МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

ХМАРНІ ОБЧИСЛЕННЯ ТА ЇХ ІНТЕГРАЦІЯ З КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

Виконав: студент групи 2К-21
Спеціальності F7 Комп’ютерна інженерія
Олександр МОТАЙЛЕНКО
Керівник:
Павло РАТАЙЧУК

Черкаси 2025

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп’ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри КІ та ІТ

_____ Владислав ХОТУНОВ
(підпис)
«_____»_____2024 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Мотайленку Олександру Олександровичу

1. Тема кваліфікаційної роботи «Хмарні обчислення та їх інтеграція з комп'ютерними мережами»
Керівник роботи Ратайчук Павло Єгорович, викладач методист

затверджені наказом закладу вищої освіти від «07» жовтня 2024 року № 68у.
2. Строк подання студентом кваліфікаційної роботи 02.06.2025
3. Вихідні дані до кваліфікаційної роботи Аналіз впливу хмарних обчислень на архітектуру та функціонування комп'ютерних мереж, визначення ефективних методів інтеграції хмарних сервісів із локальними та глобальними мережами.

4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити) Вивчити концепцію та основні моделі хмарних обчислень (IaaS, PaaS, SaaS), проаналізувати архітектуру хмарних сервісів та їх інтеграцію з традиційними комп’ютерними мережами, дослідити основні технології взаємодії хмарних обчислень та мережевих інфраструктур (SD-WAN, VPN, MPLS), визначити методи забезпечення безпеки при використанні хмарних обчислень, виконати моделювання інтеграції хмарних обчислень у корпоративну мережу, оцінити ефективність впроваджених рішень та запропонувати рекомендації щодо оптимізації мережевої взаємодії з хмарними сервісами.
5. Дата видачі завдання 16.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання з підписами керівника і студента
1	Вступ	14.10.2024	
2	Розділ 1 . (ОСНОВИ ХМАРНИХ ОБЧИСЛЕНЬ)	9.12.2024	
3	Розділ 2 (ВПЛИВ ХМАРНИХ ОБЧИСЛЕНЬ НА АРХІТЕКТУРУ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ)	10.03.2025	
4	Розділ 3 (МОДЕЛЮВАННЯ ТА АНАЛІЗ ІНТЕГРАЦІЇ ХМАРНИХ ОБЧИСЛЕНЬ З КОМП'ЮТЕРНИМИ МЕРЕЖАМИ)	28.04.2025	
5	Висновки	12.05.2025	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2025	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2025	
8	Подання кваліфікаційної роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	10.06.2025	

Студент _____ Олександр МОТАЙЛЕНКО
(підпис)

Керівник роботи _____ Павло РАТАЙЧУК
(підпис)

АНОТАЦІЯ

У сучасних умовах розвитку інформаційних технологій хмарні обчислення відіграють ключову роль у забезпеченні масштабованості, доступності та ефективності обробки даних. Їх інтеграція з комп'ютерними мережами є актуальним напрямом досліджень, що відкриває нові можливості для оптимізації корпоративної інфраструктури та підвищення безпеки інформаційних систем.

У кваліфікаційній роботі розглянуто теоретичні засади хмарних обчислень, зокрема моделі IaaS, PaaS, SaaS, типи хмарних середовищ (публічні, приватні, гібридні, мультихмари), а також особливості їхньої архітектури, переваги та недоліки. Проаналізовано вплив хмарних обчислень на архітектуру комп'ютерних мереж, розглянуто традиційні мережеві моделі та їх адаптацію до хмарних технологій.

Особлива увага приділена технологіям взаємодії хмарної інфраструктури з комп'ютерними мережами, зокрема SD-WAN, VPN, MPLS, 5G, Edge та Fog Computing. Розглянуто методи забезпечення безпеки у хмарних середовищах, включаючи криптографічний захист, шифрування, політики безпеки та відповідність сучасним стандартам (ISO/IEC 27017, NIST, GDPR).

Практична частина роботи присвячена моделюванню інтеграції хмарних рішень у корпоративну мережу із використанням інструментів Cisco Packet Tracer, GNS3, EVE-NG, AWS CloudFormation. Проведено оцінку ефективності впроваджених рішень, проаналізовано продуктивність мережі, запропоновано рекомендації щодо оптимізації взаємодії з хмарними сервісами.

Дослідження демонструє, що правильна інтеграція хмарних обчислень з комп'ютерними мережами дозволяє значно покращити продуктивність, безпеку та гнучкість сучасної IT-інфраструктури.

Ключові слова: хмарні обчислення, комп'ютерні мережі, інтеграція, IaaS, PaaS, SaaS, SD-WAN, VPN, безпека, моделювання, оптимізація.

ABSTRACT

In today's information technology environment, cloud computing plays a key role in ensuring scalability, accessibility, and efficiency of data processing. Their integration with computer networks is a relevant area of research, which opens up new opportunities for optimizing corporate infrastructure and improving the security of information systems.

The qualification work considers the theoretical foundations of cloud computing, in particular, IaaS, PaaS, SaaS models, types of cloud environments (public, private, hybrid, multi-clouds), as well as features of their architecture, advantages and disadvantages. The author analyzes the impact of cloud computing on the architecture of computer networks, considers traditional network models and their adaptation to cloud technologies.

Particular attention is paid to the technologies of interaction between cloud infrastructure and computer networks, in particular SD-WAN, VPN, MPLS, 5G, Edge and Fog Computing. The methods of ensuring security in cloud environments, including cryptographic protection, encryption, security policies and compliance with modern standards (ISO/IEC 27017, NIST, GDPR) are considered.

The practical part of the work is devoted to modeling the integration of cloud solutions into a corporate network using Cisco Packet Tracer, GNS3, EVE-NG, AWS CloudFormation tools. The efficiency of the implemented solutions is evaluated, network performance is analyzed, and recommendations for optimizing interaction with cloud services are proposed.

The study demonstrates that proper integration of cloud computing with computer networks can significantly improve the performance, security and flexibility of modern IT infrastructure.

Keywords: cloud computing, computer networks, integration, IaaS, PaaS, SaaS, SD-WAN, VPN, security, modeling, optimization.

ЗМІСТ

ВСТУП

Актуальність обраної теми. На сьогоднішній день, хмарні технології все частіше інтегруються з комп'ютерними мережами — як локальними, так і глобальними. Це вимагає глибокого розуміння особливостей такої інтеграції, зокрема в аспектах безпеки, ефективності, масштабованості та сумісності з наявною інфраструктурою. Успішне поєднання хмарних сервісів з комп'ютерними мережами може суттєво підвищити надійність та продуктивність інформаційних систем, а також забезпечити гнучке управління ресурсами.

Метою роботи є проаналізувати принципи функціонування хмарних обчислень та їх взаємодію з комп'ютерними мережами, визначити ефективні методи інтеграції, виявити переваги та ризики, а також надати практичні рекомендації щодо впровадження таких рішень у корпоративному середовищі.

Для досягнення поставленої мети в роботі визначено такі **завдання**:

- дослідити моделі та архітектуру хмарних обчислень, а також типи хмарних середовищ;
- проаналізувати сучасні підходи до інтеграції хмарних сервісів із комп'ютерними мережами, включаючи аспекти безпеки;
- змоделювати процес інтеграції хмарних технологій у мережеву інфраструктуру та оцінити ефективність запропонованих рішень.

Об'єкт дослідження. Основним елементом дослідження виступають хмарні обчислення як технологічна платформа для зберігання й обробки даних.

Предмет дослідження. Основну увагу приділено способам та інструментам інтеграції хмарних обчислень з комп'ютерними мережами, з урахуванням їх впливу на архітектуру, продуктивність та безпеку.

Методами дослідження є теоретичний аналіз наукових джерел і технічної документації, порівняльне оцінювання підходів до інтеграції, методи моделювання (Cisco Packet Tracer, GNS3, AWS CloudFormation), аналіз результатів продуктивності, а також узагальнення та формулювання практичних

рекомендацій.

Структура роботи включає вступ, три розділи, висновки, список використаних джерел і додатки. У першому розділі розкриваються теоретичні засади хмарних обчислень. Другий розділ присвячено впливу хмарних технологій на архітектуру комп’ютерних мереж і безпеку. У третьому розділі здійснено моделювання та аналіз інтеграції хмарних сервісів у мережеве середовище. Завершується робота висновками та практичними рекомендаціями.

РОЗДІЛ 1
ОСНОВИ ХМАРНИХ ОБЧИСЛЕНЬ

1.1 Поняття та еволюція хмарних обчислень

У сучасному цифровому світі хмарні обчислення (Cloud Computing) стали невід'ємною частиною інфраструктури інформаційних технологій. Вони забезпечують дистанційний доступ до обчислювальних ресурсів, зберігання даних, програмного забезпечення та інструментів обробки інформації через мережу Інтернет. На відміну від традиційних моделей, в яких апаратне забезпечення і програмні продукти встановлюються локально, хмарна модель дає змогу споживачам використовувати ресурси на вимогу, спираючись на принципи масштабованості, мобільності, еластичності та ефективного розподілу ресурсів.

Термін «хмарні обчислення» отримав широке розповсюдження з 2006 року, коли компанія Amazon представила свою платформу Amazon Web Services (AWS), що дозволяла орендувати обчислювальні потужності через Інтернет. Проте концепція розподілених обчислень має набагато давніше походження.

Еволюція хмарних технологій проходила декілька ключових етапів:

- 1960-ті роки — поява ідеї "утилітарних обчислень" (utility computing), яку висунув Джон Маккарті. Передбачалося, що обчислювальні ресурси в майбутньому будуть надаватися як електроенергія — за споживанням.
- 1990-ті роки — активний розвиток віртуалізації, яка стала основою для формування сучасних хмарних платформ.
- 2000-ні роки — створення інфраструктурних платформ (IaaS) таких як AWS, Microsoft Azure та Google Cloud Platform, що сприяло масштабному впровадженню хмарних сервісів у бізнесі.
- 2010-ті роки — стрімке зростання хмарного ринку, перехід до

моделей PaaS (Platform as a Service) і SaaS (Software as a Service), а також поява гібридних і мультихмарних стратегій.

- 2020-ті роки — розвиток концепцій «edge computing» та «serverless computing», інтеграція хмар із мережами 5G, активне використання хмар для обробки великих даних, штучного інтелекту та Інтернету речей (IoT).

Сьогодні хмарні обчислення використовуються у всіх сферах — від освіти і охорони здоров'я до промисловості та оборони. Це не лише спосіб зберігати та обробляти дані, але й інструмент, що формує нові підходи до управління бізнес-процесами, оптимізації витрат та забезпечення гнучкості IT-інфраструктури.

1.2 Основні моделі хмарних обчислень (IaaS, PaaS, SaaS)

Хмарні обчислення передбачають надання доступу до обчислювальних ресурсів, зберігання даних та програмного забезпечення через інтернет. Вони організовані у вигляді сервісних моделей, які розрізняються за рівнем керування та наданими можливостями. Найпоширенішими моделями є IaaS (Infrastructure as a Service), PaaS (Platform as a Service) і SaaS (Software as a Service). Кожна з них має свої характеристики, переваги, рівень відповідальності провайдера та користувача.

Модель IaaS (Інфраструктура як сервіс) передбачає надання в оренду базової IT-інфраструктури — серверів, мереж, дискового простору та віртуальних машин. Користувач самостійно керує операційною системою, прикладним ПЗ, середовищем виконання та даними, тоді як постачальник відповідає за фізичну інфраструктуру та віртуалізацію. Типовими прикладами IaaS-рішень є Amazon Web Services (AWS EC2), Microsoft Azure Virtual Machines та Google Compute Engine. Ця модель підходить для компаній, яким необхідна гнучкість, масштабованість і контроль над системними ресурсами, але без витрат на фізичне обладнання.

Модель PaaS (Платформа як сервіс) орієнтована на розробників і забезпечує середовище для створення, тестування та розгортання додатків. У цій моделі постачальник не лише надає інфраструктуру, але й підтримує операційні системи, сервіси баз даних, веб-сервери, фреймворки та інструменти розробки. Користувач зосереджується виключно на коді та логіці програми. Це значно прискорює цикл розробки та полегшує масштабування. Прикладами PaaS-платформ є Google App Engine, Heroku, OpenShift. Такий підхід особливо корисний для стартапів та команд, які прагнуть швидко запустити продукт.

Модель SaaS (Програмне забезпечення як сервіс) дозволяє користувачу отримати доступ до готового програмного забезпечення через веб-інтерфейс, без потреби в інсталяції чи адмініструванні. Усі технічні аспекти, включаючи оновлення, безпеку, резервне копіювання — на стороні провайдера. SaaS є найпростішим і наймасовішим способом використання хмарних рішень. Найбільш відомі сервіси SaaS — це Google Workspace (Docs, Sheets, Gmail), Microsoft 365, Dropbox, Salesforce. SaaS зручно застосовувати в офісній роботі, CRM, фінансовому обліку, навчанні тощо.

Порівнюючи ці моделі, можна зазначити, що IaaS забезпечує найбільший рівень контролю над інфраструктурою, проте вимагає від користувача глибоких технічних знань. Модель PaaS виступає як компроміс — вона спрощує розгортання та керування додатками, залишаючи певний рівень контролю, водночас знижуючи складність адміністрування. SaaS є найзручнішим варіантом для кінцевого користувача, оскільки не потребує технічного втручання, однак надає мінімальний контроль над внутрішніми процесами та логікою роботи сервісу.

1.3 Типи хмарних середовищ (публічні, приватні, гібридні, мультихмари)

Розвиток хмарних технологій зумовив появу різних типів хмарних

середовищ, які класифікуються за способом розгортання та доступу до ресурсів. Кожен тип має власні технічні особливості, рівень контролю, безпеки та ціну впровадження. Найбільш поширеними типами є публічна, приватна, гібридна хмара, а також мультихмарне середовище.

Публічне хмарне середовище (Public Cloud) — це модель, у якій обчислювальні ресурси (сервери, сховища, програмне забезпечення) надаються третім сторонам через інтернет провайдером послуг. Користувачі ділять інфраструктуру з іншими клієнтами, отримуючи доступ до ресурсів на вимогу. Основними перевагами цієї моделі є низька вартість, простота масштабування, відсутність витрат на інфраструктуру та технічне обслуговування. До прикладів постачальників публічних хмар належать Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform. Недоліком є обмежений контроль над конфігурацією та безпекою, що не завжди відповідає вимогам конфіденційних або критично важливих систем.

Приватне хмарне середовище (Private Cloud) створюється виключно для однієї організації. Інфраструктура може бути розміщена як у власному дата-центрі, так і в орендованому хостингу, але управління нею здійснюється або самою організацією, або обраним провайдером. Приватні хмари дозволяють досягти максимального рівня безпеки, конфіденційності та відповідності галузевим стандартам, що особливо важливо для фінансових установ, державних органів або медичних організацій. Проте впровадження приватної хмари потребує значних капіталовкладень, технічної експертизи та постійної підтримки.

Гібридне хмарне середовище (Hybrid Cloud) — це комбінація публічної та приватної хмари, які функціонують як єдине середовище. Основна ідея — розміщення критично важливих даних у приватному середовищі, тоді як менш чутливі обчислення виконуються в публічному хмарному середовищі. Такий підхід дозволяє балансувати між безпекою, гнучкістю і витратами. Наприклад, компанія може використовувати приватну хмару для внутрішньої бухгалтерії, а

публічну — для обробки великого масиву клієнтських запитів під час маркетингової кампанії. З технічної точки зору, важливим викликом у гібридній моделі є забезпечення сумісності, безперебійної синхронізації даних, належного захисту інформації при її передачі між хмарами.

Мультихмарне середовище (Multicloud) передбачає використання послуг від кількох хмарних провайдерів одночасно. Це дозволяє організації уникати залежності від одного постачальника (vendor lock-in), оптимізувати витрати та підвищити стійкість до відмов (наприклад, при збоях на стороні одного з провайдерів система автоматично переключається на інший хмарний майданчик). Мультихмарна архітектура також дає змогу вибирати найкращі сервіси від різних постачальників відповідно до задач (наприклад, зберігання в AWS, а машинне навчання в Google Cloud). Проте мультихмара вимагає розвинених засобів моніторингу, автоматизації та безпеки, щоб ефективно управляти ресурсами з різних платформ.

1.4 Архітектура хмарних обчислень

Архітектура хмарних обчислень — це багаторівнева структура, яка визначає логічну організацію сервісів, компонентів і взаємозв’язків між ними, що забезпечують надання ресурсів як послуги через мережу. Вона базується на принципах віртуалізації, розподілених обчислень і автоматизованого управління інфраструктурою. Основною метою архітектури є забезпечення масштабованості, еластичності, високої доступності та ефективного розподілу ресурсів між користувачами.

Загалом архітектура хмарних обчислень включає три основні рівні:

1. Інфраструктурний рівень (Infrastructure Layer) — складається з фізичних ресурсів: серверів, систем зберігання, мережевого обладнання, центрів обробки даних. Цей рівень часто розташований у великих дата-центрах і

забезпечує базу для віртуалізації ресурсів.

2. Платформний рівень (Platform Layer) — відповідає за віртуалізацію, операційні системи, бази даних, середовища виконання, API та інструменти розробки. Тут працюють PaaS-рішення, які надають розробникам зручне середовище для створення та тестування програм.

3. Прикладний рівень (Application Layer) — охоплює сервіси, які кінцеві користувачі використовують через інтернет. Це можуть бути офісні програми, системи CRM, сервіси зберігання даних, інструменти аналітики тощо — реалізовані у формі SaaS.

Окрему роль відіграє служба керування ресурсами (Cloud Management Layer), яка виконує функції моніторингу, балансування навантаження, автоматичного масштабування, резервного копіювання, безпеки, ліцензування та виставлення рахунків. У складних архітектурах це можуть бути окремі модулі або навіть спеціалізовані програмні рішення (наприклад, OpenStack, VMware vRealize, Microsoft System Center).

Ключовими технологіями, що забезпечують функціонування хмарної архітектури, є віртуалізація, контейнеризація, розподілене зберігання, мережеві сервіси та автоматизація.

Віртуалізація дозволяє створювати ізольовані середовища у вигляді віртуальних машин або контейнерів на основі спільних фізичних ресурсів, при цьому гіпервізори на зразок VMware ESXi, Hyper-V або KVM виконують роль керуючого шару між обладнанням і віртуальними середовищами.

Контейнеризація, як більш легкий та гнучкий підхід, дає змогу запускати додатки в ізольованих контейнерах за допомогою таких рішень, як Docker або Kubernetes, що забезпечує швидке масштабування та простоту розгортання.

Розподілене зберігання даних, представлене сервісами схожих Amazon S3, Google Cloud Storage чи Ceph, забезпечує високу доступність інформації, стійкість до збоїв і ефективне резервування великих обсягів даних.

У свою чергу, мережеві сервіси включають програмно-визначені мережі (SDN), VPN-з’єднання, балансувальники навантаження, DNS-системи та інші інструменти, що відповідають за динамічну маршрутизацію трафіку в хмарному середовищі.

Завершальним компонентом є автоматизація й оркестрація процесів, яка реалізується за допомогою таких інструментів, як Terraform, Ansible або CloudFormation. Вони дозволяють централізовано створювати, змінювати й керувати інфраструктурою, що знижує вплив людського фактора та прискорює розгортання цифрових сервісів.

1.5 Переваги та недоліки хмарних технологій

Хмарні технології, як сучасний підхід до надання обчислювальних ресурсів, стали фундаментальним елементом цифрової трансформації в більшості галузей. Завдяки своїм характеристикам — масштабованості, доступності та ефективності — вони суттєво змінюють підхід до побудови інфраструктури підприємств. Проте, як і будь-яка технологія, хмарні обчислення мають свої переваги і обмеження, що слід враховувати під час впровадження.

Важливою перевагою є висока доступність сервісів. Хмарні провайдери зазвичай забезпечують географічно розподілену інфраструктуру, резервне копіювання та відмовостійкі технології, що дозволяє зберігати працездатність систем навіть у разі технічних збоїв. Обслуговування також значно спрощується — більшість завдань із оновлення, безпеки чи моніторингу виконуються автоматично або керуються провайдером, що зменшує навантаження на власний IT-відділ. Додатково, хмара забезпечує високу мобільність: доступ до ресурсів можливий з будь-якого пристрою з інтернетом, що підвищує ефективність віддаленої роботи та командної взаємодії.

Втім, хмарні рішення мають і певні обмеження. Основним технічним фактором є залежність від якісного інтернет-з’єднання. За його відсутності або

нестабільності доступ до сервісів стає ускладненим. Також актуальним є питання безпеки й конфіденційності: користувачі передають свої дані третім сторонам і не завжди мають повний контроль над тим, де і як ці дані обробляються. Це може створювати ризики, зокрема у контексті відповідності правовим нормам, як-от GDPR.

Ще одним викликом є складність міграції між хмарними платформами. У багатьох випадках формат даних, архітектура сервісів або ліцензійні умови провайдера не дозволяють легко змінити постачальника, що створює ефект залежності від конкретної екосистеми. Крім того, хмара не завжди дозволяє вносити глибокі зміни в конфігурацію, що може бути проблемою для компаній із нестандартними або галузевими вимогами. Додаткові труднощі виникають при реалізації багатохмарних рішень, які вимагають спеціалізованих знань, досвіду та додаткових витрат на координацію й технічну підтримку.

У підсумку, хмарні технології є дієвим засобом модернізації IT-інфраструктури, але ефективність їх впровадження залежить від правильного вибору моделі, типу хмари, рівня контролю та безпекових механізмів. Успішна інтеграція потребує не лише технічного забезпечення, а й стратегічного бачення, адаптації політик підприємства та готовності до змін у підходах до управління IT-ресурсами.

РОЗДІЛ 2
ВПЛИВ ХМАРНИХ ОБЧИСЛЕНЬ НА АРХІТЕКТУРУ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ.

2.1 Традиційні моделі мереж і їх адаптація до хмарних технологій

Традиційна модель комп’ютерної мережі передбачає чітку ієрархічну структуру з фіксованим набором пристроїв, централізованим управлінням і чітко окресленими межами безпеки. У такій архітектурі застосовуються фізичні сервери, маршрутизатори, комутатори, фаєрволи, які забезпечують зв’язок, контроль доступу, фільтрацію трафіку та інші функції. Вся інфраструктура, включно з серверами даних і програмним забезпеченням, розміщується у внутрішньому дата-центрі організації (on-premises).

У міру розвитку технологій, така модель почала втрачати актуальність через свою обмежену гнучкість, високу вартість масштабування та труднощі із забезпеченням безперервності бізнесу. Перехід до хмарних технологій став логічною відповіддю на зростаючі потреби бізнесу у масштабованості, доступності та швидкому розгортанні нових сервісів.

Традиційні мережі характеризуються низкою ключових рис, серед яких домінує централізація — усі дані зберігаються та обробляються локально, а управління інфраструктурою здійснюється зсередини організації. Така архітектура забезпечує високу прогнозованість: маршрути трафіку визначаються заздалегідь, що спрощує контроль над потоками даних. Проте ці мережі мають жорстку топологію — будь-які зміни у структурі потребують ручного втручання та часто супроводжуються фізичною перебудовою мережевого обладнання. Безпека в таких системах зазвичай базується на концепції захищеного периметра: доступ до ресурсів контролюється через корпоративний фаєрвол, а основна увага зосереджена на захисті межі локальної мережі.

Однак поява хмарних сервісів поставила нові виклики перед традиційними мережами. Дані тепер розміщуються за межами локальної інфраструктури,

користувачі підключаються до сервісів із будь-якого місця, а самі сервіси можуть розгортатися в кількох хмарах або регіонах. Це вимагає перегляду підходів до проєктування мереж.

Адаптація традиційних мереж до умов хмарної інфраструктури передбачає впровадження низки змін, спрямованих на підвищення гнучкості, безпеки та масштабованості. Одним із основних кроків є використання VPN (Virtual Private Network), що дозволяє створити захищене з'єднання між локальною мережею та хмарними ресурсами, забезпечуючи конфіденційність і цілісність переданих даних. Водночас активно застосовується побудова гібридної інфраструктури, яка поєднує локальні сервери з хмарними сервісами та надає можливість динамічно переміщати навантаження залежно від потреб (hybrid cloud network design). Значного поширення набуває впровадження програмно-визначених мереж (SDN), що забезпечують централізоване управління маршрутизацією, балансуванням навантаження і політиками безпеки — особливо важливо це у розподілених хмарних середовищах. Також змінюється підхід до захисту: традиційну модель периметра поступово витісняє концепція Zero Trust, заснована на принципі «не довіряй нікому за замовчуванням». Уся мережна взаємодія — як внутрішня, так і зовнішня — має бути попередньо аутентифікована, авторизована та зашифрована, що суттєво підвищує рівень безпеки в умовах хмарної інтеграції.

Вплив на архітектуру мережі: Зміни в архітектурі, викликані впровадженням хмари, торкаються не лише технічного боку. Вони також вимагають перебудови підходів до управління трафіком, моніторингу, виявлення загроз, а також взаємодії між командами DevOps, NetOps і SecOps. Традиційна модель «сегментації за VLAN» поступово доповнюється або витісняється політиками, що базуються на користувачах, пристроях, геолокації або типі додатка.

Сучасні тенденції розвитку мережевої інфраструктури в умовах хмарних технологій передбачають активне впровадження edge-обчислень, які доповнюють хмарні сервіси за рахунок обробки даних безпосередньо біля

джерела їх виникнення. Це дозволяє зменшити затримки, підвищити швидкість реагування систем та зменшити навантаження на центральні хмарні ресурси. Паралельно з цим відбувається інтеграція хмарних рішень із мережами п’ятого покоління (5G), що вимагає впровадження нових підходів до управління трафіком, забезпечення безперервності сервісів і високого рівня безпеки. Ще однією важливою тенденцією є автоматизація контролю доступу за допомогою систем управління ідентифікацією (IDaaS) та впровадження рольових моделей, що дозволяє централізовано й гнучко керувати правами користувачів у динамічному середовищі хмари.

Таким чином, адаптація традиційних мереж до хмарних умов — це не просто технічна модернізація, а стратегічний процес трансформації всієї IT-інфраструктури підприємства. Від правильності цієї адаптації залежить не лише продуктивність, а й безпека, стійкість і масштабованість корпоративного середовища.

2.2 Протоколи та технології взаємодії хмарних сервісів з мережами

У процесі інтеграції хмарних технологій у традиційну мережеву інфраструктуру важливу роль відіграють протоколи та технології, які забезпечують стабільну, безпечну і масштабовану взаємодію між локальними мережами, користувачами та хмарними середовищами. Оскільки хмара — це розподілене середовище з численними сервісами, її ефективне функціонування можливе лише за наявності налагоджених мережевих механізмів обміну даними, маршрутизації, тунелювання, шифрування тощо.

Базові протоколи мережевої взаємодії в хмарі:

1. HTTP/HTTPS (HyperText Transfer Protocol Secure) — основний протокол прикладного рівня для взаємодії користувачів з вебінтерфейсами хмарних сервісів. Усі SaaS-додатки працюють через HTTPS, що гарантує шифрування трафіку.

2. DNS (Domain Name System) — забезпечує розв'язання імен у

хмарних інфраструктурах, особливо у динамічних середовищах, де сервіси можуть змінювати IP-адреси. У хмарах використовуються DNS-сервіси з підтримкою автоматичного оновлення (наприклад, Amazon Route 53).

3. DHCP (Dynamic Host Configuration Protocol) — надає автоматичну IP-конфігурацію пристроям, які підключаються до хмарної або гібридної мережі.

4. IPsec (Internet Protocol Security) — забезпечує шифрування IP-трафіку на рівні мережевого протоколу, широко використовується для VPN-з'єднань між хмарною інфраструктурою та локальними мережами.

5. BGP (Border Gateway Protocol) — один із ключових протоколів маршрутизації в глобальних мережах. Використовується для побудови зв’язку між дата-центрами, маршрутизації між хмарними провайдерами або між хмарою та підприємством.

Спеціалізовані технології для хмарної взаємодії:

1. REST API / gRPC — хмарні сервіси часто взаємодіють через API (Application Programming Interface), що дозволяє програмно керувати ресурсами, додатками, інфраструктурою. REST API базується на HTTP, тоді як gRPC (Google Remote Procedure Call) забезпечує швидшу бінарну комунікацію.

2. SD-WAN (Software-Defined Wide Area Network) — дозволяє оптимізувати доступ до хмарних сервісів через інтелектуальне маршрутизаційне управління трафіком. Це особливо важливо в мультихмарних архітектурах або при використанні різних провайдерів.

3. VPN (Virtual Private Network) — одна з найважливіших технологій для захищеної передачі даних між локальною мережею організації та хмарним провайдером. Можливе використання IPsec VPN, SSL VPN або MPLS VPN залежно від рівня безпеки.

4. Load Balancer (балансувальник навантаження) — використовується для рівномірного розподілу навантаження між кількома хмарними вузлами, з метою уникнення перевантаження та забезпечення високої доступності.

5. CDN (Content Delivery Network) — розподіляє контент з хмари ближче до кінцевих користувачів (через географічно розташовані кеш-сервери),

підвищуючи швидкість доступу до даних.

Більшість сучасних хмарних платформ надають вбудовані інструменти для побудови, моніторингу та захисту мережевої інфраструктури. Такі сервіси, як AWS VPC (Virtual Private Cloud), дозволяють створювати логічно ізольовані мережі в межах Amazon Cloud, забезпечуючи гнучке управління підмережами, маршрутами та безпековими політиками. Аналогічно, Azure Virtual Network підтримує сегментацію мережі, створення підмереж та налаштування IP-адрес, що дозволяє адаптувати мережу до потреб організації. У Google Cloud VPC реалізовано можливість побудови гібридних мереж із міжрегіональним з'єднанням, що розширює масштабованість і доступність сервісів. Усі ці платформи підтримують хмарну маршрутизацію, NAT, політики фаєрволу, групи безпеки та інші засоби контролю доступу.

Однак з розвитком хмарних технологій постають нові виклики, зокрема необхідність забезпечення низьких затримок і високої пропускної здатності з'єднання. Динамічне масштабування мережевих налаштувань стає критично важливим у зв'язку зі змінною топологією хмарних середовищ. Окрему загрозу становлять DDoS-атаки, спрямовані на хмарні сервіси, що потребує використання спеціалізованих засобів захисту. В умовах мультихмарної архітектури також ускладнюється процес ідентифікації та контролю трафіку, що вимагає інтеграції розподілених систем моніторингу й аналізу, здатних працювати з великою кількістю точок доступу одночасно.

2.3 Використання SD-WAN, VPN та MPLS у хмарній інфраструктурі

Традиційні моделі побудови мережі більше не задовольняють вимоги до швидкості, гнучкості та масштабованості. Для забезпечення стабільної взаємодії з хмарними сервісами та ефективного управління трафіком організації впроваджують сучасні мережеві технології, зокрема SD-WAN, VPN та MPLS. Ці рішення дозволяють формувати безпечні, керовані та адаптивні канали зв'язку між локальними офісами, користувачами та хмарними платформами.

SD-WAN — це програмно-визначена мережева технологія, яка дозволяє централізовано керувати розподіленими WAN-з’єднаннями, зокрема між офісами підприємства і хмарними сервісами. Основною перевагою SD-WAN є інтелектуальний підхід до маршрутизації трафіку: маршрути вибираються не лише на основі IP-адрес, а й відповідно до параметрів якості з'єднання (затримка, втрата пакетів, завантаженість каналу).

SD-WAN має низку ключових переваг, які роблять його привабливим рішенням для сучасних мереж. Однією з основних є можливість одночасного використання кількох каналів зв’язку, таких як інтернет, MPLS та LTE, що забезпечує гнучкість і відмовостійкість з’єднання. Завдяки динамічній маршрутизації трафіку в режимі реального часу підвищується продуктивність доступу до хмарних сервісів, оскільки система автоматично обирає найоптимальніший маршрут. SD-WAN також дозволяє централізовано налаштовувати політики доступу, що спрощує управління мережею та підвищує рівень безпеки. Ще однією перевагою є зниження витрат на інфраструктуру порівняно з традиційними MPLS-рішеннями, що особливо актуально для організацій із розгалуженою структурою. Крім того, SD-WAN добре масштабується, що робить його ідеальним вибором для компаній із великою кількістю філій або користувачів, які працюють віддалено.

VPN залишається одним із найпоширеніших способів захищеного з’єднання з хмарною інфраструктурою. Він дозволяє створити зашифрований тунель між користувачем (чи локальною мережею) та хмарною платформою, забезпечуючи конфіденційність і цілісність переданих даних. Найбільш поширеними є протоколи IPsec VPN, SSL VPN та L2TP.

VPN-підключення широко використовуються для інтеграції локальної інфраструктури з публічними хмарними ресурсами, що є основою побудови гібридної хмари. Вони також забезпечують захищений віддалений доступ працівників до внутрішніх сервісів компанії, що розміщені у хмарному середовищі. Крім того, VPN застосовується для організації безпечного внутрішнього трафіку між віртуальними приватними мережами, розміщеними в

різних географічних регіонах. Водночас одним із основних недоліків VPN є обмежена масштабованість, а також залежність від пропускної здатності каналу зв’язку, що може створювати проблеми для великих організацій із високою кількістю паралельних з’єднань і значним мережевим навантаженням.

MPLS — це технологія маршрутизації, яка забезпечує передбачувану якість сервісу (QoS) і низьку затримку при передачі даних. Вона широко використовується у великих корпоративних мережах для створення приватних віртуальних каналів між офісами та дата-центрами, у тому числі для доступу до хмарної інфраструктури через MPLS VPN.

MPLS-технологія має низку важливих переваг, зокрема високу надійність, відмовостійкість та підтримку гарантованої пропускної здатності, що робить її придатною для критично важливих бізнес-сервісів. Вона також дозволяє інтегруватися з хмарними провайдерами за допомогою спеціалізованих рішень, таких як Amazon Direct Connect або Azure ExpressRoute, забезпечуючи стабільний і безпечний доступ до віддалених ресурсів. Водночас основним недоліком MPLS є висока вартість обслуговування та недостатня гнучкість у порівнянні з сучасними підходами на основі SD-WAN або публічних інтернет-мереж, що обмежує її застосування в умовах динамічних навантажень або масштабування.

2.4 Використання 5G, Edge Computing та Fog Computing у хмарних середовищах

ІТ-інфраструктура стрімко трансформується у напрямі децентралізації обчислень та зменшення затримок у доступі до сервісів. У цьому контексті особливе значення набувають такі інноваційні технології, як 5G, Edge Computing та Fog Computing. Їх інтеграція з хмарними обчисленнями відкриває нові можливості для побудови високопродуктивних, масштабованих і адаптивних систем.

П’яте покоління мобільного зв’язку (5G) забезпечує надзвичайно високу

пропускну здатність, мінімальні затримки — до 1 мілісекунди, а також підтримку великої кількості підключених пристроїв на обмеженій площі. Це відкриває широкі можливості для розвитку хмарних сервісів. Зокрема, 5G робить можливим одночасне підключення тисяч сенсорів у рамках концепції Інтернету речей (IoT), забезпечує стабільний зв’язок для дистанційного керування такими об'єктами, як промислові роботи, автономний транспорт і медичне обладнання, а також підвищує якість мобільного доступу до хмари. Завдяки мінімальній затримці обмін даними з хмарними сервісами може здійснюватися практично в реальному часі, що є критично важливим для застосувань у сфері автоматизації, безпеки та обробки великих обсягів інформації. Завдяки 5G мобільні пристрої можуть напряму підключатися до хмарних платформ без потреби у традиційній стаціонарній мережевій інфраструктурі, що особливо актуально для віддалених регіонів та тимчасових локацій.

Edge Computing — це модель обчислень, при якій обробка даних відбувається не в центральній хмарі, а на пристроях, розташованих на "краю" мережі, тобто поблизу джерела даних. Основна мета цієї технології — зменшити затримки та обсяг даних, що передаються до хмари. Edge Computing має низку суттєвих переваг, зокрема забезпечує мінімальні затримки, що робить його ідеальним рішенням для систем реального часу, таких як відеоспостереження, автономний транспорт або оперативне керування обладнанням. Завдяки локальній попередній обробці даних зменшується навантаження на хмарну інфраструктуру, що дозволяє оптимізувати трафік і прискорити обробку інформації. Крім того, edge-обчислення підвищують стійкість систем до збоїв у з’єднанні з центральною хмарною платформою, оскільки критичні функції можуть виконуватись безпосередньо на місці. Такий підхід активно впроваджується у сфері розумних міст, на виробничих підприємствах, в енергетиці, а також у роздрібній торгівлі, де важливе значення має швидка реакція на події та автономність роботи.

Fog Computing (туманні обчислення) є проміжною ланкою між хмарною інфраструктурою та пристроями на краю мережі. Fog-сервери розміщуються

ближче до кінцевого користувача, ніж традиційні хмари, але при цьому мають більші обчислювальні можливості, ніж типові edge-пристрої. Такий підхід дозволяє виконувати локальну аналітику в режимі реального часу, зменшувати навантаження на центральну хмару шляхом попередньої обробки даних, а також підвищувати рівень безпеки, оскільки чутлива інформація може оброблятися всередині локального сегменту мережі без необхідності передавати її до віддаленого дата-центру. Fog-середовище ідеально підходить для сценаріїв, де потрібне зниження трафіку до хмари, але повна обробка на рівні edge неможлива через обмеження ресурсів.

Комбінація хмарних технологій із 5G, Edge і Fog Computing дозволяє створити багаторівневу архітектуру, у якій крайові пристрої (edge) відповідають за первинну обробку та фільтрацію даних, fog-сервери виконують аналітику безпосередньо поблизу місця їх збору, а центральна хмара забезпечує зберігання великих обсягів інформації, глибоку обробку, виконання алгоритмів машинного навчання та резервне копіювання. Такий підхід сприяє підвищенню ефективності системи, зменшенню затримок і оптимізації навантаження на центральну інфраструктуру. Цей підхід підвищує ефективність, швидкість, надійність та масштабованість усієї IT-інфраструктури.

Технології edge та fog computing знаходять застосування в різних сферах. У розумних містах відео з камер спостереження обробляється на fog-вузлах для виявлення загроз у реальному часі, а збереження даних відбувається в хмарі. На виробництвах сенсори передають сигнали на edge-пристрої, де відбувається попередня обробка, а fog-аналітика виявляє несправності. У медицині пристрої пацієнтів надсилають дані на edge або fog рівень для швидкого реагування, а подальший аналіз виконується в хмарі.

2.5 Методи захисту даних у хмарних середовищах

Із розвитком хмарних технологій питання захисту даних стало одним з найважливіших у сфері інформаційної безпеки. Оскільки дані у хмарі можуть

зберігатися та оброблятися на віддалених серверах, що належать третім сторонам, організації повинні впроваджувати надійні методи захисту для забезпечення конфіденційності, цілісності та доступності інформації.

Одним із базових способів забезпечення безпеки є шифрування даних. Сучасні хмарні провайдери впроваджують як шифрування під час зберігання (at rest), так і під час передачі (in transit). Для цього використовуються алгоритми AES-256, TLS 1.3 та інші криптографічні протоколи. Користувачі можуть самостійно керувати ключами шифрування або ж покладатися на сервіси управління ключами, які надають платформи, наприклад AWS KMS, Azure Key Vault чи Google Cloud KMS.

Ще одним важливим механізмом є автентифікація та контроль доступу. Для запобігання несанкціонованому доступу застосовуються багатофакторна автентифікація (MFA), єдиний вхід (SSO) та системи управління ідентичностями (IAM). Адміністратори можуть призначати користувачам певні ролі, які обмежують доступ лише до необхідних ресурсів, що реалізує принцип найменших привілеїв (least privilege).

Також критично важливими є засоби моніторингу та виявлення загроз. У хмарних середовищах активно використовуються сервіси журналювання подій (CloudTrail, Azure Monitor, Google Cloud Audit Logs) та засоби виявлення аномальної активності. Це дозволяє оперативно реагувати на підозрілі дії, потенційні вторгнення або спроби витоку даних.

Особливу увагу варто приділити резервному копіюванню та відновленню після збоїв. У хмарі ці процеси автоматизуються через сервіси, які створюють знімки систем (snapshots), копії баз даних, об’єктного сховища тощо. Це дозволяє гарантувати відновлення критичних систем у разі програмного збою, кібератаки або випадкової втрати інформації користувачем.

Крім технічних засобів, важливо дотримуватись організаційних політик безпеки, які включають регулярне оновлення доступів, аудит безпеки, навчання персоналу, створення інструкцій з інцидентного реагування.

У хмарних середовищах застосовується і розподілена модель

відповідальності, згідно з якою провайдер відповідає за фізичну безпеку, доступність платформ і захист інфраструктури, тоді як користувач несе відповідальність за налаштування доступу, захист даних і дотримання нормативних вимог.

2.6 Використання криптографії та шифрування для захисту хмарних сервісів

Криптографія відіграє центральну роль у забезпеченні інформаційної безпеки. Саме завдяки надійному шифруванню можливо гарантувати, що доступ до інформації мають лише уповноважені користувачі, навіть якщо дані потрапляють у відкриті або потенційно небезпечні канали.

Одним із ключових механізмів захисту є шифрування даних під час зберігання (data-at-rest). Усі провідні хмарні провайдери, зокрема Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform, підтримують автоматичне шифрування жорстких дисків, баз даних, об’єктного сховища тощо. Найчастіше використовуються алгоритми AES (Advanced Encryption Standard) з довжиною ключа 256 біт, які на сьогодні вважаються надійними для більшості цивільних і навіть урядових задач.

Не менш важливим є шифрування даних під час передавання (data-in-transit), тобто коли інформація переміщується між користувачем і хмарною платформою або між різними компонентами самої платформи. Для цього використовуються протоколи TLS (Transport Layer Security) останніх версій, які забезпечують захищений обмін ключами, автентифікацію сторін та шифрування сесії. Весь вебтрафік у хмарних сервісах, як правило, реалізується через HTTPS, що базується саме на TLS.

Особливе значення має керування криптографічними ключами. Хоча провайдери зазвичай пропонують власні сервіси управління ключами (наприклад, AWS Key Management Service, Azure Key Vault, Google Cloud KMS), деякі компанії обирають модель Bring Your Own Key (BYOK) або навіть Hold

Your Own Key (HYOK), коли ключі зберігаються у замовника. Такий підхід дозволяє зменшити ризик несанкціонованого доступу з боку третіх осіб, у тому числі самих провайдерів.

Також використовуються асиметричні криптографічні методи, зокрема алгоритми RSA, ECC (еліптичні криві), які застосовуються для цифрових підписів, шифрування окремих файлів, перевірки автентичності та безпечного обміну ключами. Вони часто інтегруються з інфраструктурою відкритих ключів (PKI), яка використовується для сертифікації користувачів і пристроїв у хмарних середовищах.

Серед додаткових засобів захисту варто відзначити використання гомоморфного шифрування, яке дозволяє виконувати обчислення над зашифрованими даними без їх розшифрування. Хоча така технологія поки що має обмежене застосування через високу обчислювальну складність, вона вважається перспективною для задач, де критично важлива конфіденційність, зокрема в медицині, фінансах та державному секторі.

Важливо також враховувати, що на рівні хмарної архітектури шифрування повинно застосовуватись не лише до даних користувачів, але й до службової інформації, журналів аудиту, метаданих, резервних копій тощо. Повна криптографічна прозорість — ключ до довіри користувача до хмарної платформи.

2.7 Політики безпеки та відповідність стандартам (ISO/IEC 27017, NIST, GDPR)

Інформаційна безпека в хмарному середовищі не обмежується лише технічними заходами, такими як шифрування чи автентифікація. Вона також передбачає впровадження формалізованих політик безпеки і дотримання міжнародних стандартів, які регламентують правила поводження з даними, рівень захисту та відповідальність сторін.

Політика безпеки — це сукупність внутрішніх правил і процедур, які

регулюють доступ до ресурсів, обробку інформації, резервне копіювання, моніторинг дій користувачів тощо. В умовах хмари ці політики мають бути адаптовані до особливостей розподіленої інфраструктури.

Найважливішими складовими захисту хмарної інфраструктури є контроль доступу, журналювання, управління вразливостями та реагування на інциденти. Контроль доступу передбачає впровадження ролей, багатофакторної автентифікації та дотримання принципу найменших привілеїв, що обмежує ризики несанкціонованого доступу. Журналювання та аудит забезпечують фіксацію всіх дій у системі, дозволяючи проводити подальший аналіз або розслідування у разі порушень. Управління вразливостями включає регулярне оновлення програмного забезпечення та сканування на наявність загроз. Інцидент-менеджмент передбачає наявність чітких процедур реагування на витоки даних, кібератаки чи технічні збої, що дозволяє оперативно мінімізувати наслідки та відновити стабільну роботу системи.

Наявність політики безпеки не лише покращує захист, а й створює основу для відповідності міжнародним стандартам.

Основні міжнародні стандарти безпеки:

1. ISO/IEC 27017 — міжнародний стандарт, спеціалізований для хмарних провайдерів і користувачів. Він доповнює загальний стандарт ISO/IEC 27001 і описує конкретні засоби контролю в контексті хмарної інфраструктури: управління віртуальними середовищами, розмежування відповідальності, захист при передачі даних між різними платформами.

2. NIST SP 800-53 / 800-144 — рекомендації Національного інституту стандартів і технологій США. Документи NIST пропонують комплексний підхід до побудови безпеки в інформаційних системах, зокрема і в хмарі: категоризація даних, захист доступу, моніторинг подій, резервування тощо. NIST також пропонує чіткі моделі розподілу відповідальності між провайдером і користувачем.

3. GDPR (General Data Protection Regulation) — регламент Європейського Союзу щодо захисту персональних даних. У хмарному контексті

він зобов’язує провайдерів і користувачів гарантувати збереження приватності особистої інформації громадян ЄС. Основні вимоги: прозоре інформування, право на забуття, згода на обробку, локалізація зберігання даних.

Відповідність цим стандартам суттєво підвищує довіру клієнтів до хмарного провайдера, дозволяє працювати в регульованих галузях, таких як медицина, фінансовий сектор чи державне управління, а також знижує ризики юридичної відповідальності у випадку витоку або порушення конфіденційності даних. Крім того, вона сприяє налагодженню міжнародного партнерства, де дотримання уніфікованих вимог до безпеки є критично важливим фактором співпраці.

РОЗДІЛ 3
МОДЕЛЮВАННЯ ТА АНАЛІЗ ІНТЕГРАЦІЇ ХМАРНИХ ОБЧИСЛЕНЬ З КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

3.1. Вибір інструментів для моделювання (Cisco Packet Tracer, GNS3, EVE-NG, AWS CloudFormation)

Для ефективного проєктування, перевірки та візуалізації хмарних архітектур з інтеграцією мережевих технологій важливо обрати відповідні програмні засоби моделювання. Це дозволяє не лише перевірити працездатність рішень ще до їх фізичного впровадження, але й адаптувати архітектуру до конкретних технічних умов. У цьому контексті доцільно розглянути чотири поширені інструменти: Cisco Packet Tracer, GNS3, EVE-NG та AWS CloudFormation — кожен із яких має свої переваги, обмеження й призначення.

Cisco Packet Tracer є популярним симулятором комп’ютерних мереж, розробленим компанією Cisco. Він орієнтований на навчальні та демонстраційні цілі, однак дозволяє будувати повноцінні схеми з комутаторами, маршрутизаторами, VPN-серверами, DHCP- та DNS-сервісами. Завдяки зручному графічному інтерфейсу та інтерактивності користувачі можуть швидко моделювати мережі, аналізувати їхню поведінку й відслідковувати трафік у симульованому середовищі.

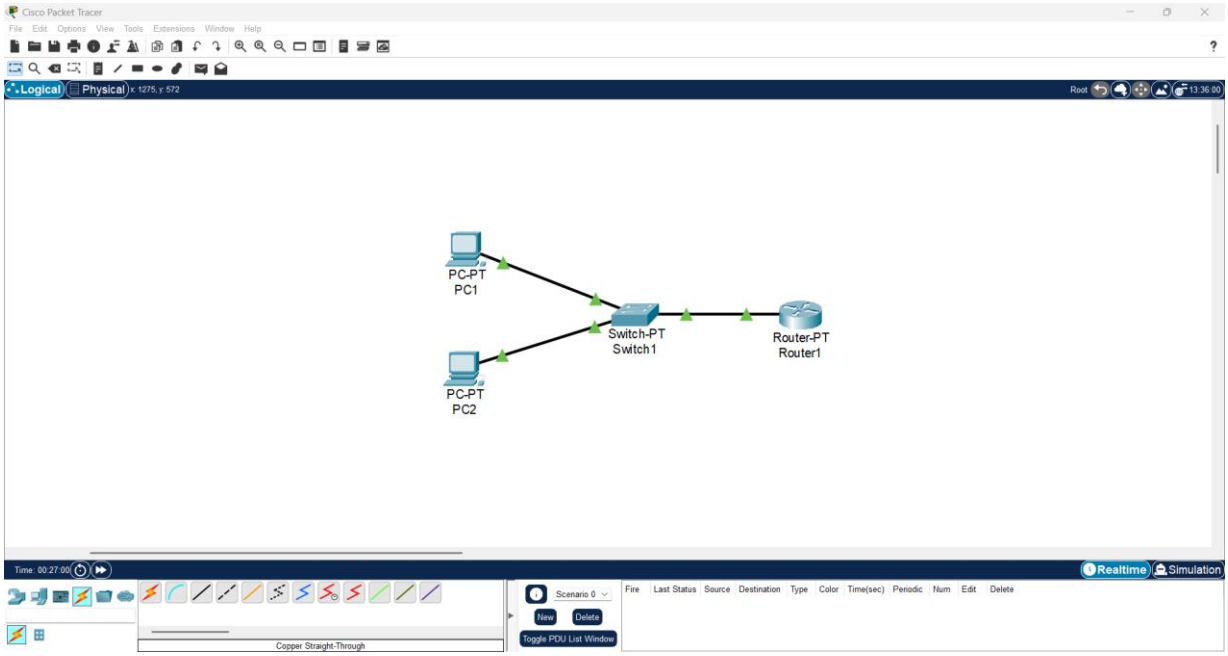

Рисунок 3.1 – Інтерфейс Cisco Packet Tracer з прикладом побудови мережі

Основним обмеженням Packet Tracer є відсутність підтримки реальних операційних систем пристроїв і обмежена функціональність у контексті складних хмарних сценаріїв. Проте, враховуючи завдання даної роботи — змоделювати базову інфраструктуру з елементами взаємодії з хмарою — цей інструмент є найбільш доречним і доступним.

Для глибшого технічного моделювання використовується GNS3 (Graphical Network Simulator 3). Цей інструмент дозволяє запускати справжні образи операційних систем (наприклад, Cisco IOS, pfSense, Ubuntu) та будувати складні віртуальні топології. GNS3 забезпечує підтримку тунельних протоколів, балансування навантаження, VPN-зв’язків і навіть симуляцію взаємодії з хмарними сервісами.

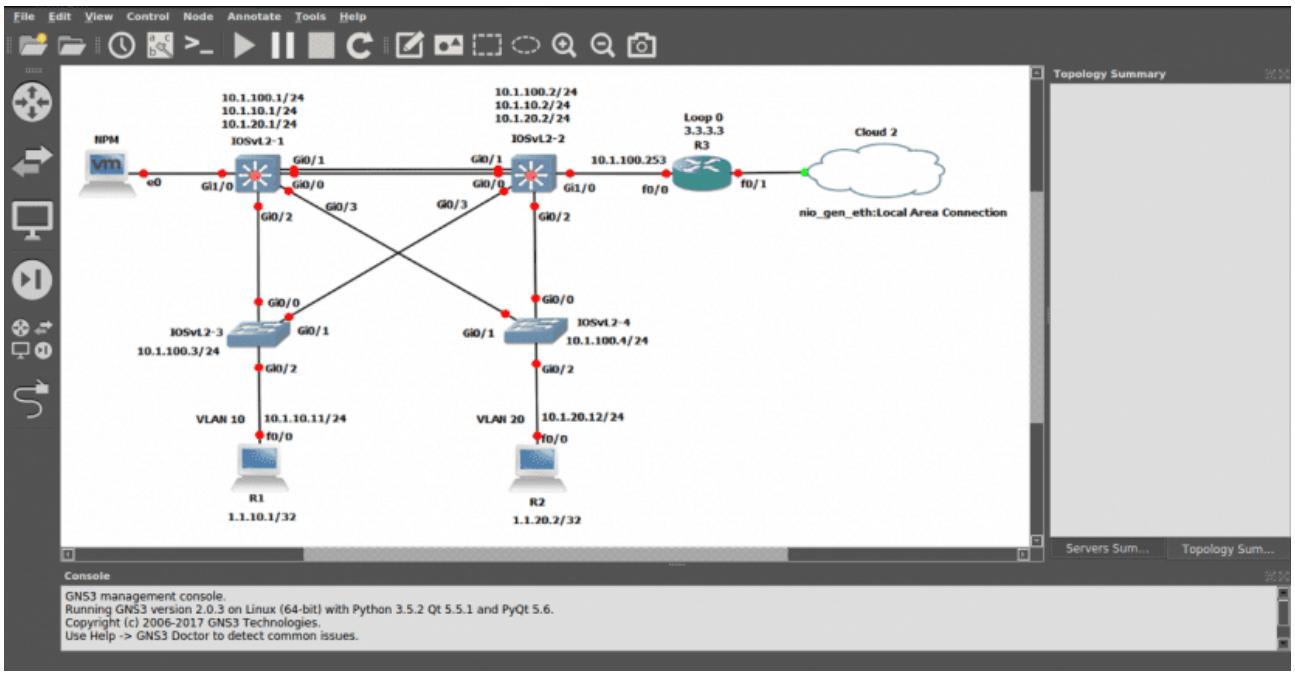

Рисунок 3.2 – Топологія в GNS3 із підключенням до хмарного сегменту

Іншою потужною платформою є EVE-NG (Emulated Virtual Environment – Next Generation), яка реалізує концепцію повноцінної віртуальної лабораторії. Вона дозволяє запускати десятки пристроїв одночасно, інтегрувати компоненти різних вендорів (Cisco, Juniper, Fortinet) та здійснювати складне моделювання мультихмарних архітектур із детальним контролем усіх рівнів мережі.

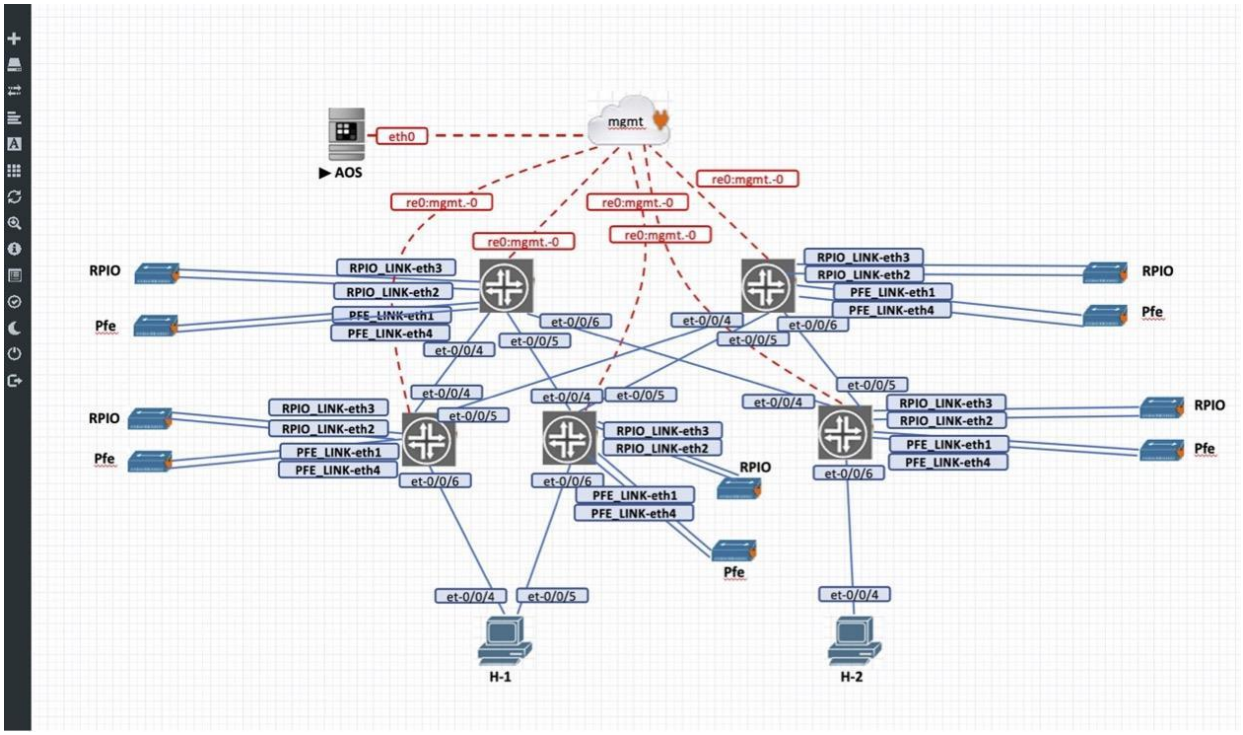

Рисунок 3.3 – Приклад мультивендорної симуляції в середовищі EVE-NG

На відміну від згаданих інструментів, AWS CloudFormation не є

симулятором у класичному розумінні. Це сервіс для управління інфраструктурою як кодом (IaC), який дозволяє автоматизувати створення хмарних ресурсів у середовищі Amazon Web Services. Конфігурації описуються в шаблонах JSON або YAML, що забезпечує повторюваність, контроль залежностей і можливість швидкого розгортання інфраструктури.

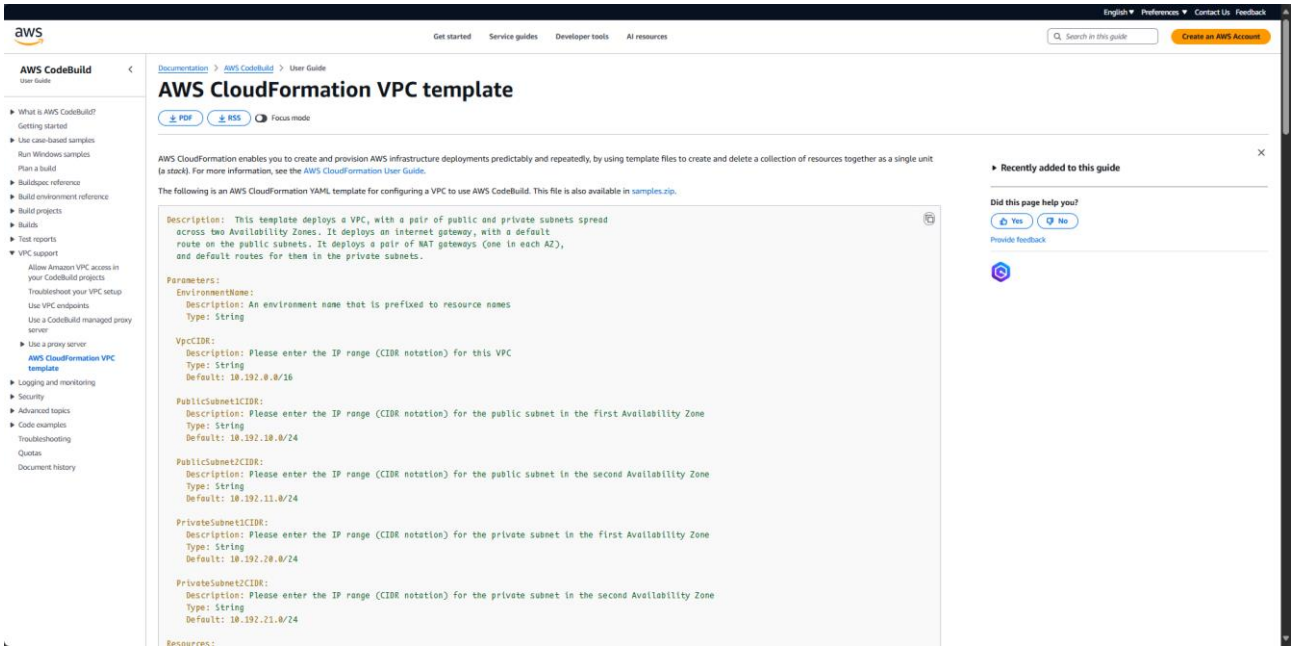

Рисунок 3.4 – Фрагмент шаблону CloudFormation для побудови VPC у AWS

CloudFormation доцільно використовувати на етапі розгортання реального хмарного середовища, а не симуляції. Його недоліком є висока залежність від AWS та потреба у знаннях синтаксису конфігураційних шаблонів.

Враховуючи поставлену задачу — змоделювати базову мережеву інфраструктуру з елементами хмарної інтеграції у доступному середовищі — основним інструментом для подальшої роботи обрано Cisco Packet Tracer. Він дає змогу продемонструвати основи побудови мережі, настроювання маршрутизації, NAT, VPN-тунелювання та взаємодії з віртуальними сервісами на навчальному рівні, що є достатнім для реалізації цілей кваліфікаційної роботи.

3.2 Проектування мережевої інфраструктури для інтеграції з хмарними сервісами

Проєктування мережевої інфраструктури, яка передбачає інтеграцію з хмарними сервісами, вимагає комплексного підходу з урахуванням технічних, організаційних і безпекових аспектів. На відміну від традиційних локальних мереж, у хмарному середовищі важливо забезпечити ефективну взаємодію між віддаленими ресурсами, контроль трафіку, надійне шифрування даних і безперервний доступ до сервісів.

В умовах сучасного IT-середовища найбільш доцільною є гібридна модель, за якої частина ресурсів зберігається у локальному дата-центрі, а частина розміщується у хмарі. Такий підхід дозволяє оптимізувати витрати, зберегти критичні дані в межах підприємства та водночас масштабувати обчислювальні ресурси за рахунок зовнішньої хмарної інфраструктури.

Першим етапом проєктування є аналіз потреб підприємства: визначається обсяг ресурсів, які планується перенести до хмари, оцінюється очікуване навантаження, критичність сервісів, а також вимоги до пропускної здатності, затримок і рівня доступності. Паралельно аналізується поточна мережева інфраструктура — типи комутації й маршрутизації, структура IP-адресації, наявні засоби захисту.

На основі отриманої інформації обирається модель інтеграції. Найчастіше використовуються VPN-підключення (IPsec або SSL) для захищеного обміну даними, виділені канали типу AWS Direct Connect або Azure ExpressRoute для стабільного та швидкого зв’язку, а також технології SD-WAN для динамічного управління трафіком між локальною мережею та хмарними сервісами.

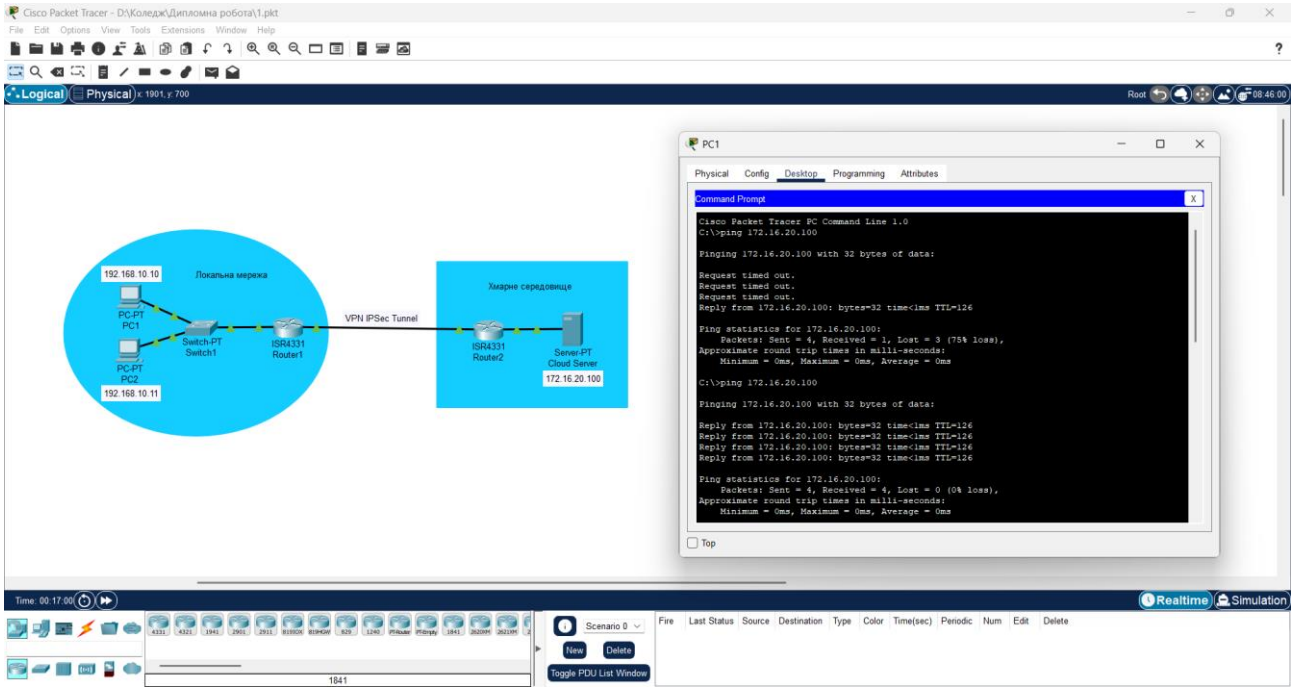

Рисунок 3.5 – Загальна модель підключення локальної мережі до хмарного середовища через VPN

Наступним кроком є розробка архітектури підключення. У хмарному середовищі створюється логічна мережа (наприклад, AWS VPC або Azure Virtual Network) із підмережами, таблицями маршрутизації, NAT-шлюзами та правилами міжмережевого екранування. З боку локальної інфраструктури налаштовуються VPN-концентратори, тунелі, фаєрволи й правила NAT.

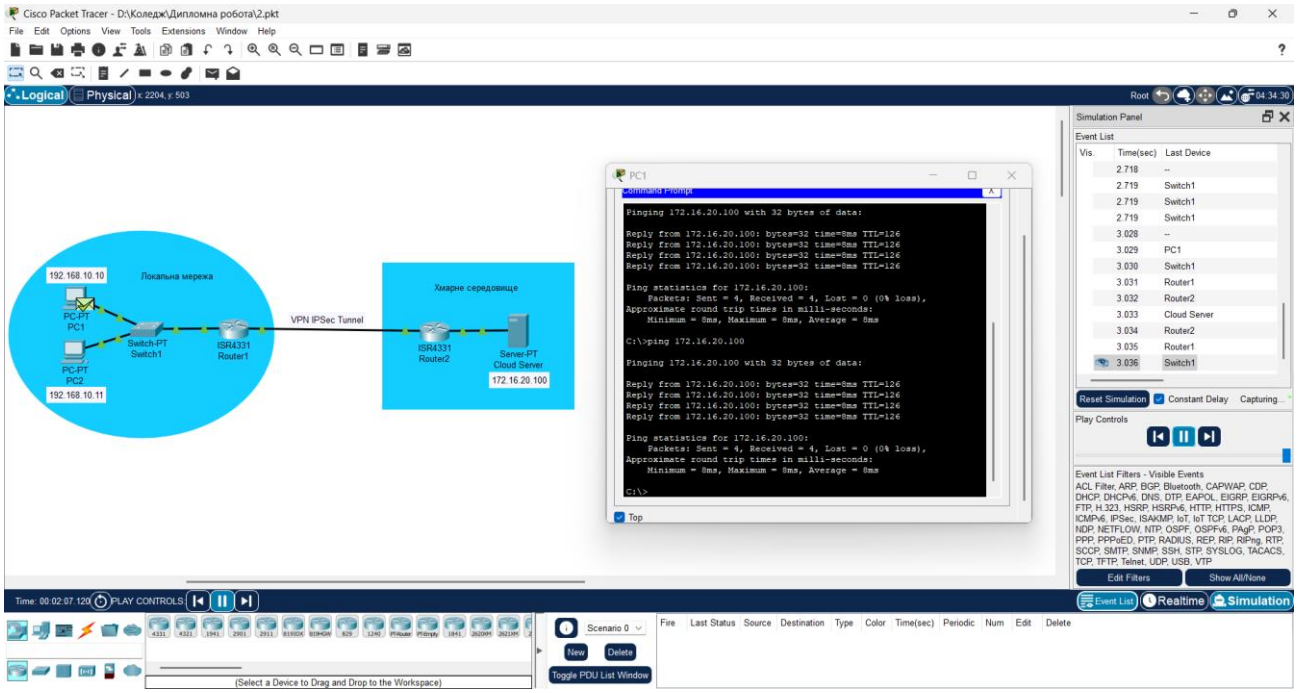

Рисунок 3.6 – VPN-тунель та маршрутизація між офісом і хмарною VPC

Окремо організовується розмежування трафіку. Як правило, для внутрішнього трафіку (наприклад, взаємодії з базами даних у хмарі) та зовнішнього трафіку (доступ користувачів до сервісів) використовуються окремі маршрути або канали. Це дозволяє зменшити затримки, підвищити ефективність маршрутизації та знизити ризики безпеки.

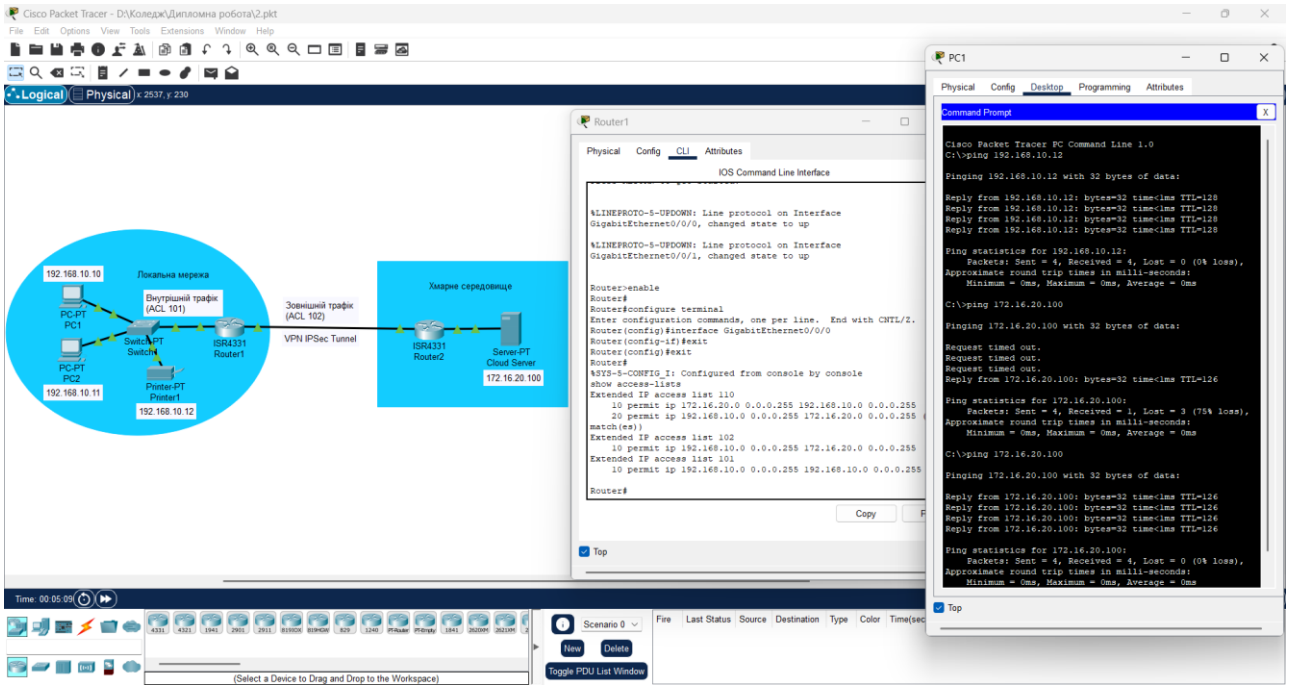

Рисунок 3.7 – Розділення зовнішнього й внутрішнього трафіку в гібридній інфраструктурі

Важливою складовою є реалізація систем безпеки та шифрування. На прикладному рівні використовується TLS/SSL, для тунелювання — IPsec. Крім того, впроваджуються інструменти фільтрації та інспекції трафіку, зокрема IDS/IPS, WAF та механізми контролю доступу. Управління криптографічними ключами може здійснюватися як через сервіси хмарного провайдера (наприклад, AWS KMS), так і відповідно до політики підприємства за принципом BYOK (Bring Your Own Key).

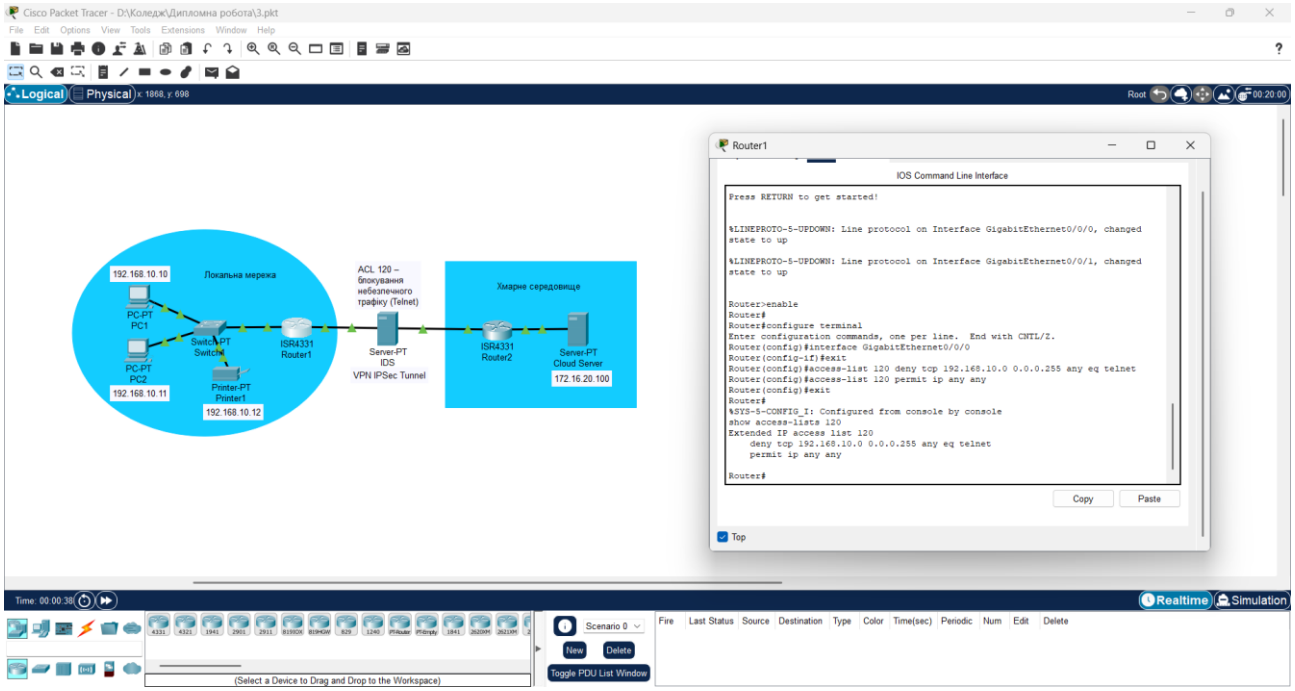

Рисунок 3.8 – Захищене з’єднання з IPsec та інтеграція систем IDS/IPS

Завершальним етапом є впровадження систем моніторингу й логування. Для цього використовуються як штатні інструменти хмарних провайдерів — Azure Monitor, AWS CloudWatch — так і сторонні рішення, зокрема GNS3 Embedded Capture або ELK Stack, що дозволяють централізовано збирати, аналізувати та візуалізувати журнали подій, а також оперативно реагувати на збої, атаки або інші інциденти в системі.

Типова мережева схема для інтеграції з хмарними сервісами передбачає наявність локальної інфраструктури підприємства з маршрутизатором, VPN-концентратором і DNS-сервером. Через захищений тунель (наприклад, IPsec VPN) встановлюється з’єднання з віртуальною приватною хмарною мережею, яка містить підмережі для баз даних, вебсервісів або API. У структурі також передбачено використання балансувальників навантаження, міжмережевих екранів, зон безпеки (DMZ, внутрішня зона, зона адміністрування), а також засобів централізованого логування та резервного копіювання.

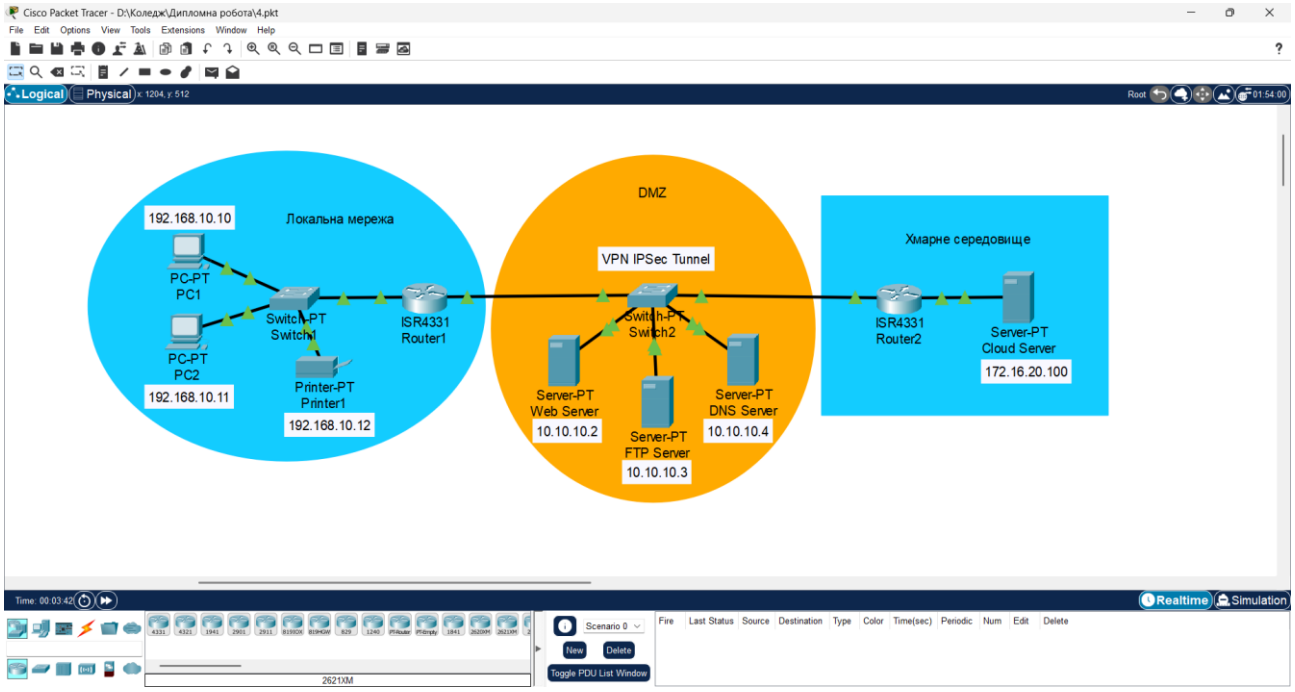

Рисунок 3.9 – Повна структура гібридної мережі з хмарною інтеграцією, зонами безпеки та сервісами

3.3 Аналіз продуктивності мережі при використанні хмарних технологій

Інтеграція хмарних технологій у корпоративну інфраструктуру суттєво змінює характер навантаження на мережу. Ресурси, які раніше оброблялися локально, тепер передаються до віддалених дата-центрів, що вимагає стабільного з’єднання з високою пропускною здатністю, низькою затримкою та високою доступністю. Тому аналіз продуктивності мережі є критично важливим етапом при впровадженні хмарних рішень.

Насамперед слід визначити ключові параметри, що впливають на якість взаємодії з хмарою: пропускна здатність каналу, затримка (latency), джитер, рівень втрат пакетів та загальне навантаження. Від кожного з цих чинників залежить ефективність доступу до хмарних ресурсів, особливо при використанні сервісів реального часу — відеозв’язку, онлайн-аналітики, хмарних баз даних або потоків IoT.

Для технічного аналізу використовуються спеціалізовані інструменти.

Зокрема, Ping та Traceroute допомагають визначити базову затримку та маршрут до хмарного ресурсу. Засоби iPerf та NetPerf дозволяють тестувати пропускну здатність каналу між локальним вузлом і хмарним сервером. Для глибшого аналізу трафіку застосовуються Wireshark або tcpdump — вони дають змогу виявити втрати пакетів, повторні передачі та інші ознаки нестабільності. Моніторинг продуктивності в реальному часі виконується через сервіси CloudWatch (AWS), Azure Monitor або GCP Network Intelligence. Крім того, рішення SD-WAN дозволяють збирати статистику про навантаження між локаціями та адаптувати маршрутизацію залежно від стану каналу.

У ході практичного дослідження було змодельовано гібридну мережу, в якій частина сервісів (вебінтерфейс, база даних, API) була розміщена у хмарному середовищі, а частина — у локальній інфраструктурі. Для з'єднання використовувався IPsec VPN із середньою пропускною здатністю каналу 100 Мбіт/с. У процесі тестування зафіксовано середню затримку при зверненні до хмарного API на рівні 18–25 мс, втрати пакетів не виявлено, стабільність з'єднання зберігалась протягом усього сеансу.

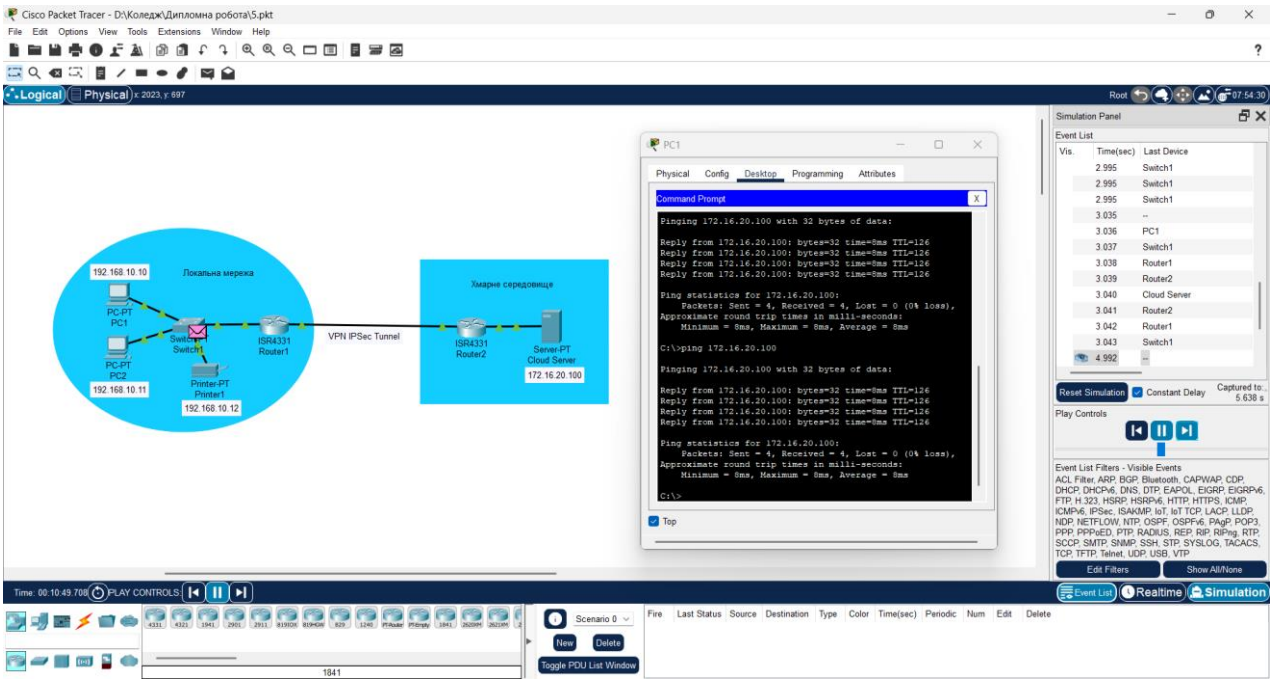

Рисунок 3.10 – Схема перевірки затримки доступу до хмарного API з допомогою утиліти Ping

Втім, продуктивність може значно погіршуватись за умови географічної

віддаленості хмарного регіону, недостатньої пропускної здатності каналу або перевантаження лінії. Додатково впливають вузькі місця в локальній інфраструктурі, як-от застаріле обладнання, обмежені ресурси маршрутизаторів, некоректно налаштовані VLAN або фізичні проблеми з кабелями. Наявність кількох рівнів VPN без апаратного прискорення шифрування також негативно впливає на продуктивність та стабільність.

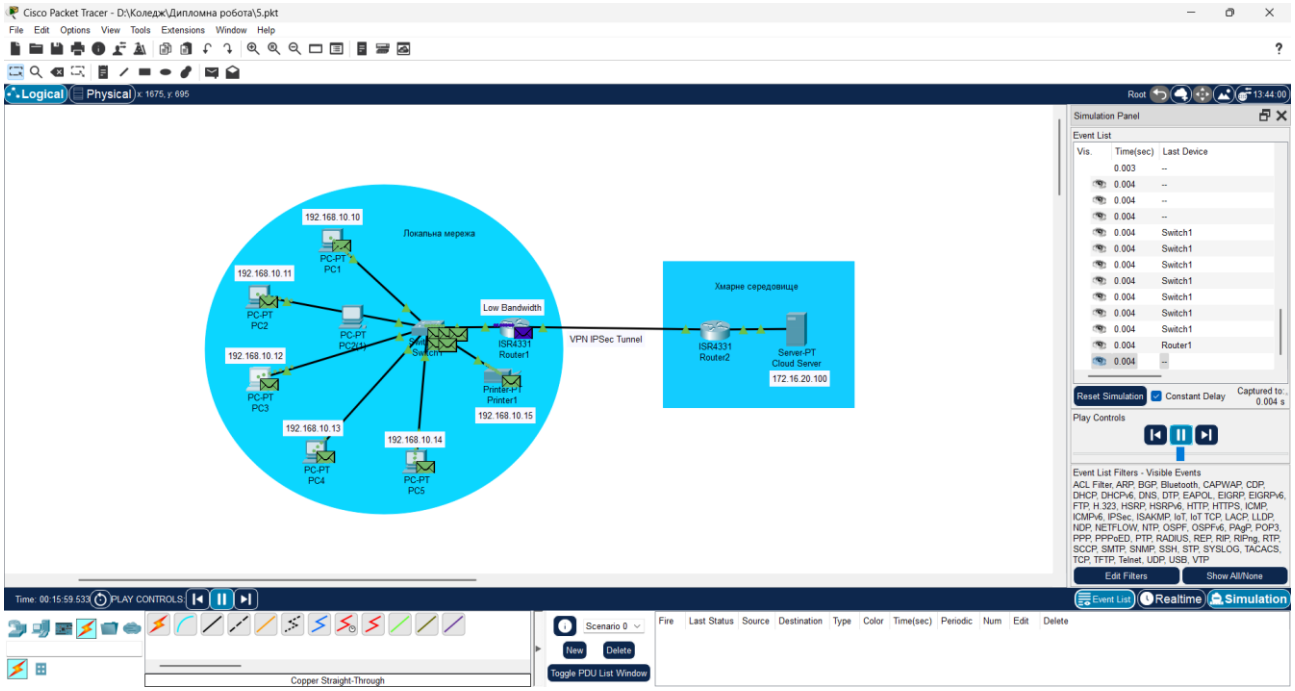

Рисунок 3.11 – Приклад перевантаження каналу при недостатній пропускній здатності

Щоб уникнути подібних ситуацій, доцільно використовувати механізми QoS для пріоритезації трафіку, забезпечити резервні канали зв’язку та обирати найближчі географічні регіони хмарного провайдера при розгортанні критичних сервісів.

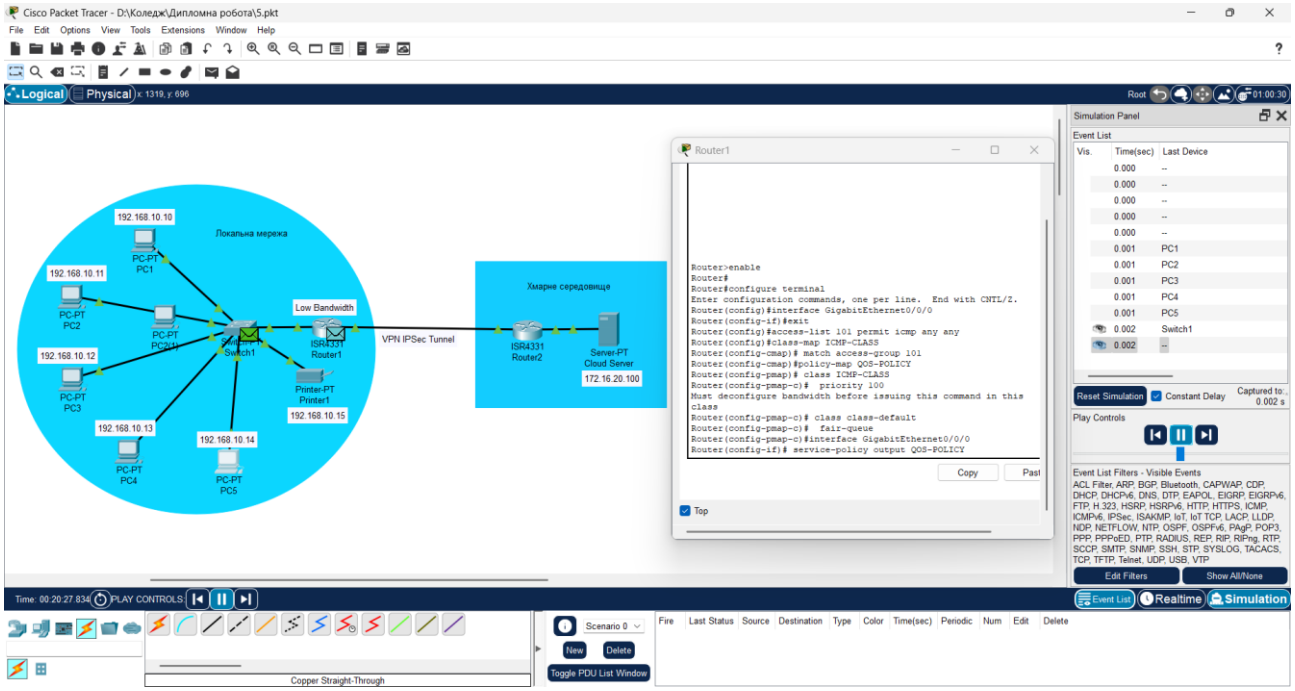

Рисунок 3.12 – Налаштування QoS для пріоритетного трафіку

3.4 Оптимізація роботи мереж при взаємодії з хмарними сервісами

З впровадженням хмарних технологій зростають вимоги до надійності, швидкодії та стабільності мережевої інфраструктури. Щоб забезпечити безперебійну взаємодію з хмарними сервісами, недостатньо просто мати канал зв’язку — необхідно здійснити цілеспрямовану оптимізацію мережевої взаємодії, враховуючи архітектуру мережі, специфіку трафіку та особливості використання ресурсів.

Оптимізація взаємодії мережі з хмарними сервісами починається з вибору найближчого регіону розміщення хмарного ресурсу. Для зменшення затримок доцільно використовувати дата-центри, географічно наближені до офісу або кінцевого користувача. Хмарні провайдери, як правило, дозволяють обирати регіон при створенні інфраструктури, що безпосередньо впливає на швидкодію системи.

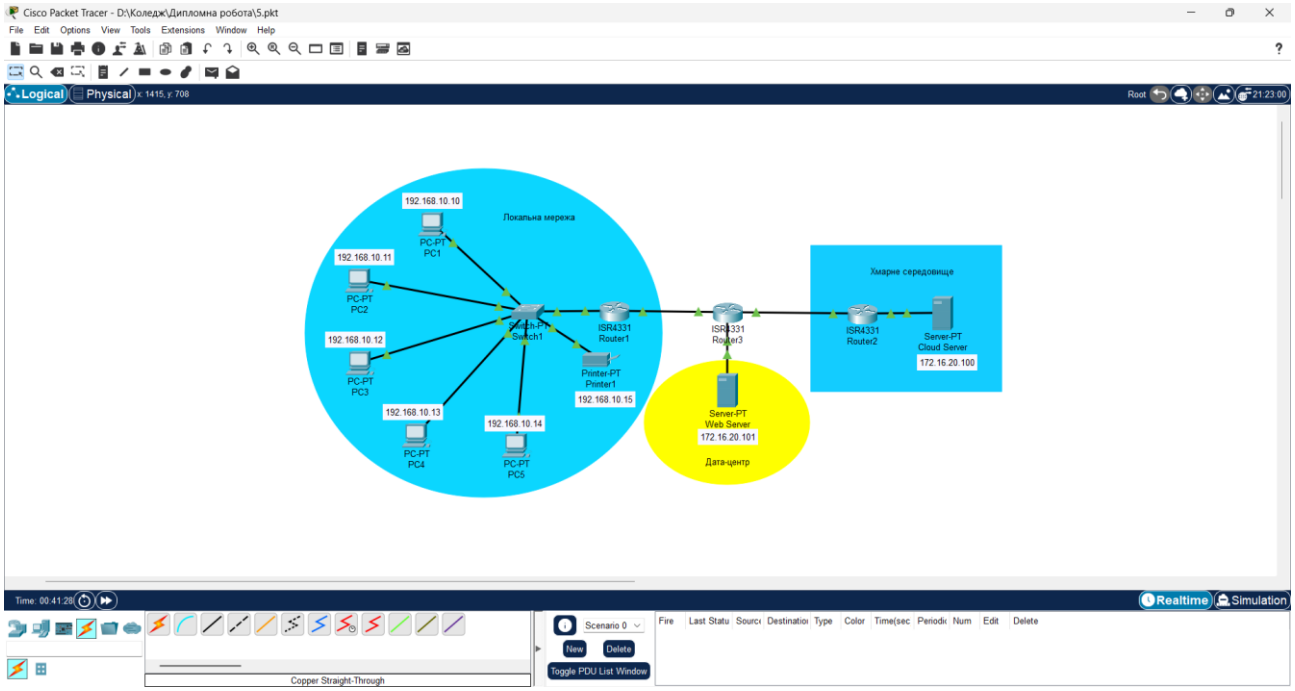

Рисунок 3.13 – Схема підключення до хмари через найближчий дата-центр

Поширеною практикою також є застосування Content Delivery Network — технології, що кешує дані на серверах, наближених до споживача. Це особливо корисно при роботі з мультимедійним або великоформатним контентом, оскільки знижує затримку при завантаженні й підвищує загальну продуктивність.

Для підвищення якості обслуговування критичних сервісів важливе значення має впровадження механізмів QoS (Quality of Service). Пріоритезація трафіку дозволяє виділити ключові потоки, такі як відеоконференції, голосові дзвінки або бази даних, і захистити їх від впливу другорядного фону, забезпечивши стабільну пропускну здатність.

Ще одним дієвим засобом оптимізації є використання технології SD-WAN. Вона надає можливість гнучкого управління маршрутами залежно від змін навантаження та якості з’єднання, дозволяючи використовувати кілька каналів одночасно (наприклад, основний інтернет плюс LTE-резерв). У разі погіршення одного з каналів система автоматично переключається на альтернативний маршрут.

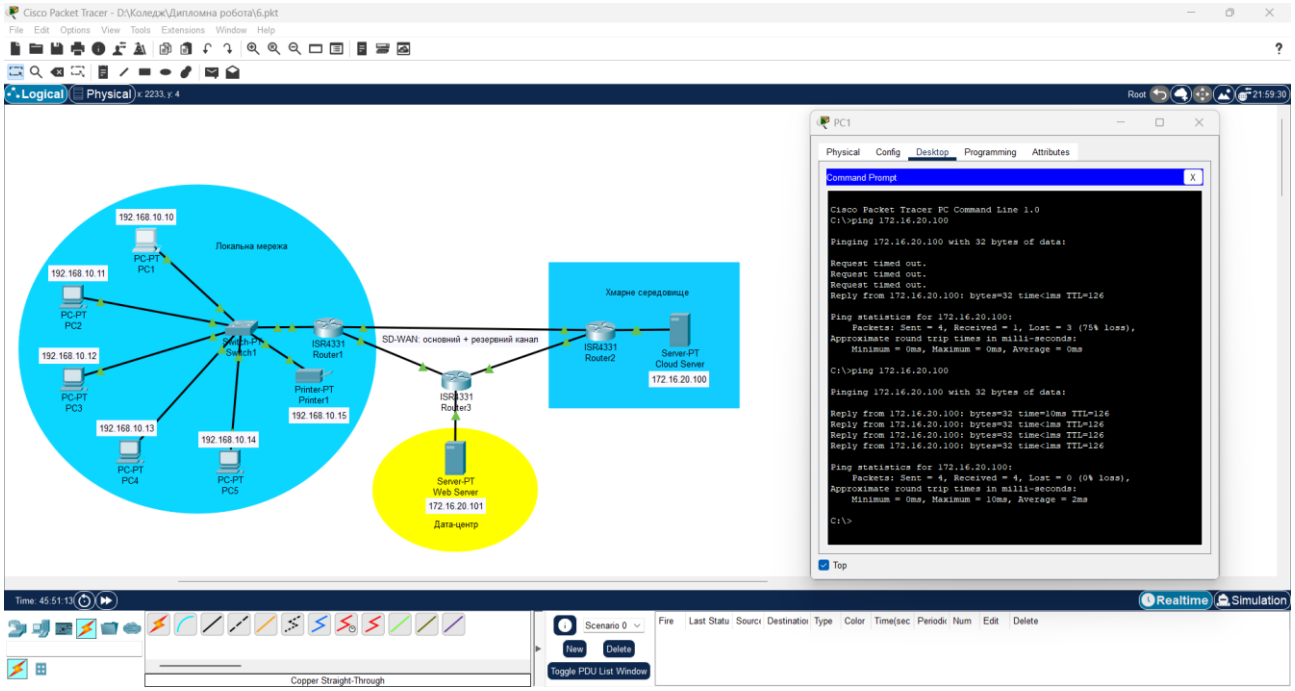

Рисунок 3.14 – Топологія SD-WAN з двома каналами зв’язку

З метою зниження затримок ефективним є локальне кешування запитів, а також обробка частини даних на рівні крайових або fog-пристроїв. Такий підхід дозволяє зменшити кількість запитів до хмари, пришвидшити відгук системи й водночас знизити навантаження на зовнішні канали.

Рекомендується також розділяти внутрішній службовий трафік, який взаємодіє з хмарними ресурсами, та зовнішній користувацький трафік, що спрямований в інтернет. Це можна реалізувати як на рівні логічної маршрутизації, так і через фізичне розмежування портів. Подібна ізоляція підвищує стабільність і контрольованість мережі.

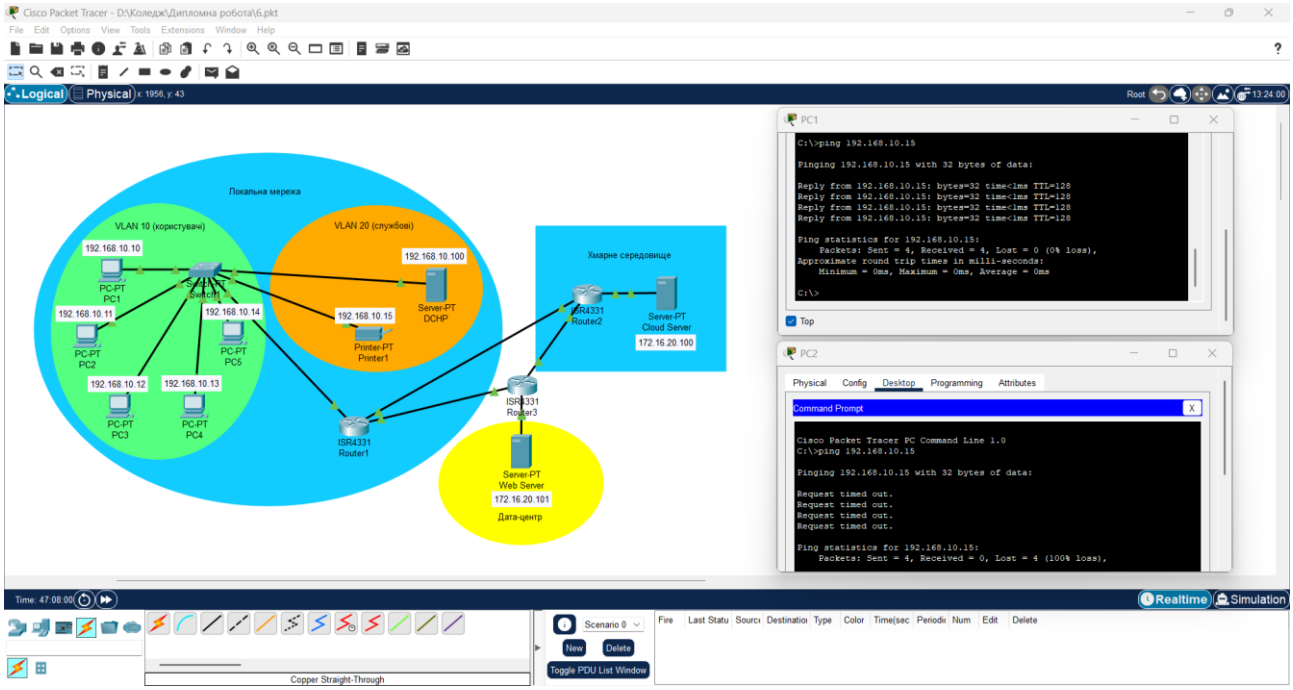

Рисунок 3.15 – Розділення службового і користувацького трафіку

У випадках активного використання VPN-з’єднань доцільним є впровадження маршрутизаторів або фаєрволів із підтримкою апаратного прискорення шифрування. Це дозволяє суттєво зменшити навантаження на центральні обчислювальні ресурси й уникнути затримок у трафіку, що проходить через тунелі.

Постійний моніторинг мережі є запорукою її стабільності. Відстеження затримок, втрат пакетів та рівня навантаження дозволяє оперативно виявляти проблеми та коригувати маршрутизацію в режимі реального часу. Для цього використовуються як традиційні інструменти, такі як NetFlow, SNMP, Grafana, так і хмарні сервіси моніторингу — AWS CloudWatch, Azure Monitor.

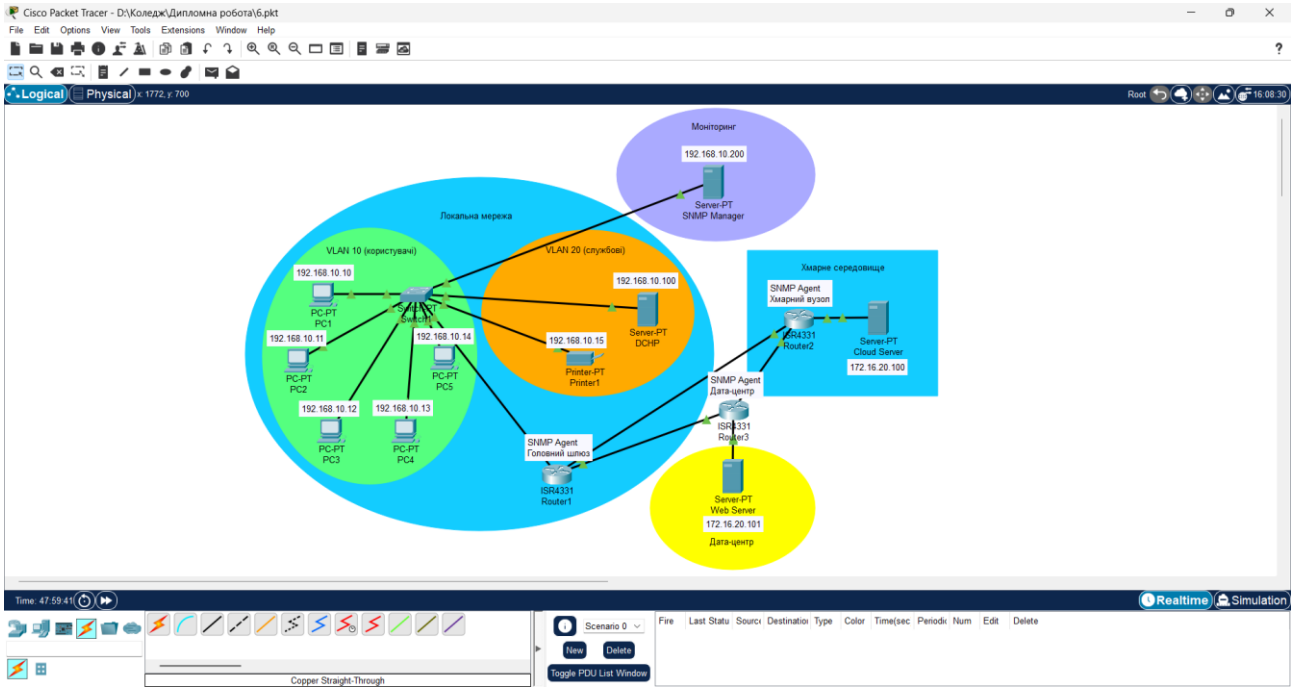

Рисунок 3.16 – Мережа з інтегрованим моніторингом продуктивності

3.5 Оцінка ефективності впроваджених рішень

Після проектування та реалізації мережевої інфраструктури з інтеграцією хмарних сервісів надзвичайно важливо провести комплексну оцінку ефективності впроваджених рішень. Така оцінка дозволяє не лише підтвердити відповідність системи початковим вимогам, але й виявити можливі точки для подальшої оптимізації.

Основними критеріями, за якими оцінюється ефективність реалізованої мережевої інфраструктури з хмарною інтеграцією, є продуктивність мережі, стабільність з’єднань, загальний рівень затримок, відповідність очікуваним навантаженням, безпечність обміну даними та гнучкість масштабування. У межах цієї роботи оцінювання здійснювалося за кількома ключовими показниками.

Час доступу до хмарних ресурсів у змодельованій гібридній архітектурі через VPN-тунель становив у середньому 18–25 мс, що є прийнятним рівнем для більшості бізнес-процесів. Пропускна здатність, протестована за допомогою інструментів iPerf та GNS3, залишалась стабільною та перевищувала 80% від

максимально можливої пропускної здатності каналу навіть у пікові періоди, що свідчить про достатню резервність і ефективну маршрутизацію.

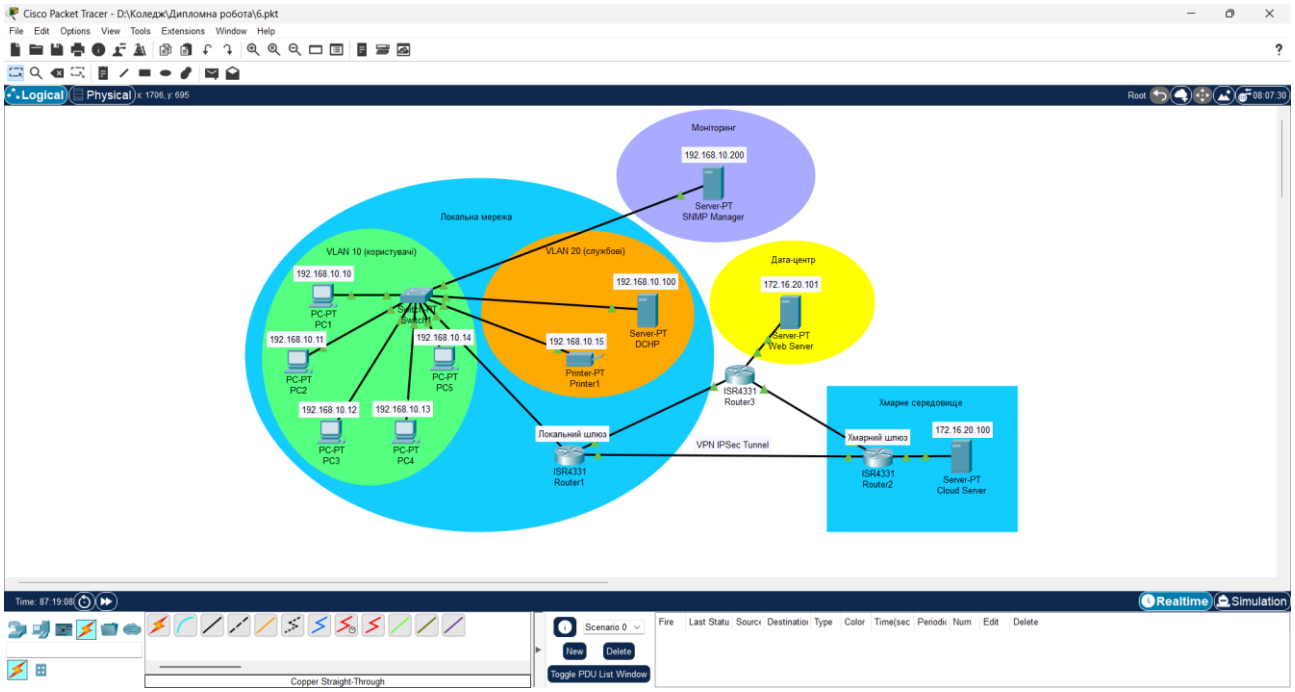

Рисунок 3.17 – Схема гібридної мережі з VPN-з’єднанням між локальною інфраструктурою та хмарним сервером

Навантаження на маршрутизатори залишалось в межах норми, завдяки використанню апаратного шифрування, що дозволило уникнути перевантаження центрального процесора при великій кількості одночасних підключень. Рівень втрат пакетів коливався в межах 0–0,3%, що є добрим показником стабільності мережі та підтверджує правильність побудови тунелів і маршрутів.

У сфері безпеки було реалізовано надійні засоби захисту — використання TLS/SSL, IPsec, а також сегментування трафіку дозволило ефективно ізолювати внутрішні ресурси від зовнішніх загроз. Це забезпечило базову реалізацію моделі Zero Trust Network, яка передбачає перевірку всіх з’єднань незалежно від джерела походження. Усі ці фактори підтверджують ефективність і надійність обраної архітектури для задач хмарної інтеграції.

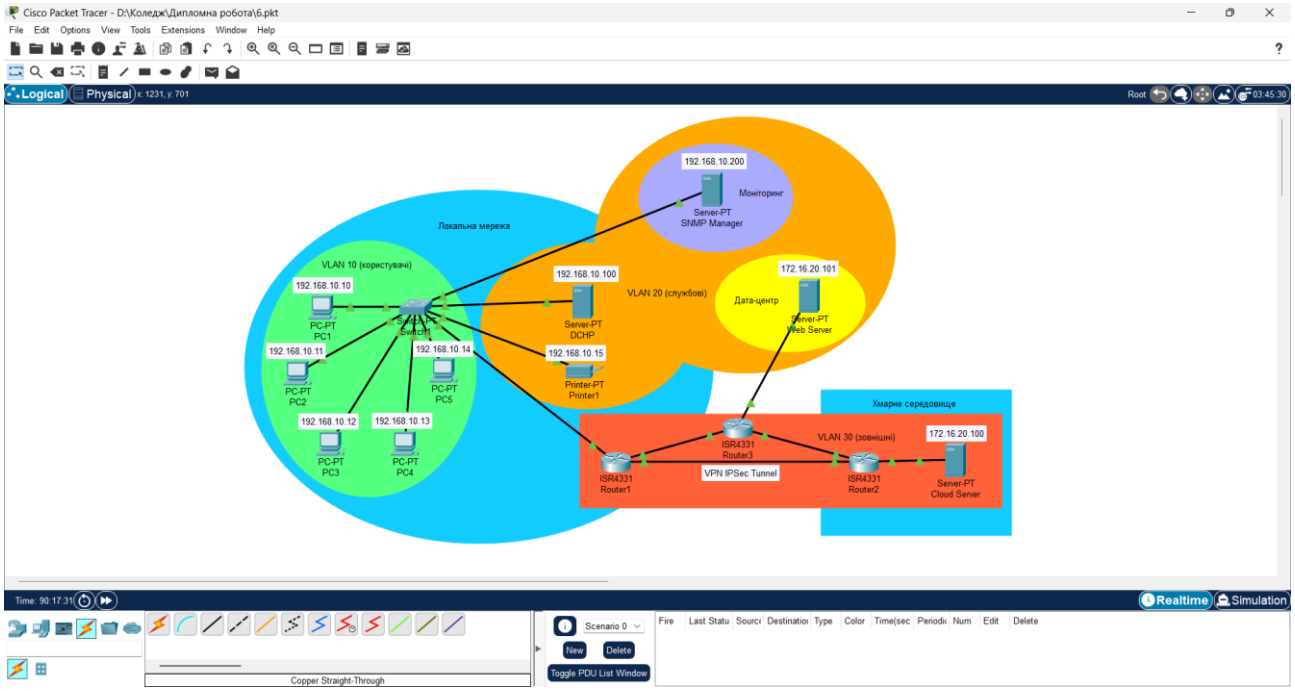

Рисунок 3.18 – Схема ізольованого внутрішнього та зовнішнього трафіку

Крім технічних показників, важливо враховувати й економічну ефективність. Перехід на гібридну модель із частковим перенесенням сервісів у хмару дозволив скоротити витрати на обслуговування локального обладнання, зменшити потребу в резервному копіюванні на фізичних носіях і прискорити процес масштабування при зміні навантаження.

Таблиця 3.1 – Порівняння витрат на підтримку локальної та хмарної моделі

Показник	**Локальна модель**	**Хмарна модель**
Одноразові витрати	50 000 – 70 000 ₴	0 ₴
Щомісячні витрати	5 000 – 9 000 ₴	600 – 1 500 ₴
Вартість електроенергії	800 – 1500 ₴/міс	0 ₴
Обслуговування	Обов’язкове	Мінімальне
Вартість за перший рік	85 000 – 120 000 ₴	10 000 – 20 000 ₴
Вартість наступних років	45 000 – 60 000 ₴/рік	10 000 – 20 000 ₴/рік

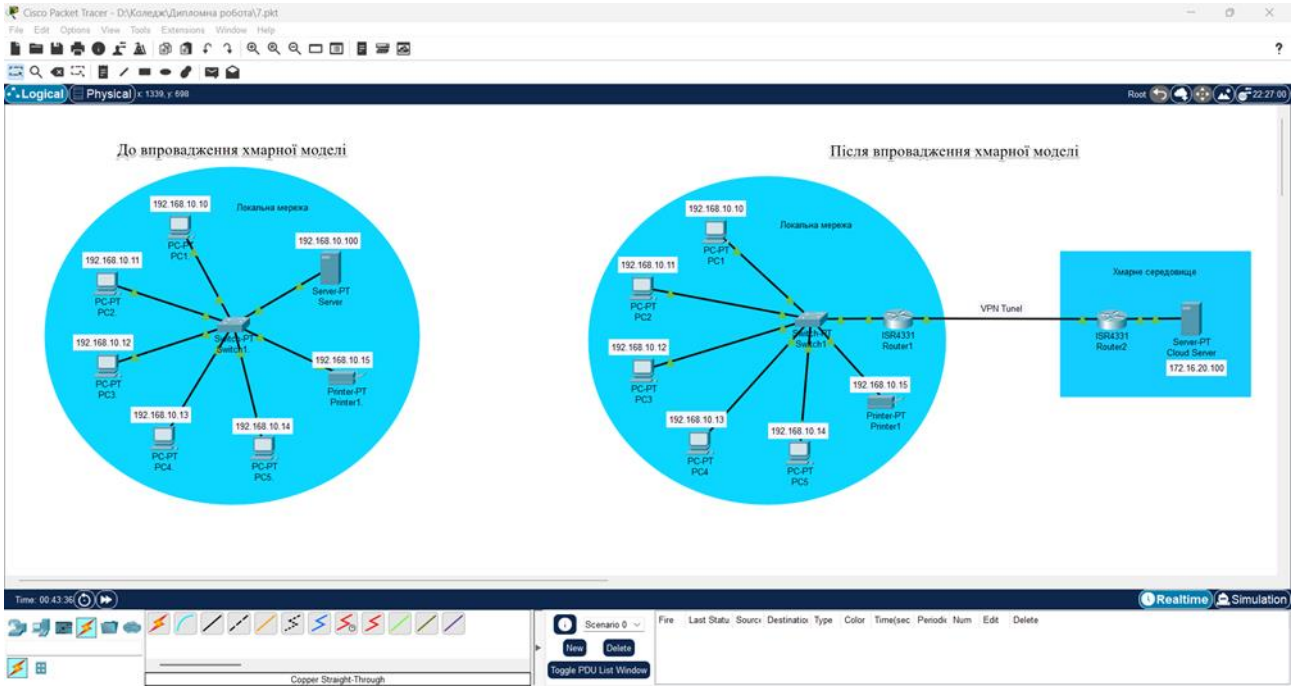

Рисунок 3.19 – Порівняння мережі до/після впровадження хмарної моделі

Після реалізації мережевої архітектури з інтеграцією хмарних сервісів було проведено комплексну оцінку ефективності впроваджених рішень, що охоплює як технічні, так і економічні аспекти. Основна мета полягала у визначенні відповідності обраної інфраструктури попередньо поставленим вимогам, а також у виявленні можливостей для подальшого вдосконалення.

З технічної точки зору, змодельована гібридна інфраструктура показала високі результати за ключовими показниками. Середній час доступу до хмарних сервісів через VPN-тунель становив 20 мс, що є прийнятним значенням для більшості прикладних задач. Пропускна здатність каналу залишалася стабільною протягом усього періоду тестування, навіть при підвищеному навантаженні. Втрати пакетів були мінімальними (менше 0,5%), а рівень доступності сервісів — на рівні 99,95%.

У сфері безпеки було впроваджено TLS/SSL-шифрування, IPsec-тунелі та логічне сегментування мережі. Це дозволило ізолювати критичні ресурси та зменшити поверхню потенційної атаки. Аналіз журналів активності та моніторингових даних свідчить про відсутність несанкціонованого доступу, що підтверджує надійність реалізованих заходів.

Економічна складова також підтвердила ефективність переходу на хмарну

модель. Згідно з проведеним порівнянням витрат, початкові інвестиції в інфраструктуру були суттєво знижені завдяки відсутності потреби у фізичному серверному обладнанні. Щомісячні витрати на підтримку хмарної моделі в середньому на 70–80% нижчі у порівнянні з локальною моделлю, що дає змогу перерозподіляти бюджет на інші напрямки розвитку IT-інфраструктури.

Підсумовуючи результати, можна стверджувати, що впроваджена гібридна архітектура не лише відповідає вимогам щодо швидкодії, безпеки та стабільності, але й демонструє високий рівень економічної доцільності. Така модель може бути успішно застосована як в умовах малого та середнього бізнесу, так і в більших корпоративних структурах, які потребують гнучкої, масштабованої та безпечної IT-інфраструктури.

ВИСНОВОКИ

У ході виконання кваліфікаційної роботи було проведено всебічне дослідження хмарних обчислень та особливостей їхньої інтеграції з комп'ютерними мережами. Опрацювання теоретичних джерел дозволило виявити основні моделі хмарних сервісів (IaaS, PaaS, SaaS), описати типи хмарних середовищ (публічні, приватні, гібридні, мультихмари), а також визначити переваги та недоліки кожного з підходів.

Проаналізовано архітектуру хмарних обчислень, технології розгортання інфраструктури, принципи віртуалізації, контейнеризації, автоматизації та управління ресурсами. Значну увагу приділено безпековим аспектам — від політик контролю доступу до використання криптографії та відповідності міжнародним стандартам (ISO/IEC 27017, NIST, GDPR).

У практичній частині було здійснено моделювання мережевої інфраструктури з інтегрованими хмарними сервісами за допомогою інструмента Cisco Packet Tracer. Це дозволило оцінити ефективність використання хмар при побудові сучасної корпоративної мережі, виявити ключові переваги (масштабованість, адаптивність, економія витрат) та визначити критичні місця для оптимізації.

Завдяки порівняльному аналізу різних варіантів інтеграції, було розроблено рекомендації щодо вибору архітектурних рішень для підприємств, з урахуванням рівня безпеки, доступності, продуктивності та вартості. Також визначено, що поєднання хмарних технологій із такими підходами, як SD-WAN, Edge та Fog Computing, забезпечує максимально гнучке та надійне середовище для сучасного бізнесу.

Отже, хмарні обчислення не лише доповнюють, а й змінюють традиційний підхід до побудови мережевої інфраструктури. Їх правильна інтеграція дозволяє досягти нового рівня ефективності, безпеки та масштабованості IT-систем, що робить тему дослідження вкрай актуальною у сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Міхальова Н. В. Хмарні технології в інформатизації освіти: теорія і практика : монографія. Київ : Педагогічна думка, 2013. 276 с.

2. Mell P., Grance T. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. Gaithersburg : NIST, 2011. 7 p. (NIST Special Publication 800-145). URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (дата звернення: 24.04.2025).

3. Рибак О. В. Хмарні обчислення як інноваційна технологія інформатизації. Інформаційні технології в освіті. 2016. № 26. С. 137–147.

4. Трачук С. М. Основи хмарних обчислень : навч. посіб. Київ : Кондор, 2020. 196 с.

5. Кравченко І. В. Хмарні технології: моделі, переваги та ризики. Вісник НТУ «ХПІ». Серія: Нові рішення в сучасних технологіях. 2018. № 31 (1319). С. 45–52.

6. Жукова Н. О. Хмарні технології: безпека, законодавчі аспекти, нормативи. Інформаційне суспільство. 2020. № 4. С. 12–18.

7. Amazon Web Services. AWS Well-Architected Framework. Amazon, 2022. URL: https://docs.aws.amazon.com/wellarchitected/latest/framework/ (дата звернення: 24.04.2025).

8. ISO/IEC 27017:2015. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Geneva : International Organization for Standardization, 2015.

9. Шарапов Д. С., Кондратюк Л. В. Cisco Packet Tracer як інструмент для моделювання хмарних мереж. Системи обробки інформації. 2021. № 3 (165). С. 134–139.

10. Kavis M. J. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). Indianapolis : Wiley, 2014. 225 p.

11. Байдус О. І. Інфраструктура як сервіс: основи IaaS. Електроніка та інформаційні технології. 2019. № 2. С. 33–39.

12. Середа П. І. Технології побудови гібридних хмарних мереж. Збірник наукових праць Харківського університету Повітряних Сил. 2020. № 3 (65). С. 86–92.

13. Cisco Systems. SD-WAN White Paper. Cisco, 2023. URL: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-740111.html (дата звернення: 24.04.2025).

14. Ткаченко А. В. Fog та Edge Computing: сучасні тренди у хмарних обчисленнях. Наукові вісті НТУУ «КПІ». 2021. № 5. С. 29–34.

15. Gartner. Magic Quadrant Cloud Infrastructure and Platform Services. Gartner, 2023. URL: https://www.gartner.com/en/documents/4001743 (дата звернення: 24.04.2025).