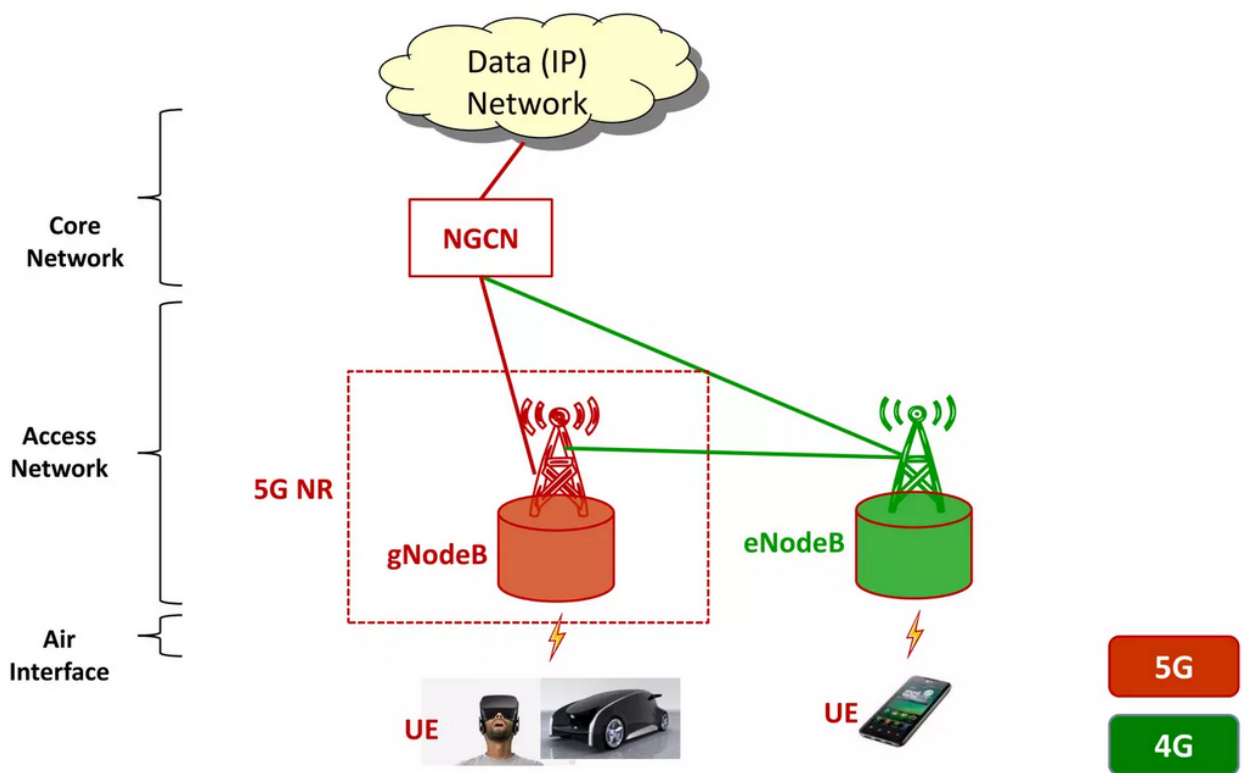


Рис. 1.6. Архітектура 5G-мережі.

Перехід від 4G до 5G є багатоетапним процесом, який включає в себе наступні етапи:

1. **Стандартизація та розробка технологій:** розробка та прийняття нових стандартів для 5G технологій. Основними організаціями, що відповідають

за розробку стандартів, є Міжнародний союз зв'язку (ITU) та Інститут інженерів електротехніки та електроніки (IEEE).

2. **Тестування та випробування:** проведення тестів та випробувань нових технологій 5G для забезпечення їх ефективності та сумісності.
3. **Розгортання інфраструктури:** розгортання нової інфраструктури для 5G, такої як базові станції (eNodeB), обладнання ядрої мережі (Evolved Packet Core), антени, а також волоконно-оптичні лінії для передачі великої кількості даних.
4. **Споживатські пристрої:** розробка та випуск на ринок сумісних з 5G смартфонів, планшеток, IoT-пристроїв та інших гаджетів.
5. **Тестування мережі:** проведення великих масштабів тестів мережі для визначення її ефективності, масштабованості та стійкості.
6. **Випробування в реальних умовах:** запуск обмежених комерційних служб 5G в обраних регіонах для випробування технології в реальних умовах та отримання зворотного зв'язку від користувачів.
7. **Широкомасштабне розгортання:** повномасштабне розгортання 5G мереж в різних регіонах та країнах, щоб забезпечити доступність для широкого кола користувачів.
8. **Оновлення існуючих мереж:** оновлення існуючих 4G мереж для забезпечення сумісності та плавного переходу до 5G.
9. **Вдосконалення сервісів та додатків:** розробка та впровадження нових сервісів та додатків, які оптимально використовують можливості 5G, таких як високоякісне відео, розширена реальність, віртуальна реальність тощо.

Цей процес вимагає співпраці між операторами зв'язку, виробниками обладнання, розробниками програмного забезпечення та регуляторами для забезпечення успішного впровадження та функціонування 5G мережі.

Висновки

Мережі 1G (першої генерації) були піонерськими мобільними телефонними системами, запровадженими у 1980-1990 роках, і вони були орієнтовані на передачу аналогового звукового сигналу. Основні характеристики мереж 1G включають аналогову технологію, низьку ємність, низьку якість звуку, великі та важкі мобільні телефони, обмежене покриття та роумінг, а також різні нестандартизовані системи у різних країнах. Мережі 1G виявилися недостатньо ефективними через нераціональне використання виділеної смуги частот, що призвело до появи нових стандартів мобільного зв'язку. Перше покоління (1G), запроваджене в 1980-1990 роках, було аналоговим та мав обмежену якість звуку. Телефони були великі та важкі, а мережі обмежувалися низькою ємністю та покриттям.

Наразі існують кілька поколінь мобільних стандартів, таких як 2G, 3G, 4G LTE та 5G, кожне з яких має свої унікальні характеристики та застосування:

- Мережі 2G надають цифровий голосовий зв'язок та можливість відправки SMS.
- Мережі 3G дозволяють передачу даних з високою швидкістю, відеодзвінки та інтернет-серфінг.
- Мережі 4G LTE забезпечують високошвидкісний Інтернет, стрімінг відео та високоякісний голосовий зв'язок.
- Мережі 5G надають найвищу швидкість передачі даних, низьку затримку та підтримку великої кількості пристроїв IoT.

Розвиток технологій мобільного зв'язку продовжується, і стандарти 4G LTE та 5G стають все більш поширеними, замінюючи застарілі стандарти. Вибір мобільного стандарту залежить від потреб користувачів та регіональних особливостей. Сучасні системи мобільного зв'язку мають складну інфраструктуру, яка забезпечує надійний та швидкий доступ до мобільних послуг. Архітектура цих систем базується на декількох ключових компонентах:

1. Мобільні пристрої: смартфони, планшети та інші пристрої, які використовуються абонентами для доступу до мережі. Мобільні пристрої мають вбудовані радіоінтерфейси, які дозволяють їм підключатися до мережі оператора мобільного зв'язку.

2. Мобільні базові станції: апаратне обладнання, яке розміщується по всій місцевості та забезпечує покриття мережі. Кожна БС видає радіосигнал для зв'язку з мобільними пристроями в своєму радіусі дії. Вони можуть бути встановлені на дахах будівель, стовпах і навіть в метрополітенах.

3. Мережевий ядро: це центральна частина мережі, де відбувається обробка даних, маршрутизація та комутація. Мережеве ядро відповідає за забезпечення з'єднання між мобільними пристроями та іншими мережами, такими як Інтернет.

4. Сервери і обладнання управління мережею: компоненти відповідають за управління ресурсами мережі, включаючи реєстрацію абонентів, аутентифікацію та авторизацію, а також контроль за якістю обслуговування.

5. Бездротовий канал: мобільні пристрої та БС використовують бездротовий канал для обміну даними. Цей канал використовує радіохвилі для передачі сигналів між пристроями та мережею.

6. Оператор мобільного зв'язку: забезпечує управління та підтримку мережі. Він також відповідає за надання послуг абонентам і підтримку мобільних пристроїв.

Архітектура 4G LTE і 5G базується на інтернет-протоколах та стандартах передачі даних, що робить їх досить схожими на роботу традиційного Інтернету. Основні особливості архітектури мобільних систем включають:

Загалом, сучасні системи мобільного зв'язку мають високу пропускну здатність, низьку затримку та підтримують широкий спектр послуг та пристроїв. Такі системи стали невід'ємною частиною сучасного життя та господарства, і їх розвиток продовжується для задоволення зростаючих потреб користувачів.

РОЗДІЛ 2

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ НАДІЙНОСТІ ІНФРАСТРУКТУРИ

2.1 Загальна характеристика доступних хмарних сервісів

Хмарні середовища – це інформаційно-технологічні інфраструктури, які надають доступ до різних обчислювальних ресурсів через мережу Інтернет. Ці середовища включають в себе різноманітні послуги та ресурси, які можна використовувати за допомогою інтернет-підключення. Хмарні послуги представляють собою програми та платформи, які допомагають підприємствам підвищити продуктивність і ефективність роботи, завдяки можливості віддаленого доступу до робочих ресурсів і інформації цілодобово, без обмежень у часі [26]. Ці послуги розташовані на серверах постачальників хмарних послуг, що звільняє клієнтів від необхідності будувати власну складну ІТ-інфраструктуру та вкладати в дороге обладнання.

В даний момент хмарні служби, такі як Google, Amazon, Dropbox, Microsoft OneDrive, які надають послуги хмарного сховища та обробки даних, набувають великої популярності. Основна причина використання хмарних продуктів - це зручність та доступність наданих послуг. Завдяки використанню технологій хмари можливо зекономити фінансові витрати на утримання та обслуговування серверів для зберігання та захисту інформації. Всі проблеми, що виникають під час зберігання та обробки даних, переносяться на постачальника хмарних послуг [1].

Основні характеристики хмарних середовищ [26]:

1. **Доступність за вимогою (On-Demand Access):** Користувачі можуть отримати доступ до ресурсів (обчислювальна потужність, зберігання, мережі) у будь-який час і з будь-якого місця.

2. Самообслуговування (Self-Service): Можливість користувачів самотійно конфігурувати та управляти ресурсами без прямого втручання з боку провайдера.
3. Масштабованість (Scalability): Здатність збільшувати або зменшувати обсяг ресурсів в залежності від потреб користувача.
4. Модель плати за використання (Pay-as-You-Go): Сплата за фактично використані ресурси, що дозволяє економити витрати.
5. Віртуалізація ресурсів: Використання віртуалізації для створення віртуальних екземплярів обчислювальних ресурсів.
6. Гнучкість (Flexibility): Можливість легко адаптувати конфігурації та параметри ресурсів.
7. Інфраструктура як код (Infrastructure as Code - IaC): Використання програмного коду для автоматизації управління та налаштуванням інфраструктури.

Хмарні середовища використовуються для розгортання, управління та масштабування застосунків без необхідності прямого володіння та утримання фізичної інфраструктури [27]. Основним завданням систем сховища є завдання обробки даних в реальному часі; проте виникає протиріччя між практичною потребою в обробці даних значущих бітів в реальному часі, обмеженими апаратними ресурсами сучасних систем, вартістю, надійністю та продуктивністю. Таким чином, необхідно збільшити швидкість арифметичних обчислень, надійність та доступність, розробивши нові математичні моделі обробки даних в хмарі, алгоритми яких використовують методи, що скорочують їхній час, а також створити нові алгоритми обробки та зберігання даних для зменшення фінансових витрат.

Коли постачальник хмарних послуг зберігає користувацькі дані, він повинен мати можливість повертати ці дані користувачеві за його вимогою. З урахуванням перерв у мережі, помилок користувача та інших обставин, виконання цього умови надійним та визначеним способом може бути складним [4]. Для підвищення надійності та стійкості обробки та зберігання даних

доцільно використовувати розподілені схеми зберігання даних на основі принципів модульної арифметики. Одним із перспективних напрямків модульної арифметики є розробка математичних методів для зберігання та обробки великомасштабних даних з високою надійністю в хмарному середовищі.

При побудові великої хмари, на якій працюють всі бізнес-системи компанії, необхідно забезпечити високу стійкість до збоїв, регулярно робити резервні копії даних так, щоб при виходженні сервера з ладу хмари не вимикалися одразу, а негайно переходили на інший сервер, або (протягом розумного часу) відновлювалися з резервних копій [48].

Використання хмарних технологій для підвищення надійності інфраструктури може бути важливим аспектом для підприємств та організацій. Це може допомогти у запобіганні відмов, забезпеченні доступності послуг та забезпеченні високої якості обслуговування. Використання хмарних технологій для підвищення надійності інфраструктури є актуальним підходом у сучасному ІТ-середовищі.

1. **Хмарні нативні технології (Cloud-Native Technologies):** Це поняття включає розробку та використання додатків, спеціально спроектованих для хмарних середовищ, що включає в себе мікросервіси, контейнеризацію (наприклад, Docker), оркестрацію контейнерів (наприклад, Kubernetes) та неперервну інтеграцію/неперервне розгортання (CI/CD) [27].
2. **Serverless архітектура:** Це модель, у якій розробники можуть створювати та запускати додатки та служби без необхідності управління інфраструктурою. Приклади включають AWS Lambda, Azure Functions та Google Cloud Functions [26,28].
3. **Інтеграція з AI та машинним навчанням:** Багато хмарних платформ тепер інтегрують можливості штучного інтелекту та машинного навчання, надаючи передові аналітичні та обчислювальні можливості.

4. **Хмарна безпека та відповідність стандартам:** Оновлення в області безпеки, такі як поліпшені шифрування та більш суворі політики керування ідентифікацією та доступом, а також забезпечення відповідності до глобальних стандартів та регуляцій, таких як GDPR.
5. **Edge Computing і Інтеграція з Хмарами:** Розвиток edge computing, де обробка даних відбувається ближче до місця збору даних, тісно інтегрується з хмарними технологіями, забезпечуючи кращу продуктивність та зменшення затримок [26]
6. **Інтеграція хмарних сервісів з IoT (Інтернет речей):** Хмарні платформи все частіше використовуються для зберігання та обробки даних з IoT пристроїв, що вимагає специфічних рішень для збору, аналізу та безпечного зберігання великого обсягу даних.
7. **Використання Штучного Інтелекту для оптимізації хмарних ресурсів:** Розвиток алгоритмів AI, які допомагають автоматизувати та оптимізувати використання хмарних ресурсів, наприклад, для прогнозування навантаження та оптимізації використання енергії.

2.2. Хмарні служби для забезпечення надійності

Хмарні технології дозволяють автоматизовано зберігати резервні копії даних на віддалених серверах, забезпечуючи надійність і доступність інформації [32]. Завдяки цьому підходу, користувачі та підприємства можуть уникнути втрати важливих даних через випадкове видалення, технічні відмови або інші непередбачені обставини.

Відновлення даних в разі втрати або видалення.

У випадку втрати або видалення даних, важливо мати ефективний процес відновлення. Хмарні служби часто надають можливість швидкого та простого відновлення резервних копій. Вони забезпечують інтерфейс для вибору

конкретного моменту в часі, на який слід відновити дані, дозволяючи максимально зменшити втрати інформації.

Переваги використання хмарних служб для резервного копіювання та відновлення даних:

- Автоматизація: Процес резервного копіювання відбувається автоматично за заданим графіком, що зменшує ризик пропуску важливих даних.
- Надійність: Дані зберігаються на віддалених та безпечних серверах, що забезпечує їхню надійність та доступність у будь-який момент.
- Швидкість відновлення: Можливість швидкого відновлення даних з резервних копій дозволяє мінімізувати час відсутності доступу до важливої інформації. [32]

Загалом, використання хмарних служб для резервного копіювання та відновлення даних є стратегічним кроком у напрямку забезпечення безпеки та стабільності інформаційної інфраструктури, надаючи користувачам та підприємствам впевненість у захищеності їхніх цінних даних.

2.3. Географічна розподіленість

Географічна розподіленість хмарних середовищ - це концепція, яка передбачає розміщення хмарних обчислень, послуг та ресурсів у різних географічних областях чи центрах даних. Це стратегічне розташування дозволяє забезпечити велику доступність та високу продуктивність для користувачів та підприємств у різних частинах світу.

Основні аспекти географічної розподіленості хмарних середовищ включають:

- Близькість до користувача: розміщення ресурсів хмарного середовища близько до кінцевого користувача дозволяє скоротити час відповіді та покращити загальний досвід використання послуг.

- **Бізнес-неперервність:** географічна розподіленість дозволяє забезпечити бізнес-неперервність, оскільки вона робить систему менш вразливою до природних катастроф, технічних відмов чи інших непередбачених подій в одному регіоні.
- **Відмінність нормативів та державних вимог:** розподіленість може враховувати різноманіття законодавчих вимог та нормативів у різних країнах чи регіонах.
- **Забезпечення захисту даних та конфіденційності:** розташування даних у визначених юрисдикціях допомагає враховувати вимоги до захисту конфіденційності та безпеки даних відповідно до законів конкретного регіону.
- **Оптимізація використання ресурсів:** географічна розподіленість може дозволити оптимізувати використання ресурсів, забезпечуючи більш ефективне використання обчислювальних потужностей та мережевих ресурсів.
- **Схеми віддаленого резервування (Disaster Recovery):** розподіленість може бути використана для створення схем віддаленого резервування, що дозволяє забезпечити відновлення послуг у випадку відмови в одному регіоні.
- **Мінімізація затримок та покращення швидкості:** правильне розташування ресурсів може допомогти мінімізувати затримки в передачі даних та покращити швидкість обчислення.

Загальний вибір географічної розподіленості повинен враховувати специфічні потреби та стратегії конкретної організації, її клієнтів та бізнес-моделі.

2.4. Автоматичне масштабування

Автоматичне масштабування хмарних середовищ - це концепція, яка передбачає автоматизацію процесів розширення чи зменшення ресурсів

(обчислювальної потужності, мережевих ресурсів, обсягу сховища тощо) у залежності від поточних потреб або навантаження системи. Це дозволяє оптимізувати використання ресурсів, забезпечуючи ефективну роботу системи при змінних обсягах роботи або навантаження.

У хмарному обчисленні існують різні типи масштабування інфраструктури, які дозволяють підприємствам адаптувати свої ресурси до змінних потреб та завдань. Основні типи масштабування інфраструктури у хмарному середовищі включають [33]:

1. Вертикальне масштабування (Vertical Scaling):

- Вертикальне масштабування відбувається за допомогою збільшення обчислювальних ресурсів одного сервера, підняттям його продуктивності та ресурсів.
- Цей тип масштабування дозволяє збільшувати потужність сервера, який вже працює, шляхом додавання процесорів, оперативної пам'яті, об'єму сховища і інших ресурсів.
- Вертикальне масштабування підходить для програм, які потребують більшої обчислювальної потужності.

2. Горизонтальне масштабування (Horizontal Scaling):

- Горизонтальне масштабування включає додавання нових серверів (інстанцій) до інфраструктури з метою збільшення загальної обчислювальної потужності.
- Цей тип масштабування підходить для розподілених систем і додатків, які можуть бути розділені на менші компоненти, які працюють на різних серверах.
- Горизонтальне масштабування забезпечує вищу доступність і здатність обробляти великий обсяг трафіку.

3. Автоматичне масштабування (Auto Scaling):

- Автоматичне масштабування включає в себе автоматизований процес збільшення або зменшення ресурсів відповідно до поточного навантаження.

- Система автоматичного масштабування використовує метрики, такі як CPU використання, обсяг трафіку, або інші показники, для прийняття рішення про додавання або видалення серверів.
- Цей підхід допомагає зменшити витрати на інфраструктуру та забезпечує ефективне використання ресурсів.

4. Гібридне масштабування (Hybrid Scaling):

- Гібридне масштабування комбінує вертикальне і горизонтальне масштабування для досягнення оптимального рішення.
- Наприклад, великі задачі можуть бути розділені на менші компоненти, які потім можна масштабувати вертикально, а потім розгортати на більше кількість серверів для горизонтального масштабування.

Користувачі хмарних послуг можуть вибирати тип масштабування відповідно до своїх потреб та обсягу роботи, що дозволяє ефективно використовувати ресурси та забезпечувати високу доступність і продуктивність системи.

2.5. Системи моніторингу та управління

Системи моніторингу та управління хмарних середовищ відіграють важливу роль у забезпеченні ефективності, доступності та безпеки віртуальних ресурсів та послуг в хмарних обчисленнях [32]. Ці системи дозволяють адміністраторам ефективно контролювати та оптимізувати використання ресурсів, моніторити стан системи та реагувати на події в реальному часі. Деякі з основних функцій систем моніторингу та управління в хмарних середовищах включають:

1. Моніторинг ресурсів. Системи надають можливість стежити за використанням ресурсів, таких як ЦП, пам'ять, сховище та мережа. Це допомагає виявляти проблеми з продуктивністю та реагувати на них.

2. Автоматизоване масштабування. За допомогою моніторингу навантаження, системи можуть автоматично масштабувати ресурси, щоб забезпечити оптимальне використання і відповідь на збільшення або зменшення потоку роботи.
3. Управління контейнерами. Деякі системи дозволяють ефективно управляти контейнеризованими додатками, надаючи інструменти для розгортання, масштабування та управління контейнерами.
4. Моніторинг мережі. Вивчення стану мережі та швидкодії є важливим для забезпечення надійного з'єднання між різними компонентами системи в хмарному середовищі.
5. Спостереження за безпекою. Визначення та виявлення потенційних загроз безпеці є критичним для забезпечення безпеки даних та ресурсів в хмарному середовищі.
6. Журналювання та аналіз подій. Запис та аналіз подій дозволяють виявляти аномалії, здійснювати аудит та відслідковувати події для поліпшення безпеки та ефективності.
7. Управління правами та ресурсами. Надання можливості контролювати доступ до ресурсів, встановлювати права доступу та ефективно управляти ресурсами на рівні користувачів та додатків.
8. Системи резервного копіювання та відновлення. Управління резервним копіюванням та відновленням даних, щоб забезпечити надійність та безпеку інформації.
9. Інтеграція з API та іншими службам. Можливість інтеграції з API та іншими сервісами для автоматизації та розширення функціональності системи.

Ефективне використання систем моніторингу та управління є ключем до успіху в хмарному обчисленні, дозволяючи підтримувати оптимальний стан та ефективність хмарних середовищ.

Існує багато різних систем моніторингу для хмарних середовищ, які надають різноманітні функції та можливості для відслідковування, аналізу та управління ресурсами.

1. **Amazon CloudWatch (AWS):** CloudWatch від Amazon Web Services (AWS) є повністю управляється службою моніторингу, яка дозволяє відслідковувати ресурси та додатки у хмарному середовищі AWS. Вона надає можливості моніторингу ЦП, сховища, мережі, а також різні сервіси, такі як Amazon EC2 та Amazon RDS [26].
2. **Azure Monitor (Microsoft Azure):** Azure Monitor від Microsoft Azure забезпечує моніторинг інфраструктури, додатків та мережі. Це дозволяє відслідковувати метрики, логи та трасування додатків, щоб забезпечити комплексний огляд стану системи [27].
3. **Google Cloud Monitoring (GCP):** Google Cloud Monitoring від Google Cloud Platform (GCP) надає можливості моніторингу для різноманітних ресурсів, включаючи віртуальні машини, сховища та служби, такі як Google Cloud Storage та Google Kubernetes Engine [28].
4. **Datadog:** Datadog є популярною системою моніторингу та аналізу, яка підтримує різні хмарні середовища, включаючи AWS, Azure, GCP, Kubernetes та інші. Вона дозволяє відслідковувати різні метрики, розробляти панелі моніторингу та надає алерти для реагування на події [30].

2.6. Автоматизована система управління

Інструменти конфігурації та автоматизації є ключовими компонентами в управлінні інфраструктурою і додатками в хмарних середовищах. Ці інструменти допомагають забезпечити консистентність конфігурації, швидкість розгортання та ефективність операцій. Давайте розглянемо два популярних інструменти: Ansible та Terraform.

Інструменти конфігурації та автоматизації є ключовими компонентами в управлінні інфраструктурою і додатками в хмарних середовищах. Ці інструменти допомагають забезпечити консистентність конфігурації, швидкість розгортання та ефективність операцій. Давайте розглянемо два популярних інструменти: Ansible та Terraform.

1. Ansible – це відкритий інструмент автоматизації, який використовує декларативний мовний засіб для опису конфігурації та управління системами. Він використовує YAML-файли для опису бажаного стану системи, що робить його легким для читання та написання. [34] Ansible може виконувати різноманітні задачі, включаючи налаштування, установку програмного забезпечення, оновлення та інше, також має велику кількість модулів для взаємодії з різними системами, що дозволяє використовувати його для різноманітних задач.

Ansible широко використовується для автоматизації розгортання додатків, налаштування серверів, управління конфігурацією та інших операційних завдань.

2. Terraform – це інструмент для автоматизації управління інфраструктурою як коду (Infrastructure as Code, IaC) який використовує декларативний підхід до опису інфраструктури. Користувачі описують бажану структуру ресурсів і їх взаємозв'язки в конфігураційних файлах, а сам Terraform забезпечує реалізацію цієї конфігурації [31]. Також підтримує багато провайдерів, включаючи AWS, Azure, Google Cloud, VMware, і багато інших. Це дозволяє користувачам працювати з інфраструктурою у різних хмарних середовищах та на локальних серверах, не змінюючи код.

Переваги використання Ansible та Terraform для хмарної інфраструктури:

- декларативний підхід, обидва інструменти використовують декларативний підхід до конфігурації, що робить код читабельним та зрозумілим.

- мультиплатформенність, Terraform і Ansible підтримують багато провайдерів і хмарних середовищ, що дозволяє їм працювати з різними інфраструктурами.
- забезпечення консистентності: Застосування коду для конфігурації дозволяє забезпечити консистентність стану інфраструктури та легкість відстеження змін.

Інтеграція цих інструментів дозволяє забезпечити ефективне управління конфігурацією та автоматизоване розгортання ресурсів у хмарних середовищах.

2.7. Кібербезпека хмарних середовищ

Кібербезпека хмарних середовищ є важливою аспектом в умовах зростання використання хмарних технологій. Хмарні середовища включають в себе різноманітні сервіси, такі як обчислення, зберігання даних, мережеві ресурси та інші, які надаються через Інтернет.

Основні виклики та аспекти кібербезпеки хмарних середовищ [32]:

1. Аутентифікація та авторизація:

- Необхідно використовувати сильну аутентифікацію для забезпечення вірності користувачів.
- Контроль доступу до ресурсів і дані, щоб забезпечити, що тільки авторизовані особи мають доступ до конфіденційної інформації.

2. Шифрування даних:

- Застосування шифрування для захисту конфіденційної інформації в процесі передачі та зберігання в хмарі.

3. Мережева безпека:

- Захист мережевих комунікацій між хмарними ресурсами та користувачами.
- Використання мережевих заходів безпеки, таких як брандмауери та виявлення вторгнень.

4. Моніторинг та журналювання:

- Систематичний моніторинг активності для виявлення ненормальних або підозрілих подій.
- Журналювання подій для відслідковування дій користувачів та можливих загроз безпеці.

5. Безпека додатків:

- Забезпечення безпеки програмних засобів та додатків, які використовуються в хмарних середовищах.

6. Фізична безпека даних:

- Захист фізичного доступу до серверних приміщень та інфраструктури хмарних постачальників.

7. Резервне копіювання та відновлення:

- Регулярне створення резервних копій даних і розробка планів відновлення в разі катастрофи або втрати даних.

8. Дотримання вимог законодавства:

- Забезпечення відповідності до законодавства та нормативних вимог, особливо з урахуванням захисту персональних даних.

Важливо враховувати, що кібербезпека є постійним процесом, і стратегії безпеки повинні постійно оновлюватися, щоб враховувати нові загрози та вразливості.

Отже, застосування хмарних технологій істотно підвищує надійність інфраструктурних рішень, пропонуючи високу доступність сервісів завдяки георозподіленим центрам обробки даних, що гарантує їх неперервну роботу навіть в умовах локальних збоїв. Одночасно хмарні рішення відзначаються високою масштабованістю та гнучкістю, дозволяючи оперативно змінювати обсяги та конфігурацію ресурсів відповідно до потреб бізнесу. Це не тільки сприяє оптимізації витрат, але й забезпечує швидку адаптацію до ринкових вимог. Постачальники хмарних сервісів беруть на себе відповідальність за оновлення та підтримку інфраструктури, знижуючи тим самим навантаження на внутрішні IT-відділи і гарантуючи використання найсучасніших інновацій.

Крім того, хмарні платформи забезпечують вдосконалені можливості резервного копіювання та відновлення даних, що є критично важливим для запобігання втратам інформації. З погляду безпеки, хмарні сервіси часто пропонують більш високий рівень захисту порівняно з традиційними ІТ-інфраструктурами, включаючи захист від DDoS-атак, шифрування даних та інші заходи безпеки.

Економічно хмарні рішення вигідні завдяки моделі оплати за фактично використані ресурси і меншим початковим вкладенням у порівнянні з власними центрами обробки даних. Нарешті, хмарні технології відкривають нові можливості для інновацій, надаючи доступ до передових технологій, таких як штучний інтелект, машинне навчання та великі дані, без потреби в значних інвестиціях.

Висновки

У даному розділі наведено загальний опис хмарних сервісів та їхніх основних характеристик. Зазначено, що хмарні середовища надають доступ до різних обчислювальних ресурсів через Інтернет і включають в себе різноманітні послуги, спрощуючи доступ до інформації та обчислювальних ресурсів. Хмарні послуги сприяють збільшенню продуктивності та ефективності роботи підприємств. Розглянуто перспективні напрямки використання хмарних технологій, такі як хмарні нативні технології, serverless архітектура, інтеграція з штучним інтелектом та машинним навчанням, хмарна безпека та відповідність стандартам, edge computing та інтеграція з хмарами, інтеграція хмарних сервісів з IoT, та використання штучного інтелекту для оптимізації хмарних ресурсів.

Також розглянуто важливі аспекти використання хмарних технологій для забезпечення надійності інформації та географічної розподіленості хмарних середовищ. За допомогою хмарних технологій можна автоматизовано зберігати резервні копії даних на віддалених серверах, що забезпечує надійність та доступність інформації. Важливою є можливість швидкого та простого

відновлення даних у випадку їхньої втрати або видалення. Використання хмарних служб для резервного копіювання та відновлення даних має численні переваги, такі як автоматизація процесу, надійність зберігання та швидкість відновлення.

Географічна розподіленість хмарних середовищ стає важливою концепцією, оскільки вона дозволяє забезпечити доступність та продуктивність для користувачів та підприємств у різних частинах світу. Вона сприяє бізнес-неперервності, захисту даних та відповідності законодавству різних регіонів. Географічна розподіленість також може оптимізувати використання ресурсів та покращити швидкодію обчислень. Загалом, використання хмарних технологій для забезпечення надійності та географічної розподіленості є стратегічно важливим для організацій, що дозволяє їм зберігати та захищати дані, забезпечувати бізнес-неперервність та оптимізувати використання ресурсів.

У хмарному обчисленні існують різні типи масштабування інфраструктури, такі як вертикальне, горизонтальне, автоматичне та гібридне масштабування, які дозволяють адаптувати ресурси до змінних потреб і завдань.

Системи моніторингу та управління важливі для забезпечення ефективності, доступності і безпеки хмарних середовищ. Вони дозволяють контролювати ресурси, моніторити стан системи, реагувати на події в реальному часі і забезпечувати безпеку даних і ресурсів. Функції систем моніторингу та управління включають моніторинг ресурсів, автоматизоване масштабування, управління контейнерами, моніторинг мережі, спостереження за безпекою, журналювання та аналіз подій, управління правами та ресурсами, системи резервного копіювання та відновлення, а також інтеграцію з API та іншими службами.

У зв'язку із зростанням популярності хмарних сервісів також набирають популярності автоматизовані системи управління, які є важливими компонентами в управлінні інфраструктурою і додатками в хмарних середовищах, інструментами конфігурації та автоматизації. Ansible та Terraform є

популярними інструментами, які надають декларативний підхід до конфігурації та управління системами. Використання цих інструментів сприяє консистентності конфігурації, швидкому розгортанню та ефективності операцій.

У даному розділі також було піднято тему кібербезпеки в хмарних середовищах, оскільки вони включають різноманітні сервіси, доступні через Інтернет. Основні аспекти кібербезпеки включають аутентифікацію та авторизацію, шифрування даних, мережеву безпеку, моніторинг та журналювання, безпеку додатків, фізичну безпеку даних, резервне копіювання та відновлення, дотримання вимог законодавства. Стратегії безпеки повинні регулярно оновлюватися для врахування нових загроз та вразливостей.

Узагальнюючи, використання хмарних технологій дозволяє підвищити продуктивність, забезпечити безпеку та гнучкість, а також оптимізувати витрати.

РОЗДІЛ 3

ПІДВИЩЕННЯ НАДІЙНОСТІ ІНФРАСТРУКТУРИ ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ ШЛЯХОМ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ АВАРІЙНОГО ВІДНОВЛЕННЯ

3.1. Характеристика поняття аварійного відновлення (disaster recovery)

Disaster Recovery (або просто DR) — це набір інструментів та спеціалізоване програмне забезпечення, які вкупі допомагають швидко відновити ІТ-інфраструктуру, а також дані, роботу всіх систем та сервісів після збою [38]. Планування та стратегії відновлення після аварії спрямовані на реагування та відновлення під час аварій - подій, які переривають або повністю припиняють роботу підприємства. Типи аварій можуть включати:

- Природні катастрофи (наприклад, землетруси, повені, торнадо, урагани чи лісові пожежі)
- Пандемії та епідемії
- Кібератаки (наприклад, атаки з використанням зловмисного програмного забезпечення, DDoS та атаки вимагання викупу)
- Інші навмисні, людським фактором спричинені загрози, такі як терористичні чи біохімічні атаки
- Технологічні небезпеки (наприклад, відключення електроенергії, вибухи нафтопроводів та транспортні аварії)
- Відмови обладнання та апаратури

Цілісна стратегія відновлення після аварії повинна включати детальні вимоги щодо надзвичайних ситуацій, операцій резервного копіювання та процедур відновлення. При створенні стратегій відновлення після аварії слід ретельно розглядати наступні ключові метрики [39]:

1. **RTO** (Recovery time objective, або «цільовий час відновлення») — це часовий проміжок, протягом якого ІТ-інфраструктура залишатиметься

недоступною у разі аварії чи іншого інциденту. Допустиме значення RTO визначається специфікою та потребами бізнес. Фактично це час, протягом якого цифрові послуги компанії можуть простоювати без відчутних наслідків. Чим менше значення RTO, тим дорожче обійдеться послуга Disaster Recovery.

2. **RPO** (Recovery point objective, або «цільова точка відновлення») — це часовий проміжок, дані за який можуть бути втрачені без серйозних наслідків. Наприклад, для RPO, що дорівнює одній годині, резервне копіювання виконується чітко один раз на 60 хвилин. Так само й IT-інфраструктура після відновлення повернеться до того стану, в якому була за годину або менше до аварійного інциденту (на практиці багато залежить від того, коли саме стався збій — через 5, 15, 30 або 55 хвилин після створення копії). Чим меншим є значення RPO, тим частіше виконується резервування IT-інфраструктури й тим дорожче коштує DR-сервіс відновлення.

Визначити оптимальні значення RTO та RPO — означає знайти компроміс між вартістю вирішення післяаварійного відновлення та серйозністю наслідків простою для бізнесу.

Типи аварійного відновлення, які вам буде потрібно, залежать від вашої IT-інфраструктури, типу резервного копіювання та відновлення, яке ви використовуєте, та активів, які вам потрібно захистити. Ось кілька найбільш поширених технологій та методів, які використовуються в аварійному відновленні:

- **Резервне копіювання:** За допомогою резервного копіювання ви копіюєте дані на віддалену систему або відправляєте зовнішній накопичувач на віддалене місце. Однак резервні копії не включають в себе жодної IT-інфраструктури, тому їх не вважають повноцінним рішенням для аварійного відновлення.

- **Резервне копіювання як послуга (BaaS - backup as a service):** аналогічно віддаленим резервним копіюванням, рішення BaaS надає регулярне резервне копіювання даних, яке надає сторонній постачальник.
- **Аварійне відновлення як сервіс (DRaaS - disaster recovery as a service):** Багато хмарних постачальників пропонують DRaaS разом з моделями хмарних послуг, такими як IaaS та PaaS. Модель обслуговування DRaaS дозволяє резервне копіювання ваших даних та IT-інфраструктури та розміщення їх на інфраструктурі хмари стороннього постачальника. Під час кризи постачальник реалізує та оркеструє ваш план відновлення після аварії, щоб допомогти відновити доступ та функціональність з мінімальними перервами в роботі.
- **Снепшоти віртуальних машин (point-in-time snapshots):** Також відомі як копії в певний момент часу, знімки реплікують дані, файли або навіть повну базу даних в певний момент часу. Знімки можна використовувати для відновлення даних, якщо копія зберігається на місці, яке не постраждало від події. Однак втрати даних можуть статися, залежно від часу створення образу [40].

Для даного дослідження я обираю створення стартапу, який надає аварійне відновлення як сервіс (DRaaS) операторам мобільного зв'язку. Аварійне відновлення на основі хмарних технологій - це найбільш ефективний з точки зору вартості та масштабованості варіант. За цією опцією хмарний центр обробляє критичні системи, дані та програми. Аварійне відновлення на основі хмарних технологій дозволяє організації підтримувати готовність цілих віртуальних середовищ, скорочуючи час відновлення після порушення бізнесу чи перебоїв до кількох хвилин або навіть секунд [45].

Основні переваги DRaaS включають:

1. **Уникнення простою:** DRaaS діє як ключовий інструмент, що дозволяє компаніям працювати на запасному сайті під час відновлення основного сайту, значно зменшуючи вплив простою.

2. **Широкі можливості використання:** хоча DRaaS часто пов'язано з природними катастрофами, його також використовують для:

- Відключень енергопостачання на місці
- Відмов апаратного забезпечення та мережі
- Помилки в програмному забезпеченні та системах ІТ
- Відмов власних дата-центрів (не пов'язаних із відключенням електроенергії)
- Кібератак та порушення безпеки

3. **Швидке відновлення:** Швидке відновлення є ключовим для мінімізації витратних періодів простою, збереження фінансової стабільності та репутації, а також забезпечення конкурентоспроможності та відповідності.

4. **Відсутність складнощів:** Зовнішнє забезпечення процесів аварійного відновлення за допомогою постачальника DRaaS усуває необхідність виконання внутрішніх витратних та часомістких оркестрацій аварійного відновлення в рамках вашої організації.

Основними параметрами для аварійного відновлення (DR) є цільовий час відновлення (RTO) та цільова точка відновлення (RPO) [46]. RTO та RPO повинні бути визначені для кожного сервісу, враховуючи будь-які взаємозалежності, які можуть впливати на інші послуги. RTO визначає, наскільки швидко службу потрібно повернути в режим доступності після події аварії, щоб бізнес міг продовжити свою роботу. RPO - це момент у часі, до якого дані повинні бути відновлені, щоб бізнес міг відновити свою діяльність. RPO є мірою того, скільки даних організація може втратити для конкретного сервісу. Метою рішення з аварійного відновлення є забезпечення географічної стійкості та відновлення послуг у випадку подій аварії, які роблять неможливим відновлення послуг на основному сайті.

Викладене у моєму дослідженні рішення базується на тому, що воно повинно бути найбільш економічно ефективним для компанії, якій надається даний сервіс. Потенційно можливо розробити рішення, яке може відповідати

цільовому часу відновлення 0 (нуль) хвилин та цільовій точці відновлення менше 60 хвилин. Однак вартість такого рішення експоненційно зростає зі зближенням цільового часу відновлення до нуля. Такі рішення рідко бувають економічно ефективними, оскільки внаслідок цього піднімається сумарна вартість кінцевого продукту, наданого споживачу, і він стає неконкурентноспроможним.

Для загального рішення з аварійного відновлення використовуються **наступні цільові показники:**

- Максимальна цільова точка відновлення (RPO) становить 5 хвилин.
- Максимальний цільовий час відновлення (RTO) складає 720 хвилин.
- Потреби у потужності для DR сайту ідентичні до продакшн сайту, він повинен підтримувати 100% пікового навантаження продакш сайту.
- DR сайт побудований за надлишковим принципом N+1 (кількість фізичних серверних машин достатня для обробки максимально очікуваного навантаження, з однією серверною машиною для додатків та однією серверною машиною для бази даних, які готові приймати навантаження у випадку відмови активних машин)
- Реплікація даних реалізована через мережеве з'єднання із гарантованою якістю обслуговування (включаючи пропускну здатність та затримку).
- Мережева конфігурація та пропускну здатність між основним та бекапним сайтами достатні для методу реплікації даних [46].

Незважаючи на всю архітектурну та технологічну резервність, вбудовану в рішення, існують потенційні події, які можуть впливати на здатність рішення досягати визначених цілей. Такі сценарії можуть варіюватися від неочікуваних подій до планового технічного обслуговування. Якщо сценарій має вплив на RPO, RTO подовжується на тривалість відновлення після події. Нижче, у таблиці 3.1, наведено аналіз таких факторів.

Таблиця 3.1.

Аналіз впливу проблемних сценаріїв різних аспектів процесу аварійного
відновлення

Проблемні сценарії різних аспектів процесу аварійного відновлення	Вплив	Відновлення
Проблеми з мережевим з'єднанням між основною та DR платформами.	Наслідки для RPO можуть бути від незначних до максимальних, залежно від тривалості проблем з'єднання.	Від 1-2 годин до кількох днів.
Розгортання нових релізів застосунків на основній платформі.	Невеликий вплив на RPO. Під час деплоїв додатки призупиняються, а мережа не генерує нові дані. Вплив обмежується часом, коли послуги працюють і перевірені, але реплікація ще не відновлена.	Оцінка часу відновлення становить 1-2 години, оскільки релізи програмного забезпечення розгортаються під час непікових годин.
Відновлення бази даних з резервного копіювання на основній платформі.	Максимальний вплив на RPO.	Копія нової бази даних повинна бути доставлена на платформу DR та відновлена.
Відмова фізичного сервера бази даних на платформі аварійного відновлення.	Середній вплив на цільову точку відновлення (RPO) – недоступно не більше 1-3 годин даних на платформі аварійного відновлення.	Після переміщення бази даних на резервний сервер відсутні дані відновлюються за допомогою журналів відновлення або інкрементальних резервних копій бази даних, і відновлення реплікації продовжується.
Технічне обслуговування сервера баз даних на платформі аварійного відновлення.	Невеликий вплив на RPO – приблизно 1 година.	Після перемикання бази даних на резервний сервер реплікація відновлюється.

3.2. Створення стартапу для надання аварійного відновлення як сервіс (DRaaS) операторам мобільного зв'язку

Катастрофа - це будь-яка подія, коли велика кількість одночасних збоїв призводить до переривання безперервного обслуговування. Основною проблемою в галузі ІТ під час катастрофи є стан даних та доступність ресурсів ІТ-інфраструктури для продовження надання послуг [42]. Якщо неможливо відновити послуги на основному сайті через фізичні обмеження або серйозні пошкодження даних, то перезапуск послуги на віддаленому сайті є найкращим варіантом для вчасного відновлення критичних послуг.

Рішення про ініціацію перемикання після відмови вимагає людської оцінки всіх факторів, багато з яких неможливо виміряти або кількісно визначити за допомогою комп'ютера. Таким чином, переміщення послуг на DR (резервний відновлювальний) сайт повинно бути ручним процесом, який включає спільне рішення всіх відповідних бізнес-підрозділів та керівництва.

Перемикання - це процес переміщення послуг на сайт резервного відновлення. Сайт резервного відновлення повинен бути завжди готовий і мати конфігурацію ІТ-інфраструктури та дані, які відповідають вимогам резервного відновлення. Коли приймається рішення про перемикання, всі послуги переносяться на резервний сайт.

Процедура відновлення після відмови схожа на процедуру перемикання, але змінює цільове та вихідне розташування. Основним вимогам для відновлення після відмови є відновлення основного сайту до початкового стану. Коли будуть відомі подробиці катастрофи, будуть визначені та затверджені особливості процедури. Оскільки перемикання - це запланована подія, на неї не поширюються певні параметри, пов'язані із SLA (рівень обслуговування) [45]. Відновлення може бути виконано без втрати даних під час не пікового моменту використання сервісу.

Компанія пропонує чотири типи рішень для відновлення після аварії. Один із них є рекомендованим типовим рішенням, яке детально описано в

цьому документі. Інші надаються або для відповідності конкретним нормативним вимогам мобільного оператора, або як більш вигідні варіанти для ліцензіатів. У таблиці 3.2 нижче проаналізуємо різні сценарії реалізації платформи аварійного відновлення.

Таблиця 3.2.

Порівняння сценаріїв реалізації платформи аварійного відновлення

Архітектурне рішення сайту аварійного відновлення	Резервне копіювання лише даних	Реплікація даних	Повноцінна платформа аварійного відновлення	Платформа повного аварійного відновлення з асинхронною реплікацією
RTO	8+ тижнів	4-8 тижнів	720 хвилин	360 хвилин
RPO	24+ годин	30 хвилин	5 хвилин	5 хвилин
Технологічний опис впровадження рішення	Лише резервні стрічки з даними, з ротацією носіїв і безпечним зберіганням за межами основної платформи. Активація вимагає повного нового налаштування платформи з нуля.	Машини для баз даних та сховищ віддалено в іншому фізичному місці, з реплікацією даних з основного майданчика. Віддалений майданчик не підтримує звичайну діяльність - його можна використовувати лише для доступу до даних в очікуванні повного нового налаштування майданчика.	Рекомендоване рішення за замовчуванням. Дані реплікуються через Інтернет-з'єднання.	Те ж саме, що і рішення за замовчуванням, але дані реплікуються за допомогою високопропускних фізичних оптоволоконних кабелів між основними і резервними платформами. Це веде за собою значні додаткові капітальні та оперативні витрати. Платформи повинні бути на відстані не більше 20 км одна від одної.

Сайт для відновлення після аварії розгортається за такою ж самою архітектурою, як і основний. Це робиться для уникнення проблем сумісності. DR-сайт компанії побудований на основі принципу N+1 забезпеченості. Кількість фізичних серверних машин досить для обробки максимально

очікуваного навантаження, з однією серверною машині для додатків і однією серверною машиною для баз даних, які зберігаються в резерві, готові взяти на себе обов'язки в разі відмови будь-яких активних машин [40]. Це менше, ніж рівень подвійної забезпеченості 2N на головному сайті (поточний галузевий стандарт для забезпечення безперебійності надання сервісу), де для кожного сервера доступні дві фізичні машини в разі відмови однієї, але цього достатньо для потреб відновлення після катастрофи.

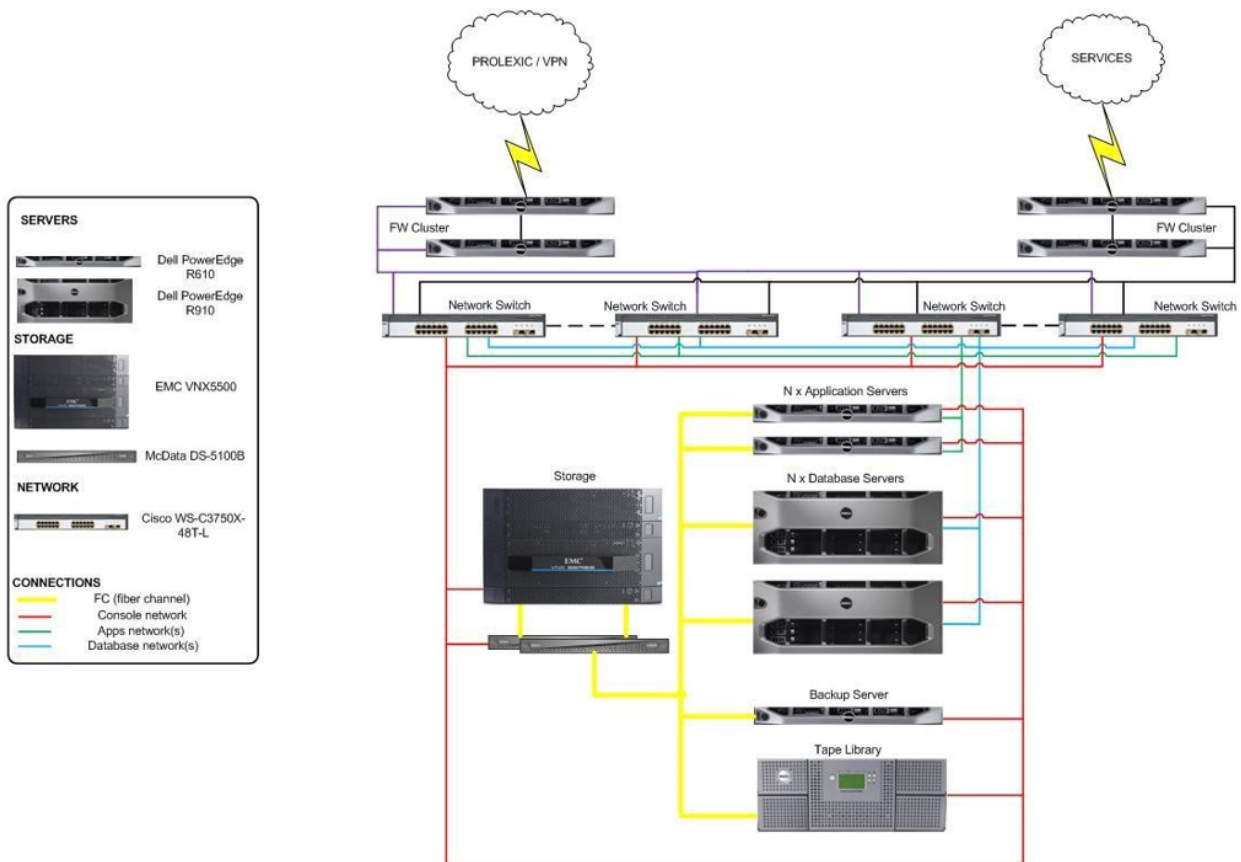


Рис. 3.1. Приклад використовуваного фізичного обладнання для побудови датацентру для побудови хмарного рішення аварійного відновлення.

DR-сайт забезпечує достатню потужність для підтримки 100% пікового навантаження головного сайту [38]. Він здатен повністю взяти на себе обов'язки головного сайту, але на цьому етапі не має забезпеченості надійності для покриття надлишкового трафіку.

Мережу ліцензіата (оператора мобільного зв'язку) захищають подвійні брандмауери, які працюють на відведеному обладнанні. Весь зовнішній трафік і весь трафік, що переходить між сегментами додатків, баз даних і адміністрації внутрішньої мережі, повинен проходити через брандмауер.

Балансувальники навантаження використовуються, якщо мережа ліцензіата передбачає їх використання.

Кожна точка з'єднання між сегментами внутрішньої мережі, а також зовнішня підключеність обслуговуються подвійними комутаторами промислового класу.

DR-сайт використовує ідентичну конфігурацію зберігання даних, як і головний сайт.

На DR-сайті буде дві серверні машини баз даних, одна з них буде діяти як запасна. В звичайних умовах база даних на DR-сайті буде неактивною і буде приймати лише потік повторної реплікації, який відображається Oracle Data Guard [49]. БД не буде слухати жодних інших з'єднань.

Сервери додатків будуть використовувати ту ж платформу (SPARC або x86), що і на головному сайті. Усі сервери будуть налаштовані та встановлені з відповідною ОС (VMware ESXi) і зонами/віртуальними машинами. Одна машина буде зберігатися як запасна.

Для досягнення високої якості надання сервісу DR-сайт повинен постійно моніторитись. Можливості моніторингу обмежені, коли сайт неактивний - основний акцент в моніторингу зосереджений на IT-інфраструктурі для виявлення будь-яких відмов апаратного забезпечення або нестачі ресурсів, які можуть покласти під загрозу доступність DR-сайту. Крім звичайного моніторингу, буде створено окреме рішення для моніторингу з метою перевірки стану даних, які реплікувалися з основного сайту на DR-сайт [37].

Наступні аспекти роботи DR-сайту мають найвищий пріоритет і моніторяться найближче:

- Реплікація даних з основного сайту повинна працювати бездоганно цілодобово. Тому моніториться стан реплікації і затримка даних.

- Моніториться обсяг трафіку, зайнятого вхідними журналами переробки. Якщо він перевищує заданий поріг, приймаються відповідні заходи.
- Моніториться використання обсягу бази даних, щоб запобігти помилкам, спричиненим нестачею місця.
- Якщо встановлюються нові версії програмного забезпечення, моніториться обсяг журналів переробки для визначення впливу.
- Моніториться доступність зовнішнього підключення DR-сайту.

Після перемикання, DR-сайт автоматично вважається повністю функціональним виробничим сайтом і підлягає стандартним вимогам компанії щодо моніторингу [36]. Моніторингом повинні бути охоплені наступні питання з метою відповідності вимогам DR-сайту та забезпечення його можливостей (таблиця 3.3).

Таблиця 3.3

Аналіз найбільш критичних показників для моніторингу DR-сайту.

Проблема	Опис	Очікувана серйозність впливу продбеми	Заходи щодо усунення
Ємність DR-сайту	Головний сайт може підтримувати більшу кількість трафіку, ніж DR-сайт.	Висока	DR-сайт буде зберігати місткість, еквівалентну основному сайту - забезпечено процесом управління місткістю шляхом періодичної ревізії.
Реплікація даних вимагає занадто багато ресурсів.	Обсяг даних для реплікації перевищує доступну пропускну здатність між сайтами.	Висока	Буде проводитися постійний моніторинг мережі.

Нестабільна мережа.	Зв'язок між основним і DR-сайтами не є достатньо стійким для безперервної реплікації даних.	Середня	Перед впровадженням рішення необхідно провести тестування мережевого навантаження. Після впровадження рішення буде встановлено постійний моніторинг.
---------------------	---	---------	--

Для відповідності вимогам до доступності компанія використовує рішення Oracle Physical Standby та Oracle Data Guard для реплікації даних. DR-база даних зазвичай працює в режимі очікування та приймає лише журнали переробки (redo logs) від основної бази даних.

Реплікація даних є асинхронною та поточною. Журнали переробки надсилаються на DR-сайт безперервно. Після запису журналів переробки на диску на основному сайті, основна база даних продовжує працювати, не чекаючи підтвердження від DR-бази даних про їхнє отримання [35]. Журнали переробки застосовуються до DR-бази даних, як тільки вони стають доступними. У разі виникнення проблем з мережею або підключенням журнали переробки застосовуються після відновлення підключення до DR-бази даних.

Це рішення визначається Oracle Data Guard як режим максимальної продуктивності, оскільки воно надає мінімальний RPO (втрата даних) та високу доступність одночасно [49]. RPO значно залежить від пропускної здатності та стійкості мережевого з'єднання, а також від обсягу журналів переробки. Якщо пропускна здатність мережі від основного сайту до DR-сайту обмежена, RPO та RTO будуть збільшені.

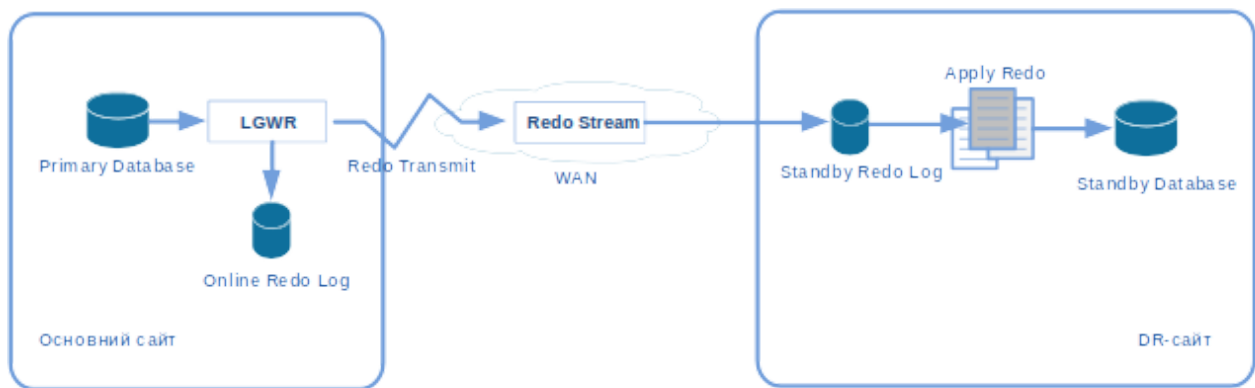


Рис. 3.2. Приклад використання технології Oracle Data Guard для забезпечення реплікації між основним та DR сайтом.

Під час активації DR-сайту, Oracle DBA будуть вживати відповідних заходів, щоб підготувати базу даних Oracle до підтримки операцій [49]. Це включає в себе зупинку реплікації, зупинку застосування журналів переробки та активацію бази даних. Функціональність та цілісність активованої бази даних перевіряються, перш ніж на неї будуть спрямовані сервери додатків.

Активація бази даних Oracle повинна включати в себе активацію всіх заходів підтримки та обслуговування, таких як снєпшоти, резервні копії, CRON-завдання і т.д.

Під час розгортання нових релізів застосунку на стороні оператора мобільного зв'язку реплікація між основним і DR-сайтом зупиняється, створюється снєпшот основної БД. Тільки після цього нова версія релізу застосовується до основної БД і до серверів додатків як на основному, так і на DR-сайті. Після цього основний сайт активується, і проводиться необхідне тестування. Якщо у релізі не виникає проблем (зокрема на рівні БД), реплікація між основним і DR-сайтом відновлюється.

Якщо реплікація даних постраждає через проблеми з мережевим з'єднанням, або потрібне відновлення з резервного сайту на основний сайт, то відновлення реплікації залежить від тривалості перерви або переривання у передачі даних:

1. Перерви тривалістю від 1 до 2 годин вирішуються за допомогою Oracle Data Guard за допомогою журналів переробки (не застосовується до відновлення на основний сайт). Передбачається, що бази даних будуть синхронізовані протягом періоду від 1-2 годин до 12 годин.
2. Перерви тривалістю понад кілька годин, і до одного тижня, вирішуються за допомогою спеціальних ручних дій, використовуючи комбінацію функціональності відновлення Oracle RMAN (інкрементальні копії бази даних) та журналів обробки [49]. Це також використовується для відновлення на основний сайт, за умови, що база даних основного сайту залишалася непошкодженою після катастрофи. Бази даних будуть синхронізовані знову протягом 1-2 днів після відновлення зв'язку.
3. Перерви тривалістю більше одного тижня розглядаються індивідуально. У разі можливості застосовується варіант 2 відновлення. Якщо обсяг втрачених даних занадто великий і вимагав би занадто багато часу на копіювання, то резервні стрічки відправляються на сайт відновлення, а журнали переробки доставляються, як завжди. (У випадку відновлення на основний сайт стрічки/журнали доставляються на основний сайт.) Бази даних будуть синхронізовані протягом 2-3 днів після доставки стрічок.

Oracle Data Guard надає комплексний спосіб збереження резервних баз даних для подолання катастроф і пошкодження даних [49]. Він підтримує ці резервні бази даних як копії виробничої бази даних. Потім, якщо виробнича база даних стає недоступною, Data Guard надає можливість переключити резервну базу даних на роль основної. Data Guard є ідеальним рішенням для географічно розподілених систем, де виробнича база даних розташована на активному сайті, а резервна база даних - на альтернативному сайті.

3.3. Забезпечення переключення кінцевих користувачів між основною та DR платформами

Функціональне DR-рішення потребує механізму, який перенаправляє запити клієнта на вторинний сайт після завершення відновлення після катастрофи. Механізми перенаправлення базуються на системі доменних імен (DNS). У такому розгортанні обидва центри обробки даних базуються на незалежних і окремих IP-адресних просторах для послуг.

Компанія використовує UltraDNS-сервіси для управління DNS. Компанія має необхідні права доступу для створення/видалення/зміни записів DNS з панелі управління UltraDNS. Під час виконання failover створюються нові DNS-записи з IP-адресами послуг DR-сайту. Старі DNS-записи експортуються і зберігаються. Для сайту з DR-рішенням TTL (час життя записів DNS) повинен бути не більше $\frac{1}{2}$ RTO [19]. Якщо RTO відрізняється від того, що зазначено в цьому документі, TTL потребує повторної оцінки і встановлюється відповідно до документації DR для конкретного сайту. Якщо сайт використовує балансувальники навантаження, то записи DNS та конфігурації клієнтів відрізняються від сайтів, які їх не використовують. Тому, якщо на основному сайті налаштований балансувальник навантаження, то і на DR-сайті також повинен бути встановлений балансувальник навантаження [46].

На рис 3.3 зображено приклад операційної інфраструктури мобільного оператора, основний сайт (primary site) підкріплений сайтом аварійного відновлення (DR site).

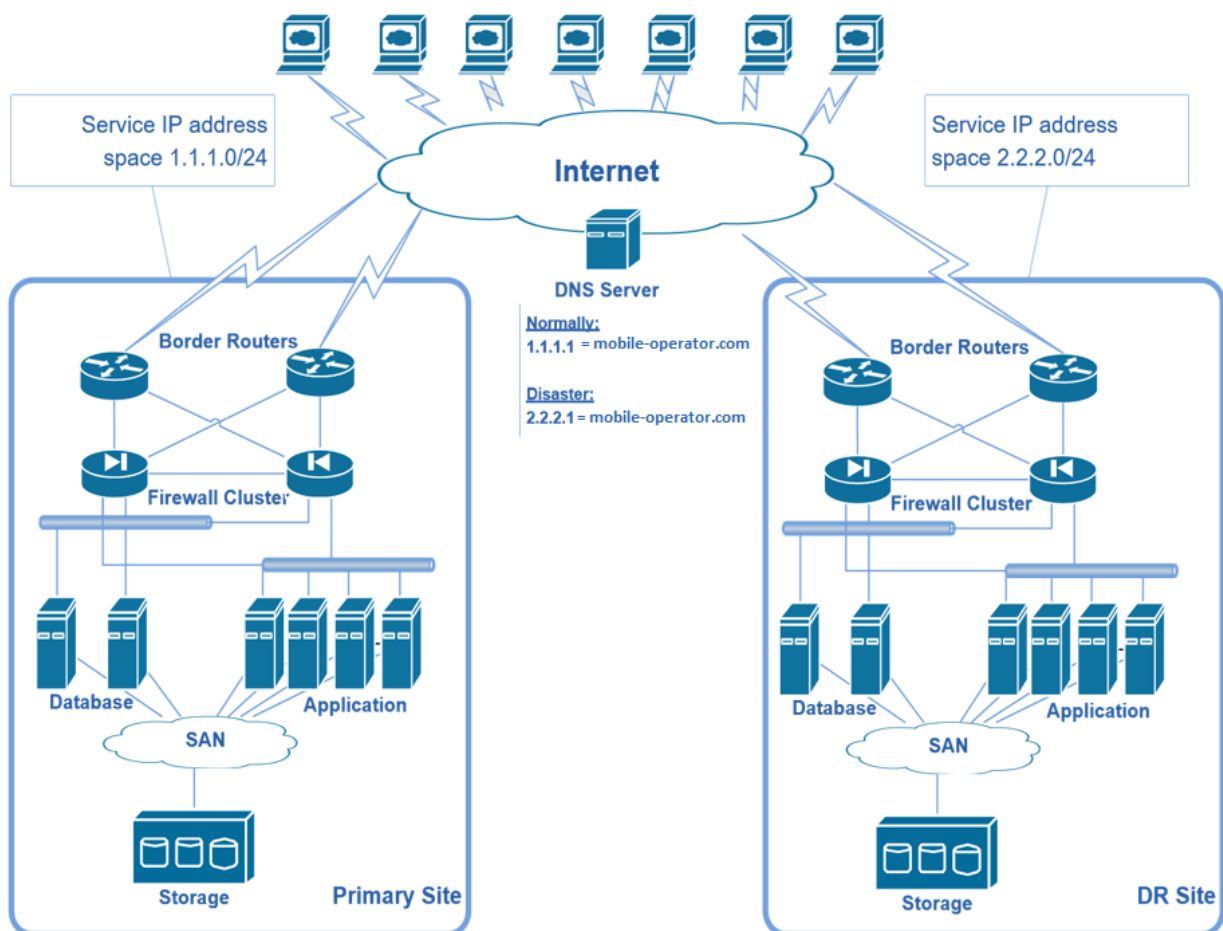


Рис. 3.3. Приклад операційної інфраструктури мобільного оператора, де переключення трафіку здійснюється шляхом зміни DNS-записів основних сервісів.

Зміни в DNS-записах виконуються відповідним DevOps спеціалістом за допомогою коду, написаного у Terraform. Це дозволяє виконувати зміни в DNS швидко і мінімізує кількість можливих помилок при введенні. На рис. 3.4 наведено приклад такого коду [31].

```
resource "ultradns_record" "A" {
  zone_name = "mobile-operator.com."
  owner_name = "A"
  record_type = "A"
  ttl = 120
  record_data = ["194.58.197.4"]
}
```

Рис. 3.4. Приклад коду terraform, який дозволяє перемикати DNS-А записи для зміни відповідності IP-адреси і доменних імен.

У відповідності до розробленої процедури перемикання на аварійний сайт (Failover Procedure) необхідно буде здійснити наступні кроки при настанні аварійної ситуації [39]:

1. Заблокувати доступ до послуг основного сайту і, якщо можливо, припинити послуги.
2. Зупинити реплікацію даних між основним і DR-сайтом після перевірки, що всі дані були репліковані.
3. Застосувати зміни DNS на рівні постачальника послуг DNS.
4. Перевірити журнали бази даних, доступні на сайті відновлення, і застосувати відсутні журнали обробки.
5. Активувати DR-базу даних для читання/запису.
6. Сповістити точний RPO (втрата даних) зацікавленим сторонам.
7. Переконфігурувати додатки в базі даних, використовуючи SQL-команди з параметрами, специфічними для сайту.
8. Запустити всі компоненти додатків компанії.
9. Видалити блоки на рівні брандмауера в два етапи.
 - 9.1. Спершу видалити внутрішні правила брандмауера.
 - 9.2. Після перевірки, що внутрішні правила працюють, видалити блоки правил зовнішніх послуг.
10. Перевірити доступність послуг відповідно до процедур тестування.

Після фейоверу (failover - перемикання на аварійний сайт) до дій після відновлення включається запуск резервних копій на диску та стрічці.

Після відновлення основного сайту до його початкового стану і встановлення всіх необхідних компонентів (таких як база даних і програмні додатки), ініціюється процедура відновлення (failback) [41]. Рішення про ініціацію відновлення приймається ліцензіатом (оператором мобільного зв'язку). Процедура відновлення відбувається як запланована зміна і

координується відповідно. Підготовка до процедури відновлення включає в себе:

1. Придбання, встановлення та налаштування ІТ-інфраструктури (якщо основна інфраструктури була знищена під час аварії).
2. Встановлення баз даних та компонентів додатків (якщо була необхідність у виконання першого кроку).
3. Основна база даних активується у режимі очікування.
4. Активується реплікація між DR-сайтом і основним сайтом (реплікація даних з DR-сайту на основний сайт).
5. Перевіряється синхронізація основної бази даних з базою даних DR-сайту.
6. Ліцензіат приймає рішення та встановлює час для відновлення.
7. Всі відповідні сторони інформуються про заплановану процедуру відновлення, отримують необхідні схвалення для повернення послуг на основний сайт.

Процедура відновлення ґрунтується на процедурі перемикання на аварійний сайт, за винятком відсутності втрати даних. Після успішного відновлення процедури відновлення DR-сайт повертається до свого початкового стану.

Висновки

Disaster Recovery (DR) - це набір інструментів і програмного забезпечення, спрямованих на швидке відновлення ІТ-інфраструктури та даних після різних аварійних ситуацій. Аварійні ситуації можуть бути різного характеру, включаючи природні катастрофи, кібератаки, технічні витоки та інші події, які можуть призвести до втрати даних та збою в роботі бізнес-систем.

Планування та стратегії відновлення після аварії повинні включати визначення RTO (цільового часу відновлення) і RPO (цільової точки відновлення), які допомагають визначити максимально прийнятний час

простою і максимально прийнятну втрату даних для бізнесу. Визначення цих цільових параметрів аварійного відновлення є важливим завданням, і вони повинні бути налаштовані для кожного сервісу окремо. В залежності від обраних значень RTO та RPO вартість утримання DR-платформи може сильно відрізнятись.

Технології та методи аварійного відновлення можуть включати резервне копіювання, резервне копіювання як послугу (BaaS), аварійне відновлення як сервіс (DRaaS), снєпшоти віртуальних машин та інші підходи.

Вибір конкретного методу аварійного відновлення залежить від потреб вашої організації, розміру бюджету та специфіки інфраструктури, а також вимог до часу відновлення та втрати даних. Забезпечення надійного та ефективного DR-плану є важливим завданням для будь-якої організації, що бажає забезпечити бізнес-неперервність та захистити свої активи в разі надзвичайних ситуацій.

Обране рішення стосовно створення стартапу, який надає аварійне відновлення як сервіс (DRaaS) операторам мобільного зв'язку, базується на використанні хмарних технологій. Зовнішнє забезпечення процесів аварійного відновлення через постачальника DRaaS допомагає уникнути складнощів та витрат внутрішніх організаційних оркестрацій.

Цей підхід є ефективним з точки зору вартості та масштабованості. DRaaS дозволяє компаніям уникати простою, працюючи на запасному сайті під час відновлення основного сайту, що значно зменшує вплив простою на бізнес.

При розгляді загального рішення з аварійного відновлення важливо враховувати фінансові аспекти та збалансовувати вартість і швидкість відновлення для досягнення оптимальних результатів. Плановані та неочікувані сценарії можуть впливати на здатність рішення досягати визначених цілей RTO та RPO, тому важливо бути готовим до різних ситуацій та мати стратегію для їх управління.

Обране рішення має потенціал стати ефективним способом надання послуг DRaaS операторам мобільного зв'язку, забезпечуючи їх

бізнес-неперервність та захист від надзвичайних ситуацій. У висновках можна підкреслити наступні ключові аспекти щодо створення та функціонування DR-сайту (сайту для відновлення після аварії):

1. Архітектура сайту: DR-сайт повністю співпадає за архітектурою з основним сайтом. Це робиться для забезпечення максимальної сумісності та уникнення проблем.

2. Принцип N+1: DR-сайт побудований на основі принципу N+1 забезпеченості, що передбачає наявність додаткових фізичних серверних машин для обробки навантаження та готовності взяти на себе обов'язки в разі відмови активних серверів.

3. Пікове навантаження: DR-сайт здатний підтримувати 100% пікового навантаження головного сайту, що є критичним для забезпечення безперебійності послуг.

4. Мережева безпека: мережу оператора мобільного зв'язку захищають брандмауери, а весь трафік оброблюється через них.

5. Балансування навантаження: використовується балансування навантаження, де це необхідно, для оптимізації роботи мережі.

6. Подвійні комутатори: кожна точка з'єднання внутрішньої мережі та зовнішня підключеність обслуговуються подвійними комутаторами промислового класу для забезпечення надійності.

7. Зберігання даних: DR-сайт використовує ідентичну конфігурацію зберігання даних, як і головний сайт, з урахуванням резервності.

8. Моніторинг та контроль: DR-сайт постійно моніториться для виявлення будь-яких відмов апаратного забезпечення чи нестачі ресурсів. Реплікація даних, доступність, та інші аспекти піддаються ретельному моніторингу.

Ключовими технологіями, які використовуються для сетапу DR-сайту, є:

- VMware ESXi: для забезпечення середовища із віртуалізації.
- Oracle Physical Standby та Oracle Data Guard використовуються для забезпечення реплікації баз даних між основним та резервним сайтами.

- UltraDNS-сервіси: управління DNS записами та можливість перемикаєти IP адреси на DR-середовище.

Загальний висновок полягає в тому, що DR-сайт ретельно налаштований та готовий взяти на себе обов'язки в разі аварії на головному сайті, забезпечуючи надійність і неперервність надання сервісу.

РОЗДІЛ 4

РОЗРОБКА СТАРТАП ПРОЕКТУ

4.1. Опис ідеї проекту

Для даного дослідження я обираю створення стартапу, який надає аварійне відновлення як сервіс (DRaaS) операторам мобільного зв'язку. Аварійне відновлення на основі хмарних технологій - це найбільш ефективний з точки зору вартості та масштабованості варіант. За цією опцією хмарний центр обробляє критичні системи, дані та програми. Аварійне відновлення на основі хмарних технологій дозволяє організації підтримувати готовність цілих віртуальних середовищ, скорочуючи час відновлення після порушення бізнесу чи перебоїв до кількох хвилин або навіть секунд.

Таблиця 4.1.

Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Аварійне відновлення як сервіс (DRaaS) операторам мобільного зв'язку	Безпроводні телекомунікаційні системи операторів мобільного зв'язку	Скорочення часу відновлення працездатності сервісів мобільних операторів після перебоїв

Аварійне відновлення на основі хмарних технологій дозволяє організації підтримувати готовність цілих віртуальних середовищ, скорочуючи час відновлення після порушення бізнесу чи перебоїв до кількох годин, або навіть хвилин.

Соціальний ефект від впровадження проекту полягає в покращенні та підвищенні стабільності роботи телекомунікаційних мереж, що є базовою потребою сучасного суспільства.

4.2. Технологічний аудит ідеї проекту

Ключовими технологіями, які використовуються для реалізації проекту, будуть:

1. VMware ESXi для віртуалізації:

- Ефективне використання ресурсів: VMware ESXi дозволяє віртуалізувати фізичні сервери, що призводить до кращого використання обчислювальних ресурсів та зменшення кількості фізичних серверів.
- Швидке відновлення: Можливість швидкого резервного копіювання та відновлення віртуальних машин сприяє зниженню часу відмови в разі аварій або інших проблем.

2. Oracle Physical Standby та Oracle Data Guard для реплікації баз даних:

- Висока доступність: Використання Oracle Data Guard дозволяє миттєво переключатися на резервний сервер у випадку відмови або неполадок на основному сервері.
- Захист від втрати даних: Регулярна реплікація даних на резервний сервер забезпечує їх захист та уникнення втрат при можливих інцидентах.

3. UltraDNS-сервіси для управління DNS:

- Швидка переключення IP: UltraDNS дозволяє легко та швидко перенаправляти DNS-запити на DR-середовище, забезпечуючи мінімальний час переходу при відновленні роботи.
- Гнучкість та надійність: Можливість зміни IP-адрес для резервного середовища під час аварій чи тестувань забезпечує гнучкість та надійність в управлінні трафіком.

Використання цих технологій в проекті дозволяє не лише забезпечити високу доступність та надійність системи, але і оптимізувати управління ресурсами та витратами під час відновлення після непередбачуваних ситуацій. DR-сайт налаштований та готовий взяти на себе обов'язки в разі аварії на головному сайті, забезпечуючи надійність і неперервність надання сервісу.

4.3. Аналіз ринкових можливостей запуску стартап-проекту

При дослідженні ринкових можливостей, в першу чергу проведений аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку. Дані наведені у таблиці нижче.

Таблиця 4.2.

Попередня характеристика потенційного ринку стартап-проекту.

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	7
2	Загальний обсяг продаж, грн/ум.од	Немає актуальних розрахунків для ринку входження (України).
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Висока вартість обладнання для облаштування датацентру DRaaS.
5	Специфічні вимоги до стандартизації та сертифікації	Немає
6	Середня норма рентабельності в галузі (або по ринку), %	32

Враховуючи загальну динаміку інтеграції нових стандартів зв'язку, розвитку ринку телекомунікацій т, водночас зі значними економічними проблемами як для телекомунікаційних операторів зв'язку, так і для країни загалом, існує попит на програмні рішення, які здатні знизити вартість утримування та обслуговування мереж, та водночас збільшити їх стійкість до збоїв та пришвидшити знаходження і ліквідацію причин цих збоїв. Розроблена система є саме такою і здатна закрити цю потребу. Тому, за попереднім оцінюванням ринок є привабливим для входження, і стартап-проект може мати

успіх.

Таблиця 4.3.

Характеристика потенційних клієнтів стартап-проекту.

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Аварійне відновлення для мобільних операторів	Мобільні оператори, провайдери телекомунікаційних послуг	Різні оператори можуть мати різні технічні вимоги та обсяги даних, а також різний рівень критичності для відновлення.	Висока надійність, швидкість відновлення, масштабованість.
2	Забезпечення надійності і безпеки мережі	ІТ-відділи та технічні спеціалісти мобільних операторів	Технічні спеціалісти можуть бути більш критичними до технічних аспектів, тоді як менеджери можуть зосередитися на вартості та результативності.	Висока безпека, надійність, можливість моніторингу та керування.
3	Мінімізація часу відновлення	Топ-керівництво та власники мобільних операторів	Керівництво може цінувати швидкий та ефективний процес відновлення для забезпечення найменших втрат.	Мінімізація часу відновлення, надійність, вартість.

У таблиці 4.4 представлені потенційні загрози, які можуть мати вплив на подальший розвиток стартап-проекту.

Таблиця 4.4

Фактори загроз

№ п/п	Фактор загрози	Зміст загрози	Можлива реакція компанії
----------	----------------	---------------	--------------------------

Продовження таблиці 4.4

1	Зміни на ринку	Зміни в попиті або конкурентному середовищі, що можуть вплинути на замовлення.	Реагувати на ринкові зміни шляхом адаптації продукту або пошуку нових ринків.
2	Фінансові обмеження	Обмеження бюджету клієнта або недостатність фінансових ресурсів для придбання послуг.	Пропонувати гнучкі фінансові умови або знижки для залучення клієнта.
3	Конфіденційність даних	Спроби несанкціонованого доступу до конфіденційних даних клієнта.	Забезпечувати високий рівень кібербезпеки та дотримання стандартів безпеки.
4	Технічні проблеми	Несправність або відмови в системі, які можуть спричинити втрату даних або доступ до них.	Надавати надійні технічні рішення та 24/7 підтримку для відновлення послуг.
5	Конкуренція	Зростаюча конкуренція в галузі, що може призвести до зниження цін або втрати клієнтів.	Змагатися на ринку шляхом розвитку унікальних функцій або покращення якості обслуговування.

Фактори можливостей - це зовнішні або внутрішні обставини та умови, які створюють сприятливий ґрунт для успішної реалізації певного проекту або бізнес-ідеї. Вони можуть включати в себе такі фактори, як попит на продукт або послугу, наявність потрібних ресурсів, нові технології, зміни в законодавстві, конкурентну перевагу та інші чинники, які можуть позитивно вплинути на виконання проекту та досягнення його цілей. Фактори можливостей вказують на можливості та переваги, які можуть бути використані для успішного впровадження проекту на ринку. Таблиця 4.5 "Фактори можливостей" описує ті чинники, які сприяють успішному впровадженню проекту на ринку.

Таблиця 4.5

Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Зростаючий попит	Зацікавленість ринку у продукті чи послугі, що пропонується	Збільшення виробництва, рекламна кампанія, розширення ринків
2	Нові технології	Використання передових технологій у виробництві чи послугах	Інвестиції у дослідження та розвиток, модернізація процесів
3	Зміни в законодавстві	Зміни в законодавстві, що сприяють бізнес-процесам	Адаптація до нових правил, юридична консультація
4	Конкурентні переваги	Унікальність продукту, яка дозволяє виділитися серед конкурентів	Підсилення маркетингових зусиль, захист інтелектуальної власності
5	Зростання ринку	Збільшення розміру ринку та кількості клієнтів	Розширення виробництва та мережі збуту

Ступеневий аналіз конкуренції на ринку - це процес оцінки та класифікації рівня конкуренції, який існує на ринку для даного продукту чи послуги. Цей аналіз дозволяє визначити, наскільки насичений ринок конкурентами і які основні характеристики конкурентного середовища впливають на можливості успіху проекту. У таблиці 4.6 наведено результати такого аналізу.

Таблиця 4.6

Ступеневий аналіз конкуренції на ринку

№ п/п	Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
1	Вказати тип конкуренції – досконала	В даній галузі спостерігається досконала конкуренція, де компанії в	Компанія має можливість встановлювати ціни на власні продукти та послуги згідно зі

Продовження таблиці 4.6

		встановлюють ціни на свої послуги самостійно.	своїми власними стратегіями.
2	За рівнем конкурентної боротьби - міжнародний	Ринок таких застосунків має міжнародний характер, оскільки кожна країна має своїх постачальників телекомунікаційних послуг.	Створюється необхідність адаптувати послуги до різних країн та їх особливостей, враховуючи різницю в підходах та потребах.
3	За галузевою ознакою - внутрішньогалузева	Конкуренція в даній галузі обмежена ринком систем для розрахунку платежів, що надає можливості для оптимізації та покращення.	Компанія може активно працювати над вдосконаленням нашого продукту з огляду на конкретні потреби цієї галузі та споживачів.
4	Конкуренція за видами товарів: - товарно-родова	Системи розрахунку рахунків, представлені на ринку, створюються для різних компаній та можуть відрізнятися функціональністю.	Потрібно розширювати функціональність і продукту, щоб задовольняти потреби різних корпоративних клієнтів та покупців.
5	За характером конкурентних переваг - нецінова	Компанія акцентує на нецінових конкурентних перевагах, таких як інновації та використання передових технологій.	Збереження креативного та наукового підходу в розробці послуг для забезпечення наявності конкурентних переваг на ринку.
6	Репутація бренду	В даному сегменті ринку брендинг не відіграє вирішальної ролі, і основний акцент робиться на якості продукту.	Зосередження на підвищенні якості послуг та продуктів, гарантуючи надійність та ефективність для клієнтів.

За допомогою моделі М. Портера проводиться більш детальний аналіз конкуренції в галузі, враховуючи п'ять основних факторів, які впливають на привабливість ринку з точки зору конкурентної ситуації. Ця модель дозволяє оцінити, наскільки сильні позиції має компанія в кожному з цих факторів, що вказує на її можливості забезпечити успішний оборот капіталу та впливати на інших гравців на ринку.

Аналіз за моделлю М. Портера допомагає визначити ступінь конкуренції з боку прямих конкурентів, визначити можливості та строки для входу на ринок, ідентифікувати потенційних конкурентів, а також розглянути вплив клієнтів і постачальників на умови роботи на ринку та можливі обмеження, пов'язані з замінними товарами.

Таблиця 4.7

Аналіз конкуренції у галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товарозамінники
	У галузі DRaaS для операторів мобільного зв'язку можуть існувати такі прямі конкуренти, як великі технологічні компанії (наприклад, Amazon Web Services, Microsoft Azure), які також надають послуги аварійного відновлення.	За ростом і популярністю ринку DRaaS можуть з'явитися нові гравці, такі як стартапи, які принесуть нові технології та підходи до аварійного відновлення. Також можливість входу великих технологічних корпорацій у цю галузь.	Для стартапу, що надає DRaaS, ключовими постачальниками можуть бути постачальники хмарних ресурсів, які надають інфраструктуру для аварійного відновлення. Також постачальники програмного забезпечення для аварійного відновлення можуть бути важливими партнерами	Оператори мобільного зв'язку є головними клієнтами для цього стартапу. Їх вимоги та потреби в аварійному відновленні будуть визначати попит на послуги DRaaS. Іншими потенційними клієнтами можуть бути компанії з інших галузей, які також шукають надійні рішення для аварійного відновлення	Товарозамінниками для DRaaS можуть бути інші методи та технології аварійного відновлення, такі як внутрішні рішення, які розробляють компанії самостійно без залучення сторонніх провайдерів DRaaS. Також існують альтернативні послуги з аварійного відновлення, які можуть конкурувати з DRaaS, наприклад, традиційні резервні копії даних.

Загалом, успішний стартап повинен ретельно розглядати фактори конкурентноспроможності наведені у таблиці 4.8 і розробляти стратегію, яка враховує їх важливість для а ринку.

Таблиця 4.8

Ступеневий аналіз конкуренції на ринку

№ п/п	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1	Технологічна інноваційність	Висока технологічна інноваційність може дозволити впроваджувати передові рішення та привертати клієнтів своєю інноваційністю.
2	Вартість послуг	Конкурентоспроможність стартапу може бути обумовлена конкурентноздатністю цінової політики та можливістю пропонувати доступні та конкурентноздатні ціни.
3	Якість обслуговування	Висока якість обслуговування може визначати здатність задовольняти потреби клієнтів та забезпечувати їхнє задоволення від користування послугами.
4	Географічна доступність	Розташування та доступність для клієнтів можуть бути ключовими факторами для конкурентоспроможності, залежно від регіональних особливостей.
5	Маркетингові стратегії	Ефективні маркетингові стратегії, такі як реклама та просування, привертатимуть більше клієнтів і змагатися на ринку.
6	Управлінський досвід	Досвідна та компетентна команда керівників може забезпечити ефективне управління та прийняття правильних стратегічних рішень для підвищення конкурентоспроможності.

Ступеневий аналіз конкуренції на ринку - це метод дослідження та оцінки рівня конкуренції в галузі або на ринку, який включає в себе вивчення та порівняння різних аспектів діяльності конкуруючих компаній. Цей аналіз наведений у таблиці 4.9, спрямований на визначення сильних та слабких сторін конкурентів, їх стратегій, можливостей та загроз, що дозволяє розробити ефективну стратегію для власного бізнесу.

Таблиця 4.9

Ступеневий аналіз конкуренції на ринку

№ п/п	Фактор конкурентоспро- можності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з проектом						
			-3	-2	-1	0	1	2	3
1	Технологічна інноваційність	14						+	
2	Вартість послуг	15				+			
3	Якість обслуговування	17					+		
4	Географічна доступність	18		+					
5	Маркетингові стратегії	14						+	
6	Управлінський досвід	10						+	

Далі був зроблений SWOT-аналіз стартап-проекту (таблиця 4.10) - інструмент стратегічного аналізу, який дозволяє оцінити сильні та слабкі сторони внутрішнього середовища стартапу (Strengths and Weaknesses) та можливості та загрози зовнішнього середовища (Opportunities and Threats) В результаті аналізу формується матриця, яка допомагає визначити потенційні переваги та недоліки стартапу і розробити стратегію розвитку, враховуючи ці фактори. SWOT-аналіз допомагає стартапам ліпше розуміти свій стан на ринку і приймати обґрунтовані рішення для досягнення успіху.

Таблиця 4.10

SWOT- аналіз стартап-проекту

Сильні сторони: Технологічна інноваційність Адаптація до вимог клиента	Слабкі сторони: Низька відомість Фінансові обмеження
--	--

Можливості: Зростаючий попит Партнерство з операторами	Загрози: Конкуренція на ринку Технічні проблеми
--	---

4.4. Розроблення ринкової стратегії проекту

Стратегія спеціалізації для компанії, яка надає послуги операторам мобільного зв'язку у сфері DRaaS:

1. Глибоке розуміння потреб операторів мобільного зв'язку:
 - Аналізувати унікальні вимоги та особливості операторів мобільного зв'язку у сфері відновлення після аварій.
 - Розробляти рішення, спеціально адаптовані до високих навантажень, типових для цієї галузі.
2. Орієнтація на високу доступність та надійність:
 - Забезпечувати можливість миттєвого відновлення послуг у разі відмови чи кризової ситуації.
 - Вдосконалювати технічні рішення для забезпечення найвищого рівня доступності.
3. Розвиток гнучких та інтегрованих рішень:
 - Підтримувати гнучкі та інтегровані рішення, які легко адаптуються до різних інфраструктур операторів мобільного зв'язку.
 - Забезпечувати сумісність з існуючими технологіями та інфраструктурою замовників.
4. Стратегічне партнерство з виробниками обладнання та розробниками програмного забезпечення:
 - Укладати стратегічні партнерства з виробниками обладнання, що використовується операторами мобільного зв'язку.
 - Розробляти інтегровані рішення, які оптимально взаємодіють із специфічними системами клієнтів.

5. Забезпечення безпеки та відповідність нормативам:

- Вдосконалювати заходи забезпечення конфіденційності та інтегрованість з вимогами законодавства та стандартів безпеки.

- Надавати сертифіковані рішення, що відповідають стандартам галузі.

6. Акцент на штучний інтелект та аналітику:

- Впроваджувати технології штучного інтелекту для передбачування можливих проблем та автоматизації процесів відновлення.

- Надавати аналітичні засоби для постійного моніторингу та оптимізації роботи систем в реальному часі.

7. Комплексне навчання та підтримка:

- Забезпечувати навчання та консультації з питань використання DRaaS для мобільних операторів.

- Надавати 24/7 підтримку для оперативного реагування на можливі проблеми.

Ця стратегія спеціалізації дозволить компанії ефективно конкурувати в галузі DRaaS та відповідати специфіці вимог операторів мобільного зв'язку.

Сформулювати основну стратегію для подальшого розвитку в обраному сегменті, яка представлена в таблиці 4.11.

Таблиця 4.11

Ступеневий аналіз конкуренції на ринку

№ п/п	Опис цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієтова ний обсяг попиту	Інтенсивність конкуренції в цьому сегменті	Простота входу у сегмент потенційних споживачів
1	Оператори мобільного зв'язку	Переважаю готові	Високий	Високий	Важко
2	Середній бізнес	Переважаю готові	Високий	Високий	Важко

4.5. Розроблення маркетингової програми стартап-проекту

Маркетингова програма - це намічений для планомірного здійснення, об'єднаний єдиною метою та залежний від певних строків комплекс взаємопов'язаних завдань і адресних заходів соціального, економічного, науково-технічного, виробничого, організаційного характеру з визначенням ресурсів, що використовуються, а також джерел одержання цих ресурсів.

Основну увагу слід приділяти вибору, значенню та формі інструментів маркетингу, їх об'єднанню в найбільш оптимальний з погляду визначеної мети комплекс, а також розподілу фінансових ресурсів у межах бюджетування маркетингу.

Першим кроком є формування маркетингової концепції товару, який отримає споживач (таблиця 4.12)

Таблиця 4.12

Визначення ключових переваг концепції потенційного товару

Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами
Забезпечення бізнес-континіуму, миттєве відновлення після аварії, масштабованість та швидкість відновлення	Ефективніше рішення за доступною ціною, підвищення зручності, зменшення витрат, зниження операційних витрат	Ефективніше рішення за доступною ціною, унікальні функції та дизайн

Маркетингова програма повинна бути гнучкою та адаптованою до змін на ринку та потреб клієнтів. Основною метою є залучення нових клієнтів, підвищення їхньої лояльності та підтримання конкурентоспроможності на ринку.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

Метою даної дипломної роботи було вивчення та аналіз можливостей використання хмарних середовищ для забезпечення надійності даних мобільних операторів. У першому розділі я розглянула основні етапи становлення та розвитку мереж мобільного зв'язку, а також архітектуру побудови сучасних мереж. Інфраструктура оператора мобільного зв'язку складається з різноманітних технологічних компонентів, які спільно забезпечують функціонування мережі та надання послуг зв'язку. Взагалі, стійкість інфраструктури оператора мобільного зв'язку є стратегічно важливою, оскільки вона визначає ефективність, безперебійність та конкурентоспроможність мобільного оператора на ринку зв'язку.

Як наслідок, забезпечення стійкості бек-енд інфраструктури мобільного оператора є ключовим аспектом для ефективності та безперебійності надання послуг мобільного зв'язку. Нижче розглянуті важливі аспекти цієї стійкості:

- Надійність послуг для користувачів: бек-енд інфраструктура мобільного оператора відповідає за обробку дзвінків, передачу даних, аутентифікацію та інші операції. Стабільність цих сервісів є критично важливою для задоволення потреб користувачів і збереження їхньої вірності оператору.
- Безпека мережі: стійкість бек-енд інфраструктури є важливою для забезпечення безпеки мобільного зв'язку. Вона допомагає уникнути атак, витоку конфіденційної інформації, а також забезпечує захист від шкідливих програм і вторгнень.
- Забезпечення безперебійності служб: мобільні оператори надають ряд різноманітних послуг, таких як голосовий та відео-зв'язок, доступ до Інтернету, месенджери тощо. Стійкість бек-енд інфраструктури гарантує безперебійність цих послуг, навіть в умовах великого обсягу трафіку або навантаження.
- Забезпечення резервування та відновлення: стійка бек-енд інфраструктура повинна мати механізми резервного копіювання та відновлення даних для

запобігання втратам інформації в разі аварій або випадків форс-мажорів.

- Дотримання стандартів і регуляторних вимог: важливо, щоб бек-енд інфраструктура відповідала вимогам законодавства та стандартам, які регулюють галузь мобільного зв'язку, зокрема в області конфіденційності і безпеки даних.
- Відмовостійкість і резервування: забезпечення стійкості в умовах можливих відмов або виникнення проблем допомагає уникнути перерв у наданні послуг і забезпечити найвищий рівень доступності.

Для підвищення стійкості сервісу стільникового зв'язку було розглянуто варіант використання сервісу аварійного відновлення (DRaaS).

Використання Disaster Recovery as a Service (DRaaS) операторами мобільного зв'язку надає ряд значущих переваг та покращень для забезпечення надійності та безпеки їхніх послуг. Декілька ключових переваг включають:

1. Швидка відновлюваність послуг: DRaaS надає можливість швидкого відновлення послуг у випадку відмови чи катастрофи. Це забезпечує мінімальний час простою та швидке відновлення нормального функціонування мережі мобільного зв'язку.

2. Автоматизовані процеси відновлення: DRaaS використовує автоматизовані процеси відновлення, що дозволяє операторам швидко та ефективно відновлювати роботу мережі без значного втручання людей.

3. Масштабованість: DRaaS надає можливість масштабування відновлюваних ресурсів в залежності від обсягу та характеру відмови чи кризової ситуації. Це дозволяє ефективно використовувати ресурси та забезпечувати стійкість мережі навіть у складних умовах.

4. Економічна ефективність: замість створення та утримання власних інфраструктур для відновлення, оператори можуть скористатися готовими рішеннями DRaaS, що робить використання цієї послуги більш економічно вигідним.

5. Тестування та вдосконалення: DRaaS дозволяє регулярно проводити тести відновлення для перевірки ефективності систем та процесів в разі

відмови. Це сприяє вдосконаленню планів відновлення та підвищенню загальної стійкості мережі.

6. Гарантована відмовостійкість: DRaaS забезпечує гарантію відмовостійкості за допомогою розташування віддалених копій даних та інфраструктури. Це зменшує ризик втрати даних та дозволяє операторам швидше відновлювати послуги.

7. Доступність експертної підтримки: DRaaS часто включає експертну технічну підтримку, яка може надавати допомогу та консультації в разі відмови чи інших аварійних ситуацій.

8. Зменшення ризиків та вартості припинення роботи: застосування DRaaS допомагає зменшити ризики та вартість припинення роботи, а також підвищує загальну стійкість і робочу продуктивність мережі мобільного зв'язку.

Всі ці переваги роблять DRaaS привабливим рішенням для операторів мобільного зв'язку, які прагнуть забезпечити стабільність та високу доступність своїх послуг в умовах сучасного технологічного середовища. В даній роботі я розглянула приклад реалізації такого рішення, яке базується на таких ключових технологіях:

- VMware ESXi: для забезпечення середовища із віртуалізації.
- Oracle Physical Standby та Oracle Data Guard використовуються для забезпечення реплікації баз даних між основним та резервним сайтами.
- UltraDNS-сервіси: управління DNS записами та можливість перемикати IP адреси на DR-середовище.

Для автоматизації процесів розгортання середовища планується використовувати такі інструменти, як Ansible та Terraform.

1. Ansible є відкритим інструментом автоматизації, який використовує декларативний підхід до опису конфігурації та управління системами. Даний інструмент широко використовується для автоматизації розгортання додатків, налаштування серверів, управління конфігурацією та інших операційних завдань. У своєму проекті я планую використовувати його для виконання різноманітних завдань, включаючи налаштування, установку пакетів,

автоматизацію розгортання нових релізів тощо.

2. Terraform – інструмент для автоматизації управління інфраструктурою як коду (Infrastructure as Code, IaC), який дозволяє автоматизувати і уніфікувати процеси розгортання та управління інфраструктурою. Terraform використовується для створення нових об'єктів у хмарному середовищі за допомогою файлів конфігурації, які містять опис певних ресурсів та їх властивостей. Для нашого сценарію ми використовуємо його для переключення DNS А записів із IP основного сайту, на IP DR-сайту.

Таким чином використання Disaster Recovery as a Service (DRaaS) разом із автоматизованими системами розгортання, такими як Ansible і Terraform, може призвести до численних переваг для бізнесу:

- Швидкість та Ефективність: автоматизація систем розгортання дозволяє швидко та ефективно створювати і налаштовувати резервні середовища в разі аварії. DRaaS разом із засобами автоматизації дозволяє бізнесу миттєво відновлювати доступ до даних та сервісів.
- Скорочення Витрат на IT-Адміністрування: автоматизація процесів, включаючи розгортання та керування резервними системами, може значно зменшити навантаження на IT-персонал. Це дозволяє витратити менше часу на рутинні завдання та зосереджувати увагу на стратегічних аспектах IT.
- Висока Надійність та Швидке Відновлення: DRaaS, поєднаний із засобами автоматизації, забезпечує високу надійність та швидке відновлення даних та систем.
- Зменшення ризиків та відновлення від помилок: автоматизовані системи дозволяють уникнути помилок, пов'язаних із ручним втручанням.

Як підсумок, поєднання DRaaS і автоматизованих систем розгортання створює ефективну та надійну інфраструктуру для відновлення бізнес-операцій у випадку аварій та забезпечення більшого контролю та гнучкості управління резервними системами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Li, Z., & Yang, Z. (2018). Cloud Computing for Mobile Users: Can Offloading Computation Save Energy? Computer 43(4) - Published by IEEE (Institute of Electrical and Electronics Engineers), 51-56 с. [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/220475756_Lu_Y-H_Yung-Hsiang_Lu_Cloud_Computing_for_Mobile_Users_Can_Offloading_Computation_Save_Energy_Computer_434_51-56
2. Garg, S. K., Versteeg, S., & Buyya, R. (2013). A framework for ranking of cloud computing services. Future Generation Computer Systems, 29(4), 1012-1023. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.sciencedirect.com/science/article/abs/pii/S0167739X12001422>
3. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (Special Publication 800-145). National Institute of Standards and Technology. [Електронний ресурс] – Режим доступу до ресурсу: <https://doi.org/10.6028/NIST.SP.800-145>
4. Issa M. Khalil 1, Abdallah Khreishah, Muhammad Azeem (2014). Cloud Computing Security: A Survey, 75, 200-222. [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/269516029_Cloud_Computing_Security_A_Survey
5. Rappaport, T. S. (2017). Wireless Communications: Principles and Practice. Second edition. Prentice Hall; Subsequent edition (January 1, 2002) - 14-22 с., [Електронний ресурс] – Режим доступу до ресурсу: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjf0tmm1b-DAxVdif0HHeGrClQQFnoECA4QAQ&url=https%3A%2F%2Ftelkom2013.files.wordpress.com%2F2014%2F02%2Fwireless-comm-princip-n-practice-theodoresrappaport.pdf&usg=AOvVaw0xJSwJd7EI_6tYDTzTVnc8&opi=89978449

6. Goldsmith, A. (2005). Wireless Communications. Cambridge University Press. [Электронный ресурс] – Режим доступа до ресурсу: Goldsmith, A. (2005). Wireless Communications. Cambridge University Press. [Электронный ресурс] – Режим доступа до ресурсу: https://www.academia.edu/34960457/WIRELESS_COMMUNICATIONS

7. Fettweis, G., Alamouti, S., Mueller, T., & Kittlaus, E. (2014). 5G: Personal mobile internet beyond what cellular did to telephony. IEEE Communications Magazine, 52(2), 140-145. [Электронный ресурс] – Режим доступа до ресурсу: https://www.vodafone-chair.org/media/publications/legacy/gerhard-fettweis/5G_%E2%80%93_Personal_Mobile_Internet_Beyond_What_Cellular_Did_to_Telephony.pdf

8. Zahariadis, T., & Kazakos, D. (2003). (R)Evolution Toward 4G Mobile Communication Systems. IEEE Wireless Communications, 10(4) [Электронный ресурс] – Режим доступа до ресурсу: https://www.researchgate.net/publication/3435921_REvolution_Toward_4G_Mobile_Communication_Systems

9. Gustafsson, E., & Jonsson, A. (2003). Always Best Connected. IEEE Wireless Communications, 49-55. [Электронный ресурс] – Режим доступа до ресурсу: <https://ieeexplore.ieee.org/document/1182111>

10. Ibrahim, J. (2002). 4G Features. Bechtel Telecommunications Technical Journal, 1(1), 11-14. [Электронный ресурс] – Режим доступа до ресурсу: <https://ftp.unpad.ac.id/orari/library/library-ref-eng/ref-eng-3/physical/wimax/wikipedia/Article2.pdf>

11. Evans, G., & Baughan, K. (2001). Visions of 4G. Electronics and Communication Engineering Journal, Jan. 2001. [Электронный ресурс] – Режим доступа до ресурсу: https://www.researchgate.net/publication/3364629_Visions_of_4G

12. Lu, W. W., & Berezdivin, R. (2002). Technologies on Fourth Generation Mobile Communications. IEEE Wireless Communications, 9(2), 8-71. [Электронный ресурс] – Режим доступа до ресурсу:

https://www.academia.edu/53766642/Guest_editorial_technologies_on_fourth_generation_mobile_communications

13. Falconer, D., Adachi, F., & Gudmundson, B. (1995). Time Division Multiple Access Methods for Wireless Personal Communications. IEEE Communications Magazine. [Электронный ресурс] – Режим доступа до ресурсу: <https://ieeexplore.ieee.org/document/339881>.

14. H. Honkasalo, K. Pehkonen, M.T. Niemi, A.T. Leino, "WCDMA and WLAN for 3G and Beyond," IEEE Wireless Communications, Volume 9, Issue 2, pp. 14-18, April 2002. [Электронный ресурс] – Режим доступа до ресурсу: <https://ieeexplore.ieee.org/abstract/document/998520>

15. Thom, G. A. (1996). H.323: The Multimedia Communications Standard for Local Area Networks. IEEE Communications Magazine, 34(12), 52-56. [Электронный ресурс] – Режим доступа до ресурсу: <https://ieeexplore.ieee.org/document/556487>

16. Short, M., & Harrison, F. (2002). A Wireless Architecture for a Multimedia World. The Journal of Communications Network, 1(Part 1), April–June. [Электронный ресурс] – Режим доступа до ресурсу: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=faa95da3815d0627c2fe063752fa1df9c2d051a5>

17. Faccin, S. M., Lalwaney, P., & Patil, B. (2004). IP Multimedia Services: Analysis of Mobile IP and SIP Interactions in 3G Networks. IEEE Communications Magazine, 42(1), 113–120. [Электронный ресурс] – Режим доступа до ресурсу: https://www.scss.tcd.ie/hitesh.tewari/bib_files/flp04.pdf

18. Chiussi, F. M., Khotimsky, D. A., & Krishnan, S. (2002). Mobility Management in Third Generation All-IP Networks, September. [Электронный ресурс] – Режим доступа до ресурсу: <https://ieeexplore.ieee.org/document/1031839>

19. Tseng, Y., Shen, C., & Chen, W. (2003). Integrating Mobile IP with Ad Hoc Networks. IEEE Computer Magazine, 36(5), 48–55. [Электронный ресурс] – Режим доступа до ресурсу: <https://ieeexplore.ieee.org/document/1031839>

ресурсы:http://ant.comm.ccu.edu.tw/course/92_3G/1_Papers_C/Integrating%20mobile%20IP%20with%20ad%20hoc%20networks.pdf

20. A. Furuskar, S. Mazur, F. Muller, and H. Olofsson, “EDGE: enhanced data rates for GSM and TDMA/136

evolution,” IEEE Wireless Commun. Mag., Vol. 6, pp. 56 - 66, June 1999
[Электронный ресурс] – Режим доступа до ресурсу:
https://www.researchgate.net/publication/3344055_EDGE_enhanced_data_rates_for_GSM_and_TDMA136_evolution

21. L. Harte, (October 5, 2006). Introduction to Mobile Telephone Systems, 1G, 2G, 2.5G, and 3G Technologies and Services, Althos Publishing; 2nd edition.
[Электронный ресурс] – Режим доступа до ресурсу:
<https://www.amazon.com/Introduction-Telephone-Systems-Technologies-Services/dp/1932813934>

22. Holma, H., & Toskala, A. (2004). WCDMA for UMTS: HSPA Evolution and LTE. John Wiley & Sons. [Электронный ресурс] – Режим доступа до ресурсу: https://www.academia.edu/6901392/WCDMA_FOR_UMTS_Third_Edition

23. Ghosh, A., Ratasuk, R., Mondal, B., Mangalvedhe, N., Thomas, T., & Caire, G. (2010). LTE-Advanced: next-generation wireless broadband technology. IEEE Wireless Communications, 17(3), 10-22. [Электронный ресурс] – Режим доступа до ресурсу:
<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f2e311661820b416c844e480ce133fafd61a6b48>

24. Li, B. (2004). 3G CDMA2000 Wireless System Engineering. Artech House. [Электронный ресурс] – Режим доступа до ресурсу:
<https://docplayer.net/10175762-3g-cdma2000-wireless-system-engineering.html>

25. Goldsmith, A. (2005). Wireless Communications. Cambridge University Press. [Электронный ресурс] – Режим доступа до ресурсу:
<http://fa.ee.sut.ac.ir/Downloads/AcademicStaff/1/Courses/7/Andrea%20Goldsmith-Wireless%20Communications-Cambridge%20University%20Press%20%282005%29.pdf>

26. Amazon Web Services (AWS). [Электронный ресурс] – Режим доступа до ресурсу: <https://docs.aws.amazon.com/>
27. Microsoft Azure. [Электронный ресурс] – Режим доступа до ресурсу: <https://docs.microsoft.com/en-us/azure/>
28. Google Cloud [Электронный ресурс] – Режим доступа до ресурсу: <https://cloud.google.com/docs/>
29. IBM Cloud [Электронный ресурс] – Режим доступа до ресурсу: <https://cloud.ibm.com/docs>
30. Datadog. [Электронный ресурс] – Режим доступа до ресурсу: <https://docs.datadoghq.com/>
31. Terrafarm. [Электронный ресурс] – Режим доступа до ресурсу: <https://developer.hashicorp.com/terraform/docs>
32. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 5. [Электронный ресурс] – Режим доступа до ресурсу: <https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5>
33. Buyya, R., Broberg, J., & Goscinski, A. M. (2011). *Cloud computing: principles and paradigms*. – Wiley, 2011. – 664 с. – ISBN: 978-0-470-88799-8
34. Ansible [Электронный ресурс] – Режим доступа до ресурсу: <https://docs.ansible.com/>
35. United States National Institute of Standards and Technology (NIST) - NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems, 2010. [Электронный ресурс] – Режим доступа до ресурсу: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf>
36. M. Wallace, L. Webber (2017). *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*, – AMACOM, 2017. – 544 с. – ISBN: 978-0-814-43876-3
37. S.Snedaker, C. Rima (2014) *Business Continuity and Disaster Recovery Planning for IT Professionals* – Syngress, 2014. – 577 с. – ISBN: 978-0-12-410526-3

38. J. Watters (2014), Disaster Recovery, Crisis Response, and Business Continuity – Apress, Berkeley, CA, 2014 – 295 c. – ISBN: 978-1-4302-6406-4
39. John W. Rittinghouse, James F. Ransome "Business Continuity and Disaster Recovery for InfoSec Managers," – Digital Press, 2006 – 338 c. – ISBN: 978-1-55558-339-2
40. E. Schultz,(2001). Incident Response: A Strategic Guide to Handling System and Network Security Breaches," – Sams, 2001 – 408 c. – ISBN: 978-1-57870-256-5
41. David H. Jonassen, Learning to Solve Problems An Instructional Design Guide – Wiley, 2004 – 253 c. – ISBN: 0-7879-6437-9
42. G. Kim, K. Behr, Ge. Spafford (2018). The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win – IT Revolution Press, 2018 – 432 c. – ISBN: 978-1942788294
43. United States Federal Emergency Management Agency (FEMA) - National Response Framework, 2021. [Електронний ресурс] – Режим доступу до ресурсу: https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf
44. United States Federal Emergency Management Agency (FEMA) - Comprehensive Preparedness Guide 101: Developing and Maintaining Emergency Operations Plans, 2010. [Електронний ресурс] – Режим доступу до ресурсу: https://www.fema.gov/sites/default/files/2020-05/CPG_101_V2_30NOV2010_FINAL_508.pdf
45. J. Petoff, N. Murphy , B. Beyer , C. Jones (2016). Site Reliability Engineering: How Google Runs Production Systems 1st Edition – O'Reilly Media , 2016 – 550 c. – ISBN: 978-1491929124
46. N. Richard Murphy, David K. Rensin, K. Kawahara, S. Thorne, B. Burns(2018). The Site Reliability Workbook: Practical Ways to Implement SRE – O'Reilly Media , 2018 – 500 c. – ISBN: 978-1492029502
47. Що таке мобільні мережі 1G, 2G, 3G. [Електронний ресурс] – Режим

доступу до ресурсу:

<https://vseplus.com/ua/article/cto-takoe-mobilnye-seti-1g-2g-3g-756>

48. 7 переваг використання хмарних рішень для сучасного бізнесу [Електронний ресурс] – Режим доступу до ресурсу:

<https://hub.kyivstar.ua/news/7-perevag-vykorystannya-hmarnyh-rishen-dlya-suchasnogo-biznesu/>

49. Oracle Data Guard [Електронний ресурс] – Режим доступу до ресурсу:

<https://docs.oracle.com/en/database/oracle/oracle-database/19/sbydb/introduction-to-oracle-data-guard-concepts.html#GUID-5E73667D-4A56-445E-911F-1E99092DD8D7>

50. Data Guard Concepts and Administration [Електронний ресурс] – Режим доступу до ресурсу:

https://docs.oracle.com/cd/E11882_01/server.112/e41134/create_ps.htm