ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «**ПРОЕКТУВАННЯ МАСШТАБОВАНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ВЕЛИКОГО ПІДПРИЄМСТВА ЗА ДОПОМОГОЮ СИСТЕМИ МЕРЕЖЕВОГО УПРАВЛІННЯ.**»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми _____
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ _____
(підпис) *(ім'я, ПРІЗВИЩЕ здобувача)*

Виконав: здобувач вищої освіти гр. КСДМ-62
Сергій МИРОНОВ
(Ім'я, ПРІЗВИЩЕ)

Керівник: кандидат технічних наук, доцент Артем АНТОНЕНКО
науковий ступінь, вчене звання (Ім'я, ПРІЗВИЩЕ)

Рецензент: _____
науковий ступінь, (Ім'я, ПРІЗВИЩЕ)

Київ 2023

ЗМІСТ

ВСТУП

Актуальність теми: Багато великих підприємств активно впроваджують цифрові технології для підвищення ефективності бізнес-процесів, і мережі виступають ключовим елементом цього процесу. З плином часу обсяги даних на підприємствах значно збільшуються. Проектування масштабованої мережі стає критичним для забезпечення ефективного обміну і обробки даних. З поглибленням цифровізації зростає і загроза кібербезпеки. Важливо мати масштабовану мережу, яка ефективно захищена від потенційних кіберзагроз. Сучасні бізнес-потреби вимагають гнучкості та мобільності в мережевих рішеннях, і масштабовані мережі дозволяють забезпечити ці характеристики. Використання хмарних рішень стає стандартом для багатьох підприємств, і масштабована мережа дозволяє ефективно інтегрувати ці технології. Великі підприємства вимагають від своїх мереж високої доступності для запобігання витратам через відмову систем та втрату продуктивності. Системи мережевого управління дозволяють ефективно керувати ресурсами, моніторити стан мережі та оперативно реагувати на проблеми.

Метою дослідження є розробка та впровадження ефективної масштабованої комп'ютерної мережі для великого підприємства, з використанням системи мережевого управління. Дослідження спрямоване на оптимізацію інфраструктури з метою підвищення продуктивності, безпеки та гнучкості мережевих рішень.

Завдання дослідження:

1. Аналіз потреб та вимог підприємства
2. Визначення технічних вимог
3. Проектування мережі
4. Впровадження та тестування
5. Система мережевого управління
6. Технічна підтримка та навчання персоналу

7. Оцінка ефективності та підготовка звіту

Методи дослідження:

Визначення технічних вимог

Проектування мережі

Впровадження та тестування

Система мережевого управління

Оцінка ефективності та підготовка звіту

Предметом дослідження є процес проектування та впровадження масштабованої комп'ютерної мережі для великого підприємства з використанням системи мережевого управління.

Об'єктом дослідження є велике підприємство, яке потребує модернізації та оптимізації своєї комп'ютерної мережі.

Теоретичне значення: Дослідження дозволить розробити та визначити оптимальні підходи до проектування масштабованих комп'ютерних мереж для великих підприємств. Дослідження може призвести до розробки нових технологій та методів управління, що відповідають сучасним вимогам ефективності та безпеки. Аналіз можливостей масштабованості та їх теоретична обґрунтованість для великих підприємств.

Практичне значення: Розробка ефективної мережі дозволить великим підприємствам оптимізувати бізнес-процеси та підвищити продуктивність. Розробка безпечної мережі сприятиме захисту важливої інформації та запобігатиме кіберзагрозам. Впровадження нової мережі дозволить підприємствам ефективно масштабувати свої операції та адаптуватися до зростаючих потреб. Вивчення ефективних методів навчання та підготовки персоналу для роботи з новою мережею. Визначення оптимальної системи мережевого управління, її впровадження та оптимізація для забезпечення ефективного контролю та моніторингу мережі. Ефективна мережа може служити додатковим ресурсом для підвищення конкурентоспроможності підприємства в сучасному бізнес-середовищі.

Новизна дослідження: Розгляд аспектів проектування мережі, що охоплює технічні, безпекові, організаційні та управлінські аспекти. Поглиблений аналіз ролі та можливостей систем мережевого управління в контексті масштабованих мереж для великих підприємств. Врахування останніх тенденцій у сфері мережевих технологій, таких як SDN (Software-Defined Networking), хмарні рішення та інші інноваційні технології. Розгляд комплексного підходу до забезпечення інформаційної безпеки великої мережі, враховуючи кіберзагрози та сучасні методи захисту. Розробка методів ефективного впровадження нової мережі та системи мережевого управління, а також плану моніторингу та управління. Розробка практичних методів для навчання та підготовки персоналу, спрямованих на забезпечення ефективної експлуатації та технічної підтримки мережі. Визначення нових показників ефективності масштабованих мереж та їх взаємозв'язок з успішністю великого підприємства.

Розділ 1. Аналіз потреб та вимог

1.1 Визначення бізнес-вимог і цілей

Для успішного проектування масштабованої комп'ютерної мережі для великого підприємства необхідно вивчити бізнес-вимоги та цілі організації, оскільки вони слугують основою для розробки оптимального та ефективного рішення. Перший і ключовий етап у цьому процесі - консультації з різними рівнями управління та представниками відділів, що користуються мережею. Під час консультацій з керівництвом підприємства, включаючи топ-менеджмент і керівників відділу IT, основна мета полягає в ретельному зрозумінні поточних вимог та проблем, з якими стикається компанія. Такі зустрічі дозволяють визначити, як саме мережа використовується в рамках бізнес-процесів, і виявити потреби та очікування від нової мережевої інфраструктури. Важливо з'ясувати, які аспекти діяльності підприємства вимагають максимальної продуктивності мережі, які дані та додатки є ключовими для операційного успіху. Консультації також допоможуть виокремити проблеми, які можуть бути пов'язані з поточною мережею: чи вистачає пропускної здатності, чи забезпечена висока доступність, як обстоїть справа з безпекою даних та які інші вимоги висуваються щодо мережевої інфраструктури. Крім того, важливо визначити плани та стратегії розвитку підприємства, оскільки нова мережа повинна бути готовою відповідати вимогам не тільки зараз, але й у майбутньому. Такий підхід дозволяє створити мережеве рішення, що буде гнучким та легко адаптованим до зростаючих потреб та технологічних викликів.[13]

Проведення аналізу бізнес-процесів є необхідним етапом визначення бізнес-вимог та цілей для проектування масштабованої комп'ютерної мережі для великого підприємства. Організаційні процеси, що залежать від мережі, можуть включати різноманітні аспекти, які важливі для функціонування підприємства.

Важливо розібрати, як саме дані бізнес-процеси використовують мережу в своїй роботі. Це може включати обмін великими обсягами даних між різними відділами чи філіями, необхідність надійного спілкування та обміну інформацією між співробітниками, а також зберігання та обробку великих обсягів даних.

Аналізуючи бізнес-процеси, можна визначити, які саме завдання виконує мережа в контексті кожного процесу. Наприклад, у виробничому середовищі це може бути підтримка системи автоматизації виробництва через обмін даними з промисловими контролерами та датчиками. У сфері обслуговування це може бути реалізація безперервного спілкування між різними відділами через віртуальні приватні мережі. Детальний аналіз також дозволить визначити можливості для оптимізації бізнес-процесів через ефективне використання мережевих технологій. Наприклад, впровадження технологій передачі даних в реальному часі може покращити точність та швидкість прийняття управлінських рішень. В цілому, аналіз бізнес-процесів визначає ключові функції мережі в організації і допомагає виокремити основні вимоги до мережевої інфраструктури.[9]

Встановлення вимог є важливим етапом у процесі проектування масштабованої комп'ютерної мережі для великого підприємства. Цей етап визначає конкретні потреби та вимоги, які повинна задовольняти мережа для ефективного функціонування підприємства. Однією з ключових вимог може бути велика пропускна здатність. Підприємствам часто потрібна можливість швидко передавати великі обсяги даних, особливо в умовах активної роботи з мультимедійним контентом, великими базами даних чи іншими великими файлами. Висока доступність є іншою важливою вимогою, оскільки багато бізнес-процесів стають критичними і вимагають неперервного доступу до мережевих ресурсів. Для підприємств, де обмін даними відбувається в режимі реального часу, недоступність мережі може призвести до значних втрат інформації чи навіть призупинення операцій.[17]

Безпека даних є критичною вимогою для будь-якої мережі, особливо для великих підприємств, які обробляють чутливу інформацію. Визначення заходів забезпечення конфіденційності, цілісності та доступності даних є важливим елементом проектування мережі. Гнучкість для майбутнього розширення також стає вимогою в сучасних умовах бізнесу, оскільки підприємства постійно змінюються та розширюються. Мережа повинна бути здатною легко адаптуватися до зростаючих потреб, нових технологій та розширення бізнес-функцій. Встановлення чітких вимог допомагає створити фундаментальну основу для подальшого проектування та впровадження мережі, яка відповідає специфічним потребам та стратегічним цілям підприємства.[24]

Формулювання цілей у контексті проектування масштабованої комп'ютерної мережі для великого підприємства є важливим етапом, що визначає конкретні показники та напрямки розвитку мережі для досягнення бізнес-вимог. Ці цілі визначають кінцеві результати, які повинна забезпечити мережа для успішного функціонування підприємства.

На основі зібраних вимог формулюються конкретні, вимірювані та досяжні цілі. Наприклад, якщо однією з вимог є велика пропускна здатність, то ціль може бути визначена як підвищення швидкості передачі даних на певний відсоток, наприклад, на 50%. Іншою можливою ціллю може бути зменшення часу відновлення мережі в разі відмови. Це може бути особливо важливим для уникнення перерв у роботі та мінімізації втрат при виникненні непередбачених ситуацій. Забезпечення високого рівня безпеки даних може бути ще однією ключовою ціллю. Наприклад, встановлення стандартів безпеки на рівні банківських вимог може гарантувати захист конфіденційної інформації підприємства. Цілі також можуть стосуватися аспектів ефективності та продуктивності, таких як оптимізація роботи мережі, покращення часу реакції та надійність системи. Кожна ціль повинна бути чітко визначена, а її досягнення повинно вносити значний внесок у покращення функціонування мережі та підтримку бізнес-процесів підприємства.[29]

При врахуванні майбутнього розвитку на етапі формулювання цілей для проектування масштабованої комп'ютерної мережі великого підприємства вирізняється стратегічний підхід, спрямований на створення мережевої інфраструктури, яка залишатиметься актуальною та ефективною на тривалий період.

Врахування майбутніх потреб передбачає аналіз тенденцій розвитку бізнес-середовища та технологічних інновацій. Зокрема, дослідження перспективних технологій, таких як Інтернет речей (IoT), штучний інтелект (AI), розширена реальність (AR) та інші, може сприяти побудові мережі, яка буде здатна інтегрувати нові функції та обслуговувати зростаючі потреби.

Сучасний бізнес швидко змінюється, і, отже, важливо враховувати не тільки поточні, але й очікувані зміни в організаційній структурі та бізнес-процесах підприємства. Мережа повинна бути побудована так, щоб вона легко адаптувалася до розвитку нових напрямків бізнесу та змін внутрішньої структури компанії. Крім того, при врахуванні майбутнього розвитку важливо визначити плани на розширення та модернізацію інфраструктури. Це може включати у себе здатність мережі масштабуватися відносно розширення бізнесу, підтримку нових локацій та філій, а також готовність до інтеграції нових технологій. Такий довгостроковий підхід дозволяє збудувати мережу, яка не тільки задовольняє поточні потреби підприємства, але й залишається гнучкою та готовою до еволюції відповідно до стратегічних напрямків розвитку бізнесу.

Документування вимог і цілей є необхідним кроком у процесі проектування масштабованої комп'ютерної мережі для великого підприємства. Цей етап є ключовим, оскільки надає структурований та систематизований підхід до всього проекту, визначаючи його основні параметри та критерії успіху. Під час документування вимог збираються, аналізуються та систематизуються всі деталі щодо потреб підприємства в мережевому середовищі. Це включає в себе технічні параметри, такі як пропускна здатність,

доступність, безпека, а також функціональні вимоги, пов'язані з підтримкою конкретних бізнес-процесів. Щодо цілей, документація включає конкретні, вимірювані та реалістичні метрики, які повинні бути досягнуті в рамках проекту. Наприклад, якщо ціллю є підвищення швидкості передачі даних на 50%, то ця ціль має бути точно визначена в документі, разом з часовим графіком та іншими параметрами.

Цей документ стає основою для всієї подальшої роботи з проектом. Він служить засобом спілкування між різними командами та стейкхолдерами, забезпечуючи єдиний інтерпретаційний каркас для всіх заходів. Також цей документ є довідковим матеріалом для всіх, хто буде залучений до розробки та впровадження мережі, надаючи їм зрозуміле та структуроване відображення завдань та цілей. Документування також дозволяє вести ефективний моніторинг та контроль за виконанням проекту, допомагає в уникненні непорозумінь та забезпечує зручний інструмент для оцінки результатів відповідно до визначених вимог і цілей. Визначення бізнес-вимог і цілей допоможе створити чітку основу для проектування мережі, забезпечить, що вона буде відповідати потребам та цілям підприємства.[27]

Вимоги до програмного забезпечення є невід’ємною частиною процесу розробки, які визначають необхідність та параметри функцій, якості та властивостей майбутнього програмного продукту. Цей процес включає знаходження, аналіз та специфікацію вимог, а також їхнє подальше тестування.

Знаходження вимог передбачає збір та визначення потреб зацікавлених осіб та систем, а аналіз вимог включає перевірку їх цілісності та закінченості. Специфікація вимог полягає в документуванні виявлених вимог, що може включати в себе створення документів про бачення та меж проекту.[14]

Три рівні вимог до програмного забезпечення, визначені Карлом Вігерсом, включають бізнес-вимоги, які визначають призначення ПЗ; вимоги користувача, що визначають завдання користувача; та функціональні вимоги, що визначають "що" повинен робити програмний продукт.

Види вимог можна класифікувати за функціональним та нефункціональним характером. Функціональні вимоги визначають поведінку системи та можуть бути бізнес-вимогами, вимогами користувача чи функціональними вимогами. Нефункціональні вимоги визначають характер поведінки системи та можуть бути бізнес-правилами, системними вимогами чи атрибутами якості.

Загальний розгляд вимог до програмного забезпечення дозволяє структуровано та систематично підходити до розробки програми, забезпечуючи відповідність її функціональності та характеристик потребам користувачів і бізнесу.

Вимоги до програмного забезпечення походять з різних джерел, які визначають потреби та параметри розробки майбутньої системи. Ці вимоги можуть бути засвідчені законодавством, вимогами стандартів, бізнес-процесами та очікуваннями користувачів. Їх знаходження та документування включає методи спілкування з майбутніми користувачами, аналіз нормативної документації, бізнес-процесів, а також методи визначення вимог. Вимоги до програмного забезпечення служать засобом комунікації між різними зацікавленими особами і мають бути зрозумілими як для звичайних користувачів, так і для розробників. Вони представляються у вигляді таких документів як технічне завдання, специфікація вимог до програмного забезпечення (SRS) або інших артефактів, що відображають ключові пункти проекту.[13]

В рамках різних методологій розробки ПЗ вимоги можуть представлятися у вигляді моделей випадків використання, специфікацій та інших артефактів на різних етапах процесу. Наприклад, водоспадна модель передбачає завершення етапу аналізу вимог перед початком розробки ПЗ, тоді як ітеративні процеси розробки дозволяють змінювати вимоги протягом кожної ітерації розробки.

1.2 Оцінка масштабірuваності

Оцінка масштабіруваності є критичним етапом у проектуванні мережі для великого підприємства, оскільки вона визначає, наскільки ефективно мережа може адаптуватися до зростання обсягів даних, користувачів та інших вимог у майбутньому. Основна мета полягає в створенні інфраструктури, яка буде гнучкою, легко розширюватися та забезпечувати оптимальну продуктивність при збільшенні масштабу.

Пропускна здатність є ключовим параметром при оцінці масштабованості мережі для великого підприємства. Цей аспект визначає, наскільки швидко та ефективно мережа може обробляти та передавати дані при збільшенні їхнього обсягу. Аналіз пропускної здатності включає оцінку різних компонентів мережі, які можуть впливати на її продуктивність.

У визначенні пропускної здатності важливо враховувати потреби підприємства в обміні даними та розуміти, як швидко дані можуть бути передані від одного вузла до іншого. Це включає в себе розгляд комутаторів, маршрутизаторів та каналів передачі даних, а також їхню потужність та можливості. У великих підприємствах, де обсяги даних значно збільшуються, важливо мати мережеву інфраструктуру, яка може легко масштабуватися для відповіді на зростаючі потреби. Проектування мережі повинно передбачати не тільки поточні, але й майбутні обсяги трафіку, дозволяючи мережі ефективно використовувати свою пропускну здатність.[10]

Зазначаючи пропускну здатність різних компонентів, важливо визначити можливості їх оптимізації та розширення. Це може включати в себе використання технологій високої швидкості передачі даних, оптимізацію протоколів та використання широкосмугових каналів. Аналіз пропускної здатності є стратегічним елементом для забезпечення стабільності та продуктивності мережі в умовах постійного зростання обсягів даних.

Архітектурна гнучкість є критичним аспектом при масштабуванні мережі для великого підприємства. Цей аспект визначає спроможність мережі адаптуватися до змін у вимогах, ефективно інтегрувати нові компоненти та забезпечувати стабільну роботу без значних перебудов і перерв.

Гнучкість архітектури мережі означає, наскільки легко можна розширювати та модифікувати мережеву інфраструктуру. Важливо визначити, які частини мережі можуть бути модифіковані чи розширені без великих втрат ефективності та доступності. Під час оцінки архітектурної гнучкості, досліджується можливість інтеграції нових компонентів, таких як сервери, комутатори, маршрутизатори чи нові технології, вже існуючими структурами мережі. Це може включати в себе розгляд різних архітектурних підходів, таких як централізовані чи розподілені системи, використання віртуалізації та контейнеризації. Добре спроектована архітектура мережі повинна забезпечити необхідну гнучкість для швидкого реагування на зміни в бізнес-вимогах чи технологічному середовищі. Це дозволяє підприємству ефективно впроваджувати нові технології та розвивати свою мережу, не зазнаючи суттєвих перешкод або перебудов. Така архітектурна гнучкість сприяє створенню мережі, яка залишається актуальною та адаптивною в умовах постійної еволюції технологій та бізнес-потреб.[11]

Оцінка розподілених систем та обробки даних грає важливу роль у забезпеченні ефективності та продуктивності мережі для великого підприємства. Цей аспект визначає, наскільки добре система може працювати з великими обсягами даних та виконувати завдання в розподіленому середовищі.

Розподілена обробка даних означає, що завдання та обробка інформації розподілені по різних вузлах мережі, замість того, щоб концентруватися в одному центрі. Це дозволяє використовувати ресурси мережі більш ефективно та швидко реагувати на змінні обсяги даних.

При оцінці розподілених систем важливо враховувати їхню спроможність взаємодіяти між собою, забезпечуючи оптимальний обмін даними та виконання

завдань. Кожен вузол мережі може виконувати обчислення та обробку даних на місці, що призводить до зменшення навантаження на централізовані ресурси та прискорює виконання завдань. Додатково, врахування розподіленої обробки даних дозволяє оптимізувати використання ресурсів, таких як обчислювальна потужність та пам'ять, щоб максимально використовувати їхні можливості. Це особливо важливо в умовах зростання обсягів даних, коли централізований підхід може призвести до перенавантаження та зниження продуктивності. Розподілені системи також дозволяють підприємствам легше масштабувати свою інфраструктуру, додавати нові вузли та розширювати можливості обробки даних відповідно до зростання бізнесу. Такий підхід забезпечує ефективну та гнучку систему обробки даних, яка може успішно впоратися з вимогами великого підприємства.[22]

З розширенням мережі виникає критична необхідність уважного та комплексного вирішення питань безпеки. Масштабування мережі призводить до збільшення кількості точок доступу та об'ємів передаваних даних, що створює сприятливе середовище для різноманітних потенційних загроз. Питання безпеки мережі включає в себе захист від різних видів атак, включаючи зовнішні та внутрішні загрози. З ростом обсягів даних та розмірів мережі важливо ретельно оцінювати існуючі методи безпеки та розробляти стратегії посилення захисту. Для забезпечення безпеки мережі при розширенні необхідно впроваджувати ефективні засоби ідентифікації та автентифікації користувачів, а також контролю доступу до різних частин мережі. Важливо розглядати імплементацію шифрування для захисту конфіденційної інформації та даних під час їх передачі по мережі. Додатково, стеження за подіями та виявленням аномалій може бути важливим компонентом в системі безпеки, дозволяючи вчасно виявляти та реагувати на потенційні загрози. Регулярні аудити та тестування безпеки також важливі для впевненості в тому, що система захисту працює ефективно та відповідає зростаючим потребам. Забезпечення безпеки в умовах масштабування мережі вимагає стратегічного та

системного підходу, а також постійного оновлення та вдосконалення заходів захисту. Це дозволяє підприємству не лише розвивати свою мережу, але й зберігати високий рівень захищеності від потенційних загроз.

Управління ресурсами стає необхідністю при масштабуванні мережі для великого підприємства. Зі зростанням обсягів даних та розширенням мережевої інфраструктури, ефективне розподілення та контроль ресурсів стає ключовим елементом забезпечення оптимальної продуктивності та стабільності системи. Цей аспект охоплює визначення та розподіл різних ресурсів, таких як пропускна здатність, обчислювальна потужність, пам'ять, та інші, для забезпечення оптимального використання. Системи моніторингу та управління виступають важливими інструментами в цьому процесі. Моніторинг ресурсів дозволяє вчасно виявляти перевантаження, аномалії та інші проблеми в мережі. Ефективні засоби моніторингу не лише допомагають виявляти потенційні проблеми, але і забезпечують можливість аналізу та прогнозування тенденцій, що допомагає в управлінні ресурсами на основі реальних потреб мережі. Управління ресурсами також включає в себе механізми для ефективного розподілу завдань та обробки даних між різними частинами мережі. Це може включати автоматичне масштабування ресурсів, використання технологій віртуалізації та облікових систем для оптимізації використання обчислювальних ресурсів. Реагування на перевантаження та відмови в мережі вимагає вдосконалених систем управління, що можуть автоматично адаптувати ресурси для забезпечення найкращої продуктивності при змінах у вимогах. Це важливий аспект управління ресурсами, який сприяє стабільності та ефективності мережі в умовах постійних змін та зростання обсягів даних.[29]

Модульність та стандартизація в проектуванні мережі відіграють важливу роль у забезпеченні швидкого та легкого розширення мережевої інфраструктури. Ці принципи спрощують процес масштабування та дозволяють більш ефективно впроваджувати нові компоненти в мережу. Модульні рішення передбачають використання стандартизованих блоків або модулів, які можна

легко додавати або замінювати в мережевій архітектурі. Це створює гнучку інфраструктуру, де нові елементи можуть бути інтегровані без значних змін у загальній структурі мережі. Модульність дозволяє швидко реагувати на зростання вимог та ефективно впроваджувати нові технології. Стандартизація визначає використання загальних норм та протоколів, що спрощує взаємодію між різними компонентами мережі та дозволяє їм працювати разом. Використання стандартів сприяє сумісності різних пристроїв та рішень, а також полегшує процес інтеграції нових технологій у вже існуючу мережу. Модульність та стандартизація є важливими аспектами в галузі масштабування мережі для великих підприємств. Вони не лише полегшують розширення мережі, але і забезпечують стабільність та надійність системи, дозволяючи використовувати передові технології та ефективно втілювати інновації.[34]

Термін "масштабованість" дещо рідко зустрічається у вживанні менеджерів, але активно використовується в контексті курсів MOOC, спрямованих на комерційну діяльність та управління операціями або виробничими системами. За аналізом, представленим у дослідженні (Putnik et al., 2013), можна визначити, що інтерес до масштабованості почав зростати в науковому та практичному співтоваристві з 2000 року.

Дослідження Путніка (G. Putnik) та його співавторів включало аналіз динаміки кількості наукових статей, знайдених за фразою "scalability AND manufacturing" у провідних світових журналах, таких як Elsevier, Springer, T&F, Wiley, Emerald, JSTOR, ACM і IEEE. Важливим є те, що кількість опублікованих робіт збільшилася з 200 у 2000 році до приблизно 1600 у 2012 році.

Результати пошуку за двома формами запиту "scalability AND operations management" на ScienceDirect.com проілюстровано на рисунку 1. Графік також підтверджує зростання кількості наукових праць. Важливо зазначити, що пошук проводився в усіх джерелах, охоплюючи такі категорії, як бізнес,

управління та бухгалтерія, науки про прийняття рішень, економіка, економетрика та фінанси, соціальні науки.

Давайте розглянемо поняття операційної системи підприємства більш детально (в англійському варіанті це "operating system" або "operations"):

Це конфігурація ресурсів, спрямована на задоволення потреб споживачів у товарах та послугах (Ray Wild, 2002).

Це повна система виробничої діяльності підприємства, спрямована на виробництво товарів та надання послуг (Михайловська, 2008).

Це один з компонентів будь-якої організації, де реалізується операційна функція - процес виробництва продукції або надання послуг зовнішнім споживачам (Капінос і Бабій, 2013).

Таким чином, операційна система створює та постачає товари та послуги. Іншими словами, ця система приймає та перетворює вхідні потоки (inputs) на очікувані результати (outputs).

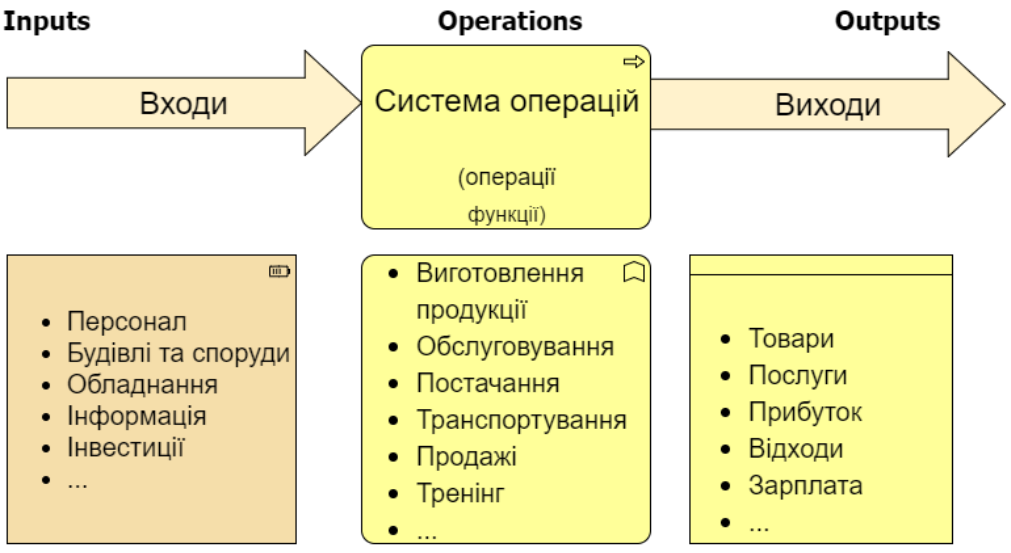

Рис.1.1 Загальна схема системи операцій

В першу чергу, систему операцій розглядають як конкретний об'єкт, включаючи обговорення матеріалів, обладнання та трудових ресурсів. Однак, з більш широкого економічного погляду, організація використовує не лише

матеріальні (тангібельні) ресурси, а й нематеріальні (інтангібельні), щоб створити цінність. Якщо організація може перетворити цю цінність в гроші, використовуючи вказані ресурси, то ці ресурси розглядаються як її активи.

Отже, активами вважаються ресурси, які задіяні підприємством для проведення операцій в межах затверджених виробничих, логістичних, збутових, сервісних та інших процесів. Серед них знаходяться людські ресурси та капітал, за допомогою яких генерується додаткова вартість і цінність, або які необхідні для виготовлення та доставки товарів, обробки вантажного транспорту, обслуговування клієнтів та виконання інших робіт, передбачених технологіями надання послуг. Іншими словами, активи представляють собою ресурси, необхідні для здійснення діяльності підприємства, при цьому враховується хто виконує роботу. Вони допомагають підприємству збільшити цінність своєї продукції та ефективно взаємодіяти з контрагентами з метою отримання економічних вигід у теперішньому та у майбутньому.

Таким чином, система операцій представляє собою комплексну конфігурацію активів та процесів, що організовані і спрямовані на забезпечення надання товарів і послуг із цінністю для споживачів. Головною метою є отримання підприємством економічних вигід у коротко- і довгостроковій перспективах. Процес трансформації входів у виходи у системі операцій відомий як виробничий процес, який, у свою чергу, може включати етапи виготовлення та монтажу (збірки).

Етап виготовлення (fabrication) охоплює створення деталей та частин готового виробу, в той час як етап монтажу (assembly) включає підбір та з'єднання цих деталей та частин у цілісний продукт, готовий до споживання або використання.

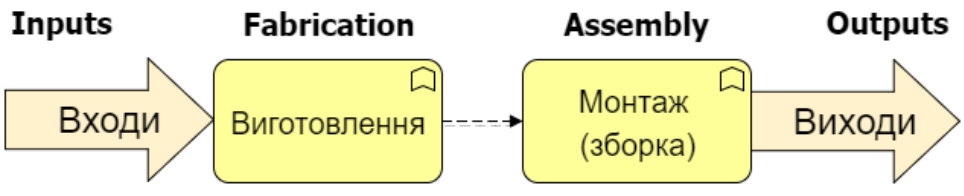

Рис.1.2 Зображення системи операцій як виробничого процесу

Підхід, зосереджений на процесах, розкриває місце та внесок активів у виробничий процес, а також вказує, як саме вони приносять вагому додану вартість і цінність. Цей підхід також розглядає різноманітні аспекти робіт, такі як умови, послідовність подій, результати, обіг документів і т.д.

В рамках процесного підходу система операцій розглядається як комплексна конфігурація активів і процесів, необхідних для постачання товарів і надання послуг, що є цінними для споживачів, з метою отримання підприємством економічних вигід у найближчому і віддаленому майбутньому.

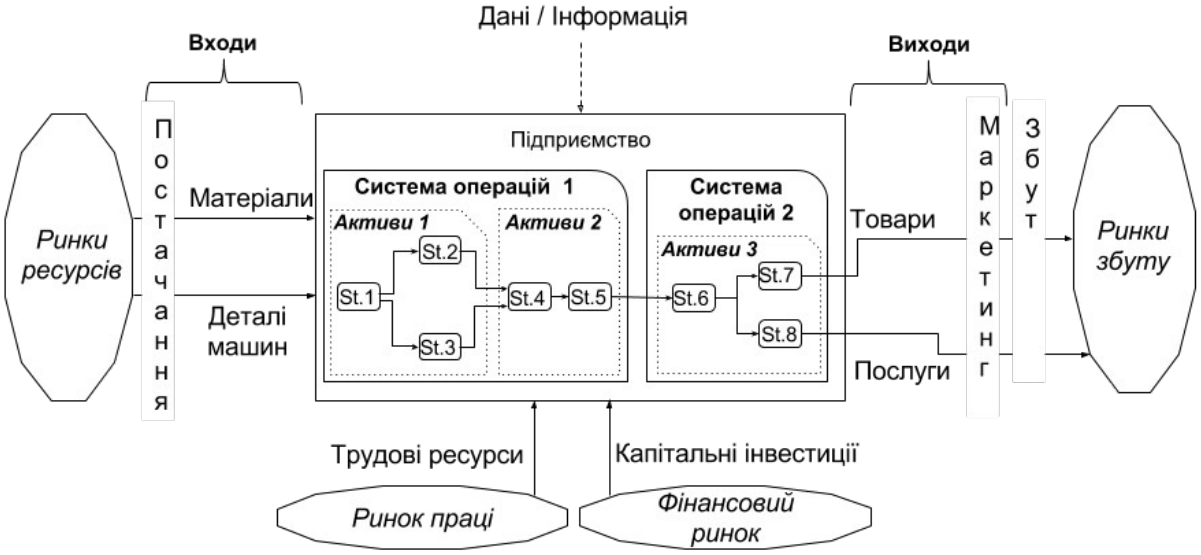

Рис.1.3 Схема системи операцій

Вхідні потоки, виготовлення та збірка, що формують виробничу функцію, разом із вихідними потоками, є необхідними компонентами поняття "виробнича система". У цій системі відбуваються всі операції, які необхідні для розробки, виробництва, розподілу і обслуговування виготовленої продукції (Sarabjeet Singh, 2012).

Додатково можна висловити ідеї Р. Уайлда (Ray Wild, 2002), який стверджує, що функція системи операцій відображає мету, якою вона служить споживачам, та корисність її виходу для них.

Важливо відзначити, що виробнича функція, що включає обробку, є ключовою для обох систем - виробничої та операційної. Ця функція відтворює фізичні властивості або змінює форму ресурсів в корисні продукти, відмінні від початкових матеріалів. Наприклад, сировина і матеріали перетворюються в товари, які є корисними для споживачів; постільна білизна, рушники і кімнати - у місця для розміщення мандрівників. Виробнича функція додає цінність до товарів або послуг та сприяє їхньому успішному впровадженню на ринку (Mahadevan, 2010).

1.3 Визначення технічних вимог

Визначення технічних вимог — це процес формулювання конкретних характеристик, функцій та параметрів, які має володіти система чи продукт. Цей етап важливий в процесі розробки чи впровадження технічного проекту і дозволяє чітко визначити очікувані результати та характеристики. Функціональні вимоги є ключовим елементом визначення технічних параметрів системи чи продукту. Це визначення того, як саме система має працювати, які функції вона повинна виконувати та які конкретні вимоги стосуються їх функціональності.

Опис функціональних вимог дозволяє чітко зрозуміти, як система буде взаємодіяти з користувачем чи іншими системами. Це може включати такі елементи, як можливості введення та виведення даних, алгоритми обробки інформації, реакцію на певні події та подальші внутрішні функції системи.

Функціональні вимоги визначають, як система буде взаємодіяти з користувачем, які сервіси вона надає та які завдання вона виконує. Наприклад, для програмного забезпечення функціональні вимоги можуть включати можливості створення, збереження та редагування файлів, виконання певних обчислень, взаємодію з базою даних, тощо.

Важливо, щоб функціональні вимоги були конкретними та однозначними, щоб уникнути непорозумінь та допомогти розробникам чітко реалізувати функціональність. Деталізація функціональних вимог може включати в себе визначення вхідних та вихідних даних, умов реалізації, варіантів використання та інших аспектів, щоб створити повний та зрозумілий опис того, як має працювати система.

Нефункціональні вимоги визначають аспекти, які не пов'язані безпосередньо з конкретними функціями системи, але визначають якість, ефективність та різні аспекти, які впливають на спосіб, яким система працює та як користувачі взаємодіють з нею.

Однією з ключових нефункціональних вимог є швидкодія. Це може охоплювати час відгуку системи, швидкість обробки даних, завантаження сторінок в веб-додатках, тощо. Важливо визначити часові рамки та очікувані показники ефективності системи. Безпека також є суттєвою нефункціональною вимогою, особливо для систем, які обробляють чутливі дані. Вимоги до безпеки визначають, які заходи повинні бути вжиті для захисту від несанкціонованого доступу, збереження конфіденційності та цілісності даних. Масштабованість визначає здатність системи адаптуватися до зростання обсягів даних або користувачів без втрати продуктивності. Ця вимога особливо важлива для підприємств, які очікують зростання та розширення.[34]

Надійність є ще однією важливою нефункціональною вимогою. Вона визначає, наскільки стійкою є система до відмов та як швидко можливо відновити роботу в разі неполадок.

Інші нефункціональні вимоги можуть включати в себе вимоги до доступності, простоти використання, сумісності з іншими системами та інші аспекти, які визначають загальний досвід використання та функціонування системи.

Характеристики продукту або системи є детальним описом технічних параметрів, що визначають фізичні та технічні аспекти продукту чи системи. Ці

характеристики грають важливу роль у визначенні та розумінні функціональності та можливостей продукту або системи.

Розміри вказують на геометричні розміри продукту чи системи, такі як довжина, ширина, висота та інші просторові параметри. Ці виміри можуть бути критичними для інтеграції продукту в певні середовища або для забезпечення сумісності з іншими компонентами.

Вага є ще однією важливою характеристикою, особливо для фізичних об'єктів. Вона може впливати на транспортування, монтаж та загальну стійкість продукту. Для електронних пристроїв чи компонентів вага може бути критичною для визначення їх придатності до використання в конкретних умовах.

Швидкість може стосуватися рухомих частин, передачі даних чи інших параметрів, які вимірюються в часових одиницях. Наприклад, для транспортного засобу це може бути максимальна швидкість руху, а для мережевого обладнання - швидкість передачі даних. Потужність визначає енергійні характеристики продукту або системи. Це може включати в себе електричну чи теплову потужність, яка важлива для ефективності, безпеки та стійкості в роботі. Характеристики продукту або системи надають інженерам та користувачам чітке уявлення про технічні аспекти та обмеження продукту. Ці параметри можуть бути визначальними при виборі продукту або при визначенні, наскільки ефективно продукт буде відповідати потребам користувача чи ринку.[30]

Вимоги до інтеграції визначаються там, де система повинна взаємодіяти з іншими системами чи компонентами, будь то в межах внутрішнього корпоративного середовища чи на рівні широкомасштабних мереж та взаємодії зовнішніх сервісів.

Це включає вимоги до інтерфейсів, які визначають, як саме система буде обмінюватися даними та комунікувати з іншими компонентами. Це може охоплювати стандарти передачі даних, протоколи комунікації, формати обміну

інформацією та інші аспекти, які забезпечують сумісність та ефективність обміну даними між різними системами.

Стандарти обміну даними можуть включати в себе такі аспекти, як формати файлів, використання мов програмування, RESTful або SOAP-схеми для веб-сервісів, або інші визначені протоколи. Важливо враховувати та відповідати стандартам галузі або внутрішнім стандартам організації. Крім того, вимоги до інтеграції можуть включати в себе інші аспекти, такі як автентифікація та авторизація для забезпечення безпеки під час обміну даними, адаптація до різних версій стандартів чи протоколів, а також управління помилками та винятками під час інтеграції. Визначення чітких та докладних вимог до інтеграції є ключовим елементом для успішного взаємодії різних систем та забезпечення надійності та ефективності обміну даними.

Вимоги до безпеки та захисту даних є критично важливим аспектом при розробці та впровадженні будь-якої інформаційної системи чи програмного продукту. Ці вимоги визначають заходи та стандарти, які необхідно впроваджувати для забезпечення високого рівня безпеки та конфіденційності даних, які обробляє система. Один із ключових аспектів вимог до безпеки - це захист від несанкціонованого доступу. Це включає в себе визначення прав доступу до різних рівнів інформації та ресурсів системи, використання механізмів аутентифікації та авторизації, а також заходи для виявлення та усунення загроз безпеки. Крім того, вимоги до безпеки можуть включати шифрування даних для захисту їх конфіденційності під час передачі та зберігання. Застосування шифрування забезпечує безпечний обмін інформацією між різними компонентами системи та зменшує ризик несанкціонованого доступу до чутливих даних. Стандарти та протоколи безпеки також можуть бути включені в вимоги для забезпечення відповідності системи визначеним стандартам та нормативам в сфері інформаційної безпеки. Це може включати в себе використання стандартів шифрування, протоколів безпеки мережі, а також використання спеціалізованих засобів захисту від загроз. Вимоги до безпеки та

захисту даних є необхідною частиною проектування будь-якої системи, яка обробляє чутливу інформацію, і грають ключову роль у забезпеченні довіри користувачів та захисту важливих даних.[37]

Вимоги до документації представляють собою важливий етап у процесі розробки та впровадження будь-якої системи чи продукту. Ці вимоги визначають, які документи повинні бути розроблені, їхню структуру та зміст, а також визначають регулярність оновлення та підтримки документації.

Однією з ключових складових вимог до документації є технічна специфікація. Цей документ детально описує технічні характеристики системи, включаючи архітектуру, інтерфейси, алгоритми та інші технічні аспекти. Технічна специфікація є основним документом для розробників, тестувальників та інших учасників проекту, які працюють над реалізацією та тестуванням системи.

Інструкції з експлуатації є ще однією важливою складовою документації. Ці інструкції надають користувачам чітке та зрозуміле керівництво з використання системи, включаючи установку, налаштування, роботу з інтерфейсом та вирішення проблем. Вони сприяють ефективному та безпечному використанню системи користувачами. Інші види документації можуть включати технічні керівництва для розробників, звіти по тестуванню, звіти з безпеки, документи з управління проектом та інші, які можуть бути важливими для розуміння, впровадження та підтримки системи. Вимоги до документації гарантують створення повноцінної та зрозумілої документації, що сприяє ефективній комунікації, забезпечує легку підтримку та подальший розвиток системи або продукту.

Визначення технічних вимог є ключовим етапом в процесі розробки та впровадження технічного проекту, оскільки вони служать основою для подальшої розробки, тестування та оцінки продукту чи системи. Чіткі та вичерпні технічні вимоги допомагають уникнути непорозумінь та забезпечити відповідність результату очікуванням клієнта чи користувача.

Аналіз вимог - це визначення потреб і умов, які висуваються до нового чи зміненого продукту, з урахуванням можливо конфліктних вимог різних замовників, таких як користувачі чи бенефіціари.

Аналіз вимог є вирішальним для успішного розроблення проекту. Вимоги повинні бути задокументованими, виміряними, тестовними, пов'язаними з бізнес-потребами і описаними з рівнем деталізації, достатнім для конструювання системи. Вимоги можуть бути архітектурними, структурними, поведінковими, функціональними та не функціональними.

В мові моделювання SysML вимоги можна моделювати за допомогою діаграм вимог, а в UML для цього інколи використовується діаграма прецедентів. Аналіз вимог включає три види діяльностей:

1. Виявлення вимог: це взаємодія з користувачами для визначення їхніх вимог, також це може бути названо збором вимог.

2. Аналіз вимог: це виявлення недоліків вимог і їх виправлення.

3. Запис вимог: вимоги можна задокументувати в різних формах, таких як опис звичайною мовою, прецеденти, користувацькі історії чи специфікації процесу.

Аналіз вимог може бути складним і тривалим процесом, який вимагає використання тонких психологічних навичок. Нові системи можуть змінювати середовище і взаємини між людьми, тому важливо враховувати всі зацікавлені сторони, їхні потреби і наслідки, які нова система може мати. Аналітики можуть використовувати різні методи для отримання від споживачів вимог, такі як інтерв'ю, фокус-групи або створення списків вимог. Сучасні підходи включають прототипування та використання прецедентів.

Інженерія вимог (або систематичний аналіз вимог) - це піддисципліна системної інженерії та програмної інженерії, яка займається визначенням цілей, функцій та обмежень апаратних і програмних систем. Цей процес може бути розділений на кілька етапів: збір (виявлення) вимог, аналіз та узгодження

вимог, специфікація вимог, моделювання системи, перевірка вимог та управління вимогами.[33]

Визначення зацікавлених сторін (ЗС) означає осіб чи організацій, які проявляють реальний інтерес до системи і можуть бути впливовані нею прямо чи опосередковано.

Слід відзначити, що зацікавлені сторони не обов'язково обмежуються організацією, яка здійснює найм аналітиків. До них також входять:

1. Всі, хто буде управляти системою (включаючи звичайних та обслуговуючих операторів).

2. Всі, хто отримає вигоди від системи (функціональні, політичні, фінансові та соціальні бенефіціари).

3. Учасники в процесі придбання чи закупівлі системи. У розробці продуктів для масового ринку відділи управління продуктом, маркетингу і іноді продажі можуть діяти як замінники споживачів для направлення розробки продукту.

4. Організації, що регулюють аспекти системи (фінансові, безпекові та інші регулятори).

5. Особи та організації, які протистоять системі (негативні зацікавлені сторони).

6. Організації, відповідальні за системи, які будуть взаємодіяти з розроблюваною системою.

7. Організації, які горизонтально інтегруються з організацією, для якої аналітики будують систему.

Інтерв'ю з зацікавленими сторонами є звичайним методом в аналізі вимог. Цей підхід дозволяє отримати глибше розуміння, яке часто не виявляється на спільних сесіях розробки вимог, де увага зацікавлених сторін зосереджена на наданні більш широкого контексту. Крім того, особистий характер інтерв'ю створює більш розслаблене середовище, де можна більш детально пояснити хід думок.

Спільні сесії розробки вимог важливі, оскільки вимоги часто мають крос-функціональні наслідки, які невідомі окремим зацікавленим сторонам і можуть бути упущені або неправильно описані під час інтерв'ю з зацікавленими сторонами. Ці крос-функціональні наслідки можуть бути виявлені під час сесій розробки в контрольованому середовищі, де зацікавлені сторони беруть участь у дискусії для виявлення вимог, їх аналізу та розкриття крос-функціональних наслідків. Для документування дискусії зазвичай присутні спеціальний секретар і бізнес-аналітик. Використання кваліфікованого посередника для управління дискусією дозволяє бізнес-аналітику сконцентруватися на процесі визначення вимог. Сесії розробки вимог схожі на сесії спільного проектування програмного забезпечення. По-перше, сесії виявляють вимоги, які направляють дизайн, а потім визначають властивості, які мають бути реалізовані для задоволення отриманих вимог.[27]

Створення списків вимог у формі контракту є традиційним методом документування вимог, і в складних системах такий список може мати сотні сторінок.

Можна використовувати метафору дуже довгого списку покупок для пояснення цього підходу. Однак у сучасному аналізі цей метод не завжди є ефективним, оскільки він часто не досягає своїх цілей. Тим не менше, такі списки можна спостерігати і сьогодні.

Переваги:

1. Надає чіткий перелік вимог.

2. Створює контракт між спонсорами проекту та розробниками.

3. Для великих систем може надати високорівневий опис.

Недоліки:

1. Списки можуть бути дуже об'ємними (сотні сторінок), що робить їх майже незчитуваними та неспроможними надати повний огляд системи.

2. Створюють абстракцію від усіх вимог, що призводить до відсутності контексту.

3. Ускладнюють визначення взаємозв'язків та взаємодії між вимогами.

4. Ускладнюють правильне встановлення пріоритетів між вимогами.

5. Збільшують ймовірність неправильної інтерпретації вимог через велику кількість читачів.

6. Важко визначити повноту вимог.

7. Створюють фальшиве враження взаєморозуміння між сторонами.

Списки в стилі контракту можуть створювати у ЗС хибне відчуття надійності, що розробники зобов'язані виконати певні завдання. Проте через природу таких списків, вони не враховують критичні вимоги, які виявляються пізніше в процесі розробки. Усунення відкритих вимог може допомогти перегляду умов договору на користь розробників.

Існують альтернативи великим спискам вимог, такі як гнучка розробка програмного забезпечення, яка використовує історії користувачів для опису вимоги простими та зрозумілими термінами.

Вимірювані цілі:

Кращі практики включають складний список вимог як вказівку та постійно питають "Чому?", поки не з'ясується справжня бізнес-ціль. Сторони та розробники можуть розробити тести для вимірювання досягнення цілей, що змінюються повільніше за об'ємний, але не конкретний перелік вимог.

Прототипи:

Хоча прототипування визнано корисним методом, воно не вирішує основну проблему визначення вимог. Менеджери часто перестають розуміти, що проект не готовий, коли бачать прототип. Дизайнери можуть відчувати необхідність використання прототипу в реальній системі, бо бояться "втратити час" на початок спочатку. Прототипи допомагають у конструкторських рішеннях та інтерфейсі користувача, але не визначають початкові вимоги.

Ці альтернативи можуть бути більш ефективними, оскільки вони дозволяють зберігати простоту та зрозумілість, що полегшує спілкування між сторонами та поліпшує розуміння проекту.

Прецеденти:

Прецеденти є методом документування потенційних вимог до нової чи зміненої програмної системи. Кожен прецедент включає один чи кілька сценаріїв, які ілюструють, як система взаємодіє з користувачем чи іншою системою для досягнення конкретної бізнес-цілі. Ці документи уникають технічного жаргону та використовують мову, зрозумілу для кінцевого користувача чи експерта у предметній області. Інженери вимог та ЗС часто співпрацюють у створенні прецедентів. Прецеденти є зручними, але при цьому простими інструментами для опису поведінки системи. Вони надають текстовий опис різних способів взаємодії користувачів з програмним забезпеченням, не вдаваючись у внутрішні процеси чи реалізацію системи. Ці документи висвітлюють лише кроки, які користувач повинен виконати для вирішення своєї задачі та взаємодії з системою.

Специфікація вимог до програмного забезпечення (SRS):

SRS є повним описом поведінки системи, яка розробляється. Вона включає набір прецедентів, що описують всі можливі взаємодії користувача з системою. Прецеденти в SRS також відомі як функціональні вимоги. Окрім цього, SRS містить нефункціональні вимоги, які ставлять обмеження на проект чи реалізацію, такі як вимоги щодо продуктивності, стандартів якості чи обмежень дизайну.

Рекомендовані підходи до створення SRS описані у стандарті IEEE 830–1998, який надає вказівки щодо можливих структур, бажаного вмісту та якостей специфікації вимог.

Типи вимог:

Вимоги поділяються на декілька категорій. Один зі звичайних підходів до категоризації вимог з точки зору технічного менеджменту включає:

1. Вимоги споживача: Висловлюють очікування до системи в термінах цілей, середовища, обмежень та міри ефективності й придатності. Операційні

вимоги описують базову необхідність і відповідають на запитання, такі як де використовуватиметься система, яким чином буде виконувати завдання та інші.

2. Архітектурні вимоги: Пояснюють, яку системну архітектуру слід реалізувати.

3. Структурні вимоги: Визначають необхідну структуру системи.

4. Поведінкові вимоги: Описують необхідну поведінку системи.

5. Функціональні вимоги: Ідентифікують завдання, дії чи діяльності, які мають виконуватися системою.

6. Нефункціональні вимоги: Задають критерії для оцінки операцій системи, замість її поведінки.

Вимоги продуктивності:

Вимоги продуктивності визначають міру досягнення місій чи функцій, часто вимірювану за кількістю, якістю, охопленням, своєчасністю чи готовністю. Під час аналізу вимог, вимоги продуктивності розробляються взаємодійно для всіх виявлених функцій, що базуються на факторах життєвого циклу системи. Вони характеризуються термінами визначеності їхніх оцінок, ступеня критичності для успіху системи та їхнього відношення до інших вимог.

Вимоги дизайну:

Вимоги "будувати до," "кодувати до" та "купувати до" стосуються продуктів, а "як виконати" застосовується до процесів, виражених у технічних пакетах даних та інструкціях.

Успадковані вимоги:

Це вимоги, що виникають внаслідок вищих рівнів або трансформації з них. Наприклад, вимога щодо великої дальності чи високої швидкості може викликати вимогу щодо дизайну легкої системи.

Розподілені вимоги:

Це вимоги, які визначаються розбиттям або іншим перерозподілом високорівневих вимог на кілька низькорівневих вимог. Наприклад, пристрій

вагою 100 кілограм, що складається з двох підсистем, може викликати вимоги щодо ваги не більше 70 та 30 кілограм для конкретних систем нижчого рівня.

До відомих моделей категоризації вимог належать FURPS та FURPS+, розроблені в компанії Hewlett-Packard.

Проблеми аналізу вимог:

Правильно сформульовані вимоги до програмного проєкту мають вирішальне значення для його успіху. Дослідження свідчать про те, що невірно визначені вимоги часто є основною причиною невдач проєктів. З часом виправити помилки, допущені при визначенні вимог, стає складніше і дорожче.

Проблеми з зацікавленою стороною:

Зацікавлені сторони можуть ускладнити процес збору вимог:

- Нерозуміння користувачами того, що їм потрібно або відсутність чіткого уявлення про їхні вимоги.

- Відсутність участі користувачів у письмовому формулюванні вимог.

- Наполягання користувачів на нових вимогах після фіксації цін та графіку розробки.

Проблеми з інженерами/розробниками:

Проблеми, пов'язані з інженерами та розробниками під час аналізу вимог:

- Різномовність мови між технічним персоналом та кінцевими користувачами.

- Тенденція розробляти вимоги, що відповідають існуючій системі чи моделі, замість створення системи, що відповідає потребам клієнта.

- Аналіз, проведений інженерами чи програмістами, а не фахівцями з комунікацій та предметної області.

Можливі рішення:

Щоб подолати проблеми комунікації, можна розглянути найм фахівця з бізнес-аналізу чи системного аналізу. Використання технологій, таких як прототипування, Unified Modeling Language (UML), прецеденти та гнучка розробка програмного забезпечення, також може полегшити процес. Нові

інструменти симуляції програмного забезпечення дозволяють тестувати додатки перед написанням коду, зменшуючи ризики та витрати. Важливо також враховувати обмеженість інформації та знань учасників і забезпечити вірне виставлення пріоритетів.

Розділ 2. Проектування мережі

2.1 Топологія мережі

Топологія мережі визначає структурний дизайн, спосіб підключення та взаємодії пристроїв у мережі. Різні типи топологій використовуються в залежності від потреб конкретного проекту чи організації. Зіркова топологія є однією з основних структурних моделей побудови комп'ютерних мереж. У цій топології кожен комп'ютер або мережевий пристрій підключений безпосередньо до центрального вузла, який зазвичай виступає в ролі комутатора чи концентратора. Такий центральний елемент є центром керування, через який всі з'єднання в мережі проходять.

Основний принцип зіркові топології полягає в тому, що кожен пристрій має власний окремий канал для спілкування з центральним вузлом. Це спрощує процес збирання та розподілу даних в мережі, а також забезпечує структурну простоту. Якщо один пристрій несправний чи вимагає заміни, це не впливає на решту мережі.

Особливості зіркові топології дозволяють легко розширювати мережу, додаючи або вилучаючи пристрої без значного впливу на решту мережі. Також, завдяки централізованому характеру структури, виявлення та усунення несправностей стає швидшим та ефективнішим процесом. Перевагою зіркової топології є її простота у встановленні та керуванні, що робить її ідеальним варіантом для невеликих до середніх мереж. Також, ця топологія забезпечує невелику кількість конфліктів та колізій в передачі даних. Однак, важливо враховувати, що при збільшенні розміру мережі і збільшенні об'єму передаваних даних, пропускна здатність центрального вузла може стати обмежувальним фактором.[17]

Кільцева топологія є структурною моделлю мережі, де кожен вузол підключений до двох інших вузлів, утворюючи кільце. Цей кільцевий механізм передачі даних дозволяє інформації обходити мережу, проходячи через кожен

вузол в заданому порядку. Така організація мережі створює специфічний маршрут передачі даних, що характеризується взаємодією між сусідніми вузлами. Основним принципом кільцевої топології є те, що кожен вузол підключений до точно двох інших, що створює неперервне кільце. Якщо один із вузлів виявляється несправним чи відмовляє, дані можуть продовжувати обходити кільце через інші маршрути, що робить систему стійкою до відмов. Однією з основних переваг кільцевої топології є її висока стійкість до відмов. Завдяки наявності альтернативних маршрутів для передачі даних, якщо один шлях перестає працювати, інші можуть використовуватися. Це робить таку топологію популярною для мереж, де надійність є критично важливою.[13]

Однак у кільцевої топології є свої обмеження. Додавання чи вилучення вузлів може бути складним завданням, оскільки це може порушити структуру кільця. Крім того, створення кільцевої топології може вимагати великої кількості кабелю для з'єднання кожного вузла з двома сусідами, що може призвести до деяких витрат та ускладнення управління кабелями. Усі ці аспекти важливі при виборі типу топології в залежності від конкретних потреб та вимог мережі.

Шинна топологія є однією з основних структурних моделей мережі, де всі пристрої підключені до спільної шини чи кабелю. В цьому варіанті топології пристрої ділять одне з'єднання для обміну даними, і вся інформація, що передається одним пристроєм, доступна всім іншим пристроям на цій шині.

Основний принцип шинної топології полягає в тому, що всі пристрої підключені до одного центрального каналу зв'язку. Якщо один з пристроїв вирішить передати дані, ці дані будуть доступні всім іншим пристроям на цій шині. Це робить шинну топологію простою та економічно вигідною в плані витрат на кабелі, оскільки для підключення пристроїв використовується лише один канал.

Однак існують певні недоліки у шинній топології, основними з яких є можливість переповнень та конфліктів. Якщо кілька пристроїв намагаються

передавати дані одночасно, це може призвести до конфліктів і порушень в роботі мережі. Це особливо стає проблемою у великих мережах, де збільшується ймовірність одночасних передач. Шинна топологія часто використовується в невеликих мережах, де необхідної пропускної здатності досить для поточних завдань, і де простота у встановленні та керуванні важливіша за потенційні обмеження в продуктивності.[7]

Деревоподібна топологія є гібридом інших топологій, зокрема зіркової та шинної. У цій структурі групи пристроїв підключені до центрального вузла, а сам цей центральний вузол є також підключеним до іншого центрального вузла. Такий пристосований підхід дозволяє створювати більші мережі, комбінуючи переваги різних топологій.

Однією з основних особливостей деревоподібної топології є можливість побудови більших та більш складних мереж. Кожна група пристроїв, яка може представляти окремий відділ чи підрозділ в організації, підключена до свого центрального вузла, а ці вузли в свою чергу об'єднані в ще більший центральний вузол. Це дозволяє ефективно керувати різними частинами мережі та сприяє легшому масштабуванню.

Недоліками деревоподібної топології можуть бути більш складне керування та витрати на обладнання. З ростом мережі ускладнюється координація роботи різних центральних вузлів, а також можуть збільшитися витрати на обладнання та його управління. У цілому, деревоподібна топологія використовується там, де необхідно об'єднати переваги різних топологій для створення більш гнучких та масштабованих мереж.

Меш-топологія є однією з найбільш гнучких та надійних структурних моделей мережі. У цій топології кожен пристрій підключений безпосередньо до кожного іншого пристрою в мережі, утворюючи велику матрицю з'єднань. Такий підхід забезпечує велику надійність, оскільки існує багато альтернативних маршрутів для передачі даних.

Однією з особливостей меш-топології є висока надійність передачі даних. Якщо один маршрут виявляється несправним або перегруженим, існують інші шляхи для передачі інформації. Це робить меш-топологію дуже стійкою до відмов та ідеальною для великих мереж, де надійність є критично важливою.

Однак недоліками меш-топології є велика кількість кабелів та портів на обладнанні, що може призвести до великих витрат на обладнання та ускладнення управління. Збільшення кількості підключень може призвести до значного зростання вартості та складнощі в обслуговуванні. Крім того, керування такою мережею вимагає вдумливого планування та конфігурації, щоб забезпечити оптимальну ефективність та ресурсозбереження.

Кожен з цих типів топологій має свої переваги та обмеження, і вибір топології залежить від конкретних вимог та умов конкретного проекту.

2.2 Забезпечення безпеки

Забезпечення безпеки є невід'ємною частиною будь-якого проектування масштабованої комп'ютерної мережі для великого підприємства. Безпека мережі стає ключовою, оскільки із збільшенням розміру мережі зростає загроза вразливостей та атак. Аутентифікація та авторизація становлять основний фундамент безпеки в будь-якій комп'ютерній мережі, особливо в контексті проектування масштабованої інфраструктури для великого підприємства. Аутентифікація є процесом перевірки ідентичності користувача або пристрою перед наданням доступу до мережевих ресурсів. В масштабованих мережах важливо використовувати сильні методи аутентифікації, такі як багатофакторна аутентифікація, що включає в себе крім паролів, наприклад, використання біометричних даних чи токенів. Це допомагає уникнути ризику несанкціонованого доступу через втрату чи компрометацію паролів. Після успішної аутентифікації система повинна визначити, які ресурси та функціональні можливості має право використовувати користувач чи пристрій.

Системи авторизації встановлюють правила, що визначають, на які дані і ресурси може мати доступ кожен користувач або група користувачів. Це включає в себе визначення рівнів доступу, ролей та правил обмежень.[3]

Реалізація сильної аутентифікації сприяє підвищенню безпеки мережі, запобігаючи несанкціонованому доступу. Встановлення правильно налаштованих систем авторизації дозволяє точно визначити, які ресурси може використовувати кожен користувач, що є важливим у великих організаціях з різнорівневою структурою та різноманітними вимогами щодо безпеки. В цілому, ці два елементи взаємодіють для створення надійного механізму контролю доступу, який ускладнює завдання потенційного зловмисника та допомагає уникнути компрометації мережевих ресурсів.

Шифрування даних є ключовим елементом забезпечення безпеки в масштабованих комп'ютерних мережах для великих підприємств, де конфіденційні дані часто передаються через різноманітні пункти мережі. Використання шифрування дозволяє перетворювати інформацію в нечитабельну форму для неповноважних осіб та забезпечує захист від небажаного доступу.[1]

Під час передачі даних по мережі важливо використовувати шифрування для захисту від прослуховування та перехоплення інформації. Застосування шифрування відбувається на різних рівнях мережевого стеку, включаючи рівень застосунків, транспорту та мережі. Такі протоколи, як TLS (Transport Layer Security) або SSL (Secure Sockets Layer), використовуються для забезпечення зашифрованого каналу передачі даних. Крім того, важливо встановлювати стандарти шифрування для безпечного зберігання даних на серверах та інших пристроях. Зашифроване зберігання гарантує, що навіть у випадку фізичного доступу до обладнання конфіденційна інформація залишається захищеною від несанкціонованого доступу. Використання сучасних алгоритмів шифрування, таких як AES (Advanced Encryption Standard) чи RSA (Rivest–Shamir–Adleman), забезпечує високий рівень безпеки для даних

у мережевому середовищі. Шифрування даних є необхідним елементом комплексної стратегії безпеки, яка допомагає уникнути ризиків порушення конфіденційності та забезпечує безпеку інформації в усіх точках її перебування в мережі.[24]

Захист від атак є невід'ємною частиною будь-якої масштабованої комп'ютерної мережі для великого підприємства. Це включає в себе ряд стратегій та заходів, спрямованих на виявлення та запобігання різноманітним загрозам безпеки. Реалізація мережевих брандмауерів є ключовою для контролю трафіку, що входить та виходить з мережі. Брандмауери встановлюють правила, які регулюють доступ користувачів та пристроїв до різних частин мережі та визначають дозволені та заборонені види трафіку.[37]

Інтрузійні виявники (IDS) використовуються для виявлення непередбачених або підозрілих патернів у мережевому трафіку, що можуть свідчити про атаки або несанкціонований доступ. Активне виявлення інтрузій дозволяє оперативно реагувати на потенційні загрози та негайно вживати заходів для їх запобігання.

Проведення регулярних аудитів безпеки є важливою частиною стратегії захисту мережі. Це включає в себе перевірку конфігурацій систем, реалізацію кращих практик безпеки та виявлення слабких місць, які можуть бути використані зловмисниками.

Сканування портів допомагає виявляти відкриті порти на системах та пристроях, що може свідчити про потенційні проблеми безпеки. Виявлення відкритих портів дозволяє швидко реагувати та закривати непотрібні або потенційно небезпечні точки доступу. В цілому, впровадження цих стратегій дозволяє підприємствам ефективно захищати свою мережу від різноманітних атак, забезпечуючи високий рівень безпеки та надійності.

Фізична безпека є однією з найважливіших аспектів загальної стратегії забезпечення безпеки комп'ютерної мережі для великого підприємства. Цей аспект охоплює заходи, спрямовані на захист фізичних ресурсів, таких як

серверні кімнати, комутатори та інше обладнання, які є ключовими складовими інфраструктури мережі.

Серверні кімнати та інші приміщення, де знаходиться мережеве обладнання, повинні бути обладнані високорівневими заходами безпеки. Це включає в себе використання систем контролю доступу, таких як електронні картки або біометричні сканери, які дозволяють обмежити доступ лише авторизованим особам. Крім того, важливо враховувати вогнестійкість, вентиляцію та системи відновлення в разі аварії для забезпечення найвищого рівня захисту для обладнання, яке забезпечує стабільну роботу мережі.

Запобігання несанкціонованому фізичному доступу до мережевого обладнання - це критичний аспект фізичної безпеки. Це може бути досягнуто за допомогою фізичних бар'єрів, таких як замки на дверях, контрольні пункти та системи відеоспостереження. Додатково, важливо встановлювати жорсткі правила щодо доступу до серверних приміщень та обладнання, надавати доступ лише необхідним співробітникам і вести журнал доступу для ведення контролю та аудиту. Загальною метою фізичної безпеки є забезпечення того, щоб ті, хто не має необхідних повноважень, не мали фізичного доступу до чутливих ресурсів мережі. Це допомагає уникнути фізичних загроз та зберігає надійність і доступність мережевих служб для авторизованих користувачів.

Політики безпеки визначають рамки та правила, які регулюють використання мережі та забезпечують високий рівень безпеки. Ці політики є фундаментом для визначення стандартів безпеки, які повинні дотримуватися всіма користувачами та працівниками підприємства. Ефективні політики безпеки повинні бути чіткими, доступними та легкими для розуміння. Вони визначають, які заходи безпеки слід застосовувати, як зберігати та обробляти конфіденційні дані, які правила використання мережевих ресурсів та інші стандарти безпеки повинні бути дотримані. Політики безпеки також повинні визначати відповідальність за виконання та дотримання цих правил. Вони

можуть включати в себе вимоги щодо використання паролів, шифрування даних, управління патчами та інші заходи для запобігання безпековим загрозам.

Важливим елементом ефективної політики безпеки є тренінг персоналу. Співробітники повинні бути усвідомлені щодо потенційних загроз безпеці та знати, як діяти в разі виявлення аномальностей чи підозрілих активностей. Тренінги можуть включати в себе навчання про правильне використання паролів, розпізнавання соціально інженерних атак, ознайомлення з політикою безпеки та інші аспекти, які допоможуть персоналу бути більш усвідомленим та готовим до взаємодії з питань безпеки. Узгоджені та впроваджені політики безпеки сприяють створенню безпечного та відповідального використання мережевих ресурсів, зменшуючи ризики та забезпечуючи стійкість мережі в умовах зростаючих загроз безпеки.[30]

Резервне копіювання та відновлення є ключовими аспектами стратегії безпеки мережі для забезпечення стійкості та відновлення нормального функціонування в разі втрати даних або непередбачуваних ситуацій. Один із основних принципів безпеки - це не тільки запобігання втраті даних, але і готовність до їх відновлення. Регулярне резервне копіювання включає в себе створення резервних копій важливих даних, таких як корпоративна інформація, конфігурації систем та інші критичні ресурси мережі. Цей процес має бути ретельно спланованим і автоматизованим, щоб гарантувати регулярність та надійність. Резервні копії повинні зберігатися в безпечних місцях, захищених від фізичного та кібернетичного впливу. Під час втрати даних або ситуації відмови, швидке відновлення має вирішальне значення для уникнення простої та збереження продуктивності. Це включає відновлення даних з резервних копій та відновлення конфігурацій систем.[41]

Тестування процесів відновлення є важливим етапом у забезпеченні ефективності цієї стратегії. Регулярні вправи з відновлення допомагають перевірити, наскільки ефективно вони працюють та як швидко можна відновити мережеві сервіси після втрати даних чи конфігурацій. Резервне

копіювання та відновлення визначається як стратегічний елемент, який забезпечує надійність та стійкість мережі, забезпечуючи бізнес-процеси навіть в умовах виникнення непередбачених обставин. Загальна стратегія забезпечення безпеки повинна бути комплексною та поєднувати технічні, організаційні та фізичні заходи для максимальної ефективності у виявленні та запобіганні потенційним загрозам.

2.3 Масштабування та резервування

Масштабування в контексті мережі відноситься до можливості розширення ресурсів мережі для задоволення зростаючих потреб підприємства. Це може бути досягнуто різними способами, такими як додавання нових пристроїв, розширення пропускної здатності, використання балансування навантаження та інші техніки. Масштабування дозволяє мережі адаптуватися до зростаючого обсягу даних, користувачів та вимог до продуктивності. Важливо визначити потреби масштабування на етапі проектування мережі та впроваджувати рішення, які дозволять еластичність та масштабованість в майбутньому.[49]

Резервування стосується створення запасних або альтернативних ресурсів для забезпечення продуктивності та доступності в разі виникнення проблем або відмов. Це може включати в себе наявність резервних серверів, додаткових каналів передачі даних, дублювання мережевого обладнання та інші стратегії. Резервування грає критичну роль у забезпеченні стійкості мережі. Заходи резервування можуть включати автоматизоване перемикання на резервні пристрої у разі відмови, використання технологій балансування навантаження та створення планів відновлення для різних сценаріїв відмов. Забезпечення високого рівня доступності та надійності мережі вимагає інтеграції обох стратегій. Правильне масштабування разом із резервуванням гарантує, що

мережа може ефективно функціонувати навіть у випадку несподіваних подій чи зростаючих навантажень.[42]

Створення резервних копій даних надає можливість виконати відновлення інформації у випадку втрати оригіналу, з якого було створено резервну копію. Втрата, в даному випадку, визначається як подія, що спричинила зміну даних, внаслідок чого вони втратили свою цінність або були видалені з носія. Наприклад, це може стосуватися умисного завдання шкоди через видалення важливої для підприємства інформації.

Об'єкти резервного копіювання представляють собою дані або їх сукупність, з яких можна створити резервну копію. Такі об'єкти можуть включати файли або теки, дані прикладних програм, дані операційної системи чи саму операційну систему (наприклад, Windows System State або AIX System Backup), образи віртуальних машин та їхні диски, файлові системи тощо.[47]

Вимоги для відновлення даних:

Для визначення вимог до швидкості відновлення та періодичності створення резервних копій використовуються наступні терміни:

- Recovery Point Objective (RPO): Цільова точка відновлення, яка визначає періодичність створення резервних копій. Відновлення можливе лише на останню RPO у випадку втрати даних.

- Recovery Time Objective (RTO): Цільовий час відновлення, який визначає час від початку до завершення відновлення даних з резервної копії.

Для можливості відновлення під час катастрофи існують такі терміни:

- Disaster Recovery Point Objective (DRPO): Цільова точка відновлення під час катастрофи, що визначає RPO у разі настання катастрофи.

- Disaster Recovery Time Objective (DRTO): Цільовий час відновлення під час катастрофи, що визначає RTO у разі настання катастрофи.

Рівні резервного копіювання:

- Повне резервне копіювання (Full Backup або L0): Представляє собою повну копію всіх даних, що дозволяє забезпечити максимальну відповідність оригіналу.

- Диференційне резервне копіювання (Differential Backup або L1): Копіює зміни, які сталися після останньої повної копії, спрощуючи процес відновлення.

- Додаткове резервне копіювання (Incremental Backup або L2): Копіює зміни, які відбулись після останньої повної, диференційної або додаткової копії, що зменшує час копіювання, але може збільшити час відновлення.

- Lx (Level X): Стандарт опису методів резервного копіювання, де x вказує на рівень, що залежить від попереднього Lx-1 або Lx-n.

Важливо враховувати різні терміни та рівні для правильного планування та виконання процесів резервного копіювання та відновлення даних.

Цілісність резервних копій даних визначається відповідністю даних резервної копії та оригіналу на момент її створення. Якщо вибрати неправильний метод створення резервної копії, можливість успішного відновлення даних може бути обмеженою. З метою забезпечення цілісності резервних копій застосовуються різні методи, залежно від об'єкта резервного копіювання. Узагальнено, необхідно виконати кілька операцій:

1. Забезпечити незмінність даних під час створення копії, щоб перевірити відповідність створеної копії. Контрольні суми збереженої копії та оригіналу повинні співпадати.

2. Розблокувати дані для можливості читання. Операційна система може блокувати доступ навіть до спроб читання файлів з носія.

3. Виконати запис змін, здійснених у оперативній пам'яті, на жорсткий диск (у Linux - команда sync). Це необхідно для того, щоб усі зміни відобразилися на резервній копії.

Приклади включають в себе:

- Під час створення резервної копії файлів операційної системи Windows, доступ до деяких системних файлів може бути недоступним. Проте за

допомогою технології Volume Shadow Copy Services може виконуватися створення тіньової копії перед копіюванням.

- При створенні копії образу віртуальної машини VMware vSphere використовується програмне забезпечення VMware Tools для сповіщення операційної системи про підготовку даних до резервного копіювання, особливо, якщо використовується операційна система Windows, що ініціює запуск компонентів VSS.

Методи передачі резервних копій:

1. З використанням агента: Копіювання даних здійснюється через програмне забезпечення, встановлене на стороні системи, що виконує захист даних. Цей метод, хоча обтяжливий для адміністрування, надає можливість інтеграції у програмне середовище клієнта.

2. Off-host: Метод, що дозволяє створювати резервну копію без навантаження на клієнтську систему, зазвичай передаючи дані безпосередньо зі сховища даних на сервер резервного копіювання.

3. Serverless: Метод, який передбачає передачу даних від клієнта до сховища резервних копій без участі сервера резервного копіювання.

Методи створення копій даних:

1. Тіньова копія (Shadow Copy): Створення миттєвої копії з дискового розділу операційної системи, використовуючи властивості файлової системи.

2. Snapshot дисків: Замороження змін на основному диску та їх перенаправлення в окремий файл під час створення резервної копії.

3. Snapshot дискового розділу: Створення миттєвої копії даних безпосередньо на дисковому масиві, використовуючи можливості дискових масивів.

Сховища резервних копій:

- Стрічкова бібліотека або стример: Запис резервних копій на магнітну стрічку стримера. Має переваги в швидкості запису та відносно низькій

вартості зберігання, але обмежується повільним доступом та іншими недоліками.

- Дискове сховище: Запис резервних копій на диски, що можуть бути об'єднані в RAID або на дискову систему збереження. Забезпечує швидкий доступ до інформації та необмежену кількість одночасних операцій.

- Virtual Tape Library: Запис резервних копій на диски, але представляється клієнту як стрічкова бібліотека. Забезпечує швидкість доступу та більшу кількість одночасних операцій.

- "Хмарний" бекап: Запис резервних даних за технологією "хмари" через онлайн-служби. Має низьку вартість обслуговування, але обмежений швидкістю доступу та безпекою доступу до даних.

Розділ 3. Впровадження та управління

3.1 План впровадження

Попередній аналіз та підготовка до впровадження масштабованої комп'ютерної мережі для великого підприємства — це важливий етап, що визначається комплексним вивченням існуючої інфраструктури. Огляд обладнання, програмного забезпечення та топології дозволяє здійснити аналіз параметрів продуктивності, визначити сильні та слабкі сторони системи. Одночасно здійснюється активний збір бізнес-вимог від ключових представників підприємства. Це дозволяє визначити стратегічні цілі та завдання, які має вирішити нова мережа. Паралельно встановлюються ключові показники продуктивності, які відображатимуть ефективність мережі в контексті бізнес-процесів. Оцінка готовності персоналу до змін є також необхідною частиною попереднього аналізу. Це включає аналіз навичок та компетентності IT-персоналу, їхню готовність до оволодіння новими технологіями та взаємодії з новою мережевою інфраструктурою. Усі ці аспекти попереднього аналізу створюють основу для подальшого проектування та впровадження масштабованої комп'ютерної мережі, спрямованої на вирішення конкретних потреб та завдань великого підприємства.[46]

Проектування масштабованої комп'ютерної мережі для великого підприємства є ключовим етапом, на якому визначається технічна архітектура та функціональні можливості нової мережі. Взаємодія з керівництвом та відділом інформаційних технологій (IT) є першочерговим завданням. Зустрічі з ключовими представниками підприємства дозволяють зрозуміти їхні поточні проблеми та очікувані покращення. Важливо визначити стратегічні вимоги бізнесу та врахувати їх при подальшому проектуванні. Аналіз бізнес-процесів, що залежать від мережі, є важливою складовою процесу проектування. Ретельне вивчення того, як взаємодіють різні підрозділи підприємства через мережу, дозволяє ефективно визначити технічні вимоги до майбутньої мережі.

Визначення технічних вимог і характеристик мережі включає в себе розгляд аспектів, таких як пропускна здатність, безпека, доступність, модульність та інші. Це допомагає створити фундамент для технічного проектування та реалізації. Формулювання цілей та розробка документації є завершальним етапом проектування. Це включає в себе конкретизацію вимог, які були зібрані під час взаємодії з керівництвом та IT-відділом, та створення документа, який визначає майбутню мережу та визначає шлях до її впровадження.[40]

Вибір інфраструктурних рішень є важливим етапом у процесі проектування масштабованої комп'ютерної мережі для великого підприємства. На цьому етапі вирішуються ключові питання, пов'язані з технологічним стеком та обладнанням, яке буде використовуватися. Вибір технологій та обладнання вимагає ретельного аналізу вимог, що були сформульовані на попередніх етапах. Це включає в себе розгляд різних типів комутаторів, маршрутизаторів, бездротових точок доступу та іншого обладнання, яке відповідає потребам мережі. Розгляд систем мережевого управління також є важливою частиною цього етапу. Вибір оптимального рішення для мережевого управління грає критичну роль у забезпеченні ефективності, безпеки та масштабованості мережі. Укладання договорів з постачальниками технічних засобів та послуг є практичним аспектом вибору інфраструктурних рішень. Це включає в себе переговори з виробниками обладнання, постачальниками програмного забезпечення та іншими сторонами, щоб забезпечити оптимальні умови для реалізації проекту. На етапі вибору інфраструктурних рішень ключовою метою є створення технічної основи, яка відповідає бізнес-вимогам і забезпечить ефективне функціонування мережі в майбутньому.[44]

Впровадження та налаштування – це етап, на якому концепції та плани перетворюються в реальну фізичну інфраструктуру. Цей процес включає кілька ключових кроків, які спрямовані на створення функціональної та оптимізованої мережі для великого підприємства. Фізична реалізація мережі та інтеграція нового обладнання включає в себе розгортання комутаторів, маршрутизаторів,

бездротових точок доступу та інших пристроїв. Це може вимагати фізичного підключення кабелів, монтажу обладнання в серверних кімнатах та інших місцях. Важливо дотримуватися проектного плану та впевнитися, що реалізація відбувається у відповідності до зазначених технічних вимог. Встановлення та налаштування систем мережевого управління є критично важливим етапом для забезпечення ефективності та безпеки мережі. Це включає встановлення програмного забезпечення для моніторингу, керування та виявлення проблем в мережі. Налаштування систем управління також може включати в себе встановлення політик безпеки, створення резервних копій конфігурацій та інші аспекти, що забезпечують ефективну роботу мережі. Тестування та відлагодження нової мережі – це процес перевірки всіх компонентів мережі для переконання, що вони працюють правильно та взаємодіють між собою без проблем. Це включає в себе проведення тестів продуктивності, перевірку безпеки та ідентифікацію можливих проблем. У випадку виявлення неполадок чи відхилень від визначених стандартів, здійснюється коригування та додаткове тестування для забезпечення якості та надійності мережі.[43]

Етап "Навчання та перехід" є ключовим у впровадженні нової мережі, оскільки від нього залежить успіх та ефективність усього процесу. На цьому етапі акцент робиться на підготовці персоналу та максимальній підтримці для зручного та безперервного переходу до нової інфраструктури. Один із ключових аспектів цього етапу - це забезпечення персоналу необхідними навичками та знаннями для роботи з новими технологіями та системами управління мережею. Тренінгові курси охоплюють різні аспекти, від роботи з новим обладнанням до вивчення політик безпеки та оптимального використання ресурсів. Під час переходу до нової мережі важливо мати ефективну систему підтримки для оперативного вирішення питань та виявлення можливих проблем. Забезпечення надійної системи відгуку на запитання персоналу та користувачів допомагає уникнути затримок та зберегти продуктивність під час перехідного періоду. Завершення етапу "Навчання та

перехід" включає проведення тестування в міру впровадження нових рішень. Тестування дозволяє виявити та виправити можливі проблеми, забезпечуючи найвищу якість функціонування нової мережі.

Запуск систем моніторингу є важливим етапом, оскільки він дозволяє постійно контролювати роботу мережі та негайно реагувати на будь-які аномалії чи проблеми. Оцінка результатів етапу "Навчання та перехід" надає можливість визначити вдачі та виявити аспекти, які можна покращити. Звіт з цього етапу є цінним інструментом для прийняття рішень та вдосконалення всього процесу впровадження нової мережі.[49]

Після успішного впровадження нової мережі починається етап моніторингу та оптимізації, який спрямований на забезпечення ефективності, безпеки та надійності мережевої інфраструктури протягом тривалого періоду. Цей етап є критичним для того, щоб виявляти можливості для поліпшення та гарантувати високий рівень продуктивності. На цьому етапі важливо встановити системи моніторингу, які будуть постійно відстежувати ключові показники ефективності мережі. Це може включати в себе моніторинг пропускної здатності, витрат ресурсів, роботи обладнання та інші параметри. Запуск таких систем дозволяє оперативно реагувати на можливі проблеми та попереджати їх до їх виникнення.[52]

Моніторинг не лише допомагає виявляти проблеми, але й надає дані для аналізу та визначення можливостей для оптимізації. Це може включати удосконалення конфігурацій обладнання, вдосконалення алгоритмів маршрутизації, розширення пропускної здатності та інші заходи, що підвищують ефективність мережі. Сучасна мережева інфраструктура потребує постійного оновлення для забезпечення сумісності з новими технологіями та забезпечення безпеки. Регулярні оновлення програмного та апаратного забезпечення, а також патчі для виправлення потенційних уразливостей, є необхідним елементом забезпечення безпеки та стабільності мережі. Ефективний моніторинг дозволяє оперативно реагувати на ризики та зміни в

середовищі мережі. Здатність адаптуватися до нових умов та забезпечувати безперервну роботу системи стає ключовою для успішного функціонування мережі в динамічному бізнес-середовищі.[51]

Оцінка ефективності є важливим етапом в життєвому циклі мережевого проекту, оскільки вона дозволяє визначити, наскільки добре мережа відповідає бізнес-потребам та чи досягає поставлених цілей. Цей процес включає в себе регулярні оцінки та вдосконалення для забезпечення оптимальної продуктивності та надійності. Аудит продуктивності та безпеки є ключовим елементом оцінки ефективності мережі. Під час аудитів оцінюються параметри, такі як пропускна здатність, час відновлення в разі відмови, ефективність заходів безпеки та інші фактори. Регулярні аудити дозволяють виявляти можливі слабкі місця та негайно реагувати на них. Фідбек від користувачів та іТ-спеціалістів, які працюють з мережею, надає цінну інформацію про реальний досвід використання системи. Аналіз цього фідбеку дозволяє виявляти проблеми та вимагає змін, щоб мережа відповідала потребам користувачів та бізнесу.[50]

Основною метою оцінки ефективності є вдосконалення. На основі результатів аудитів та фідбеку виробництва приймаються рішення щодо оптимізації стратегій, покращення технічних рішень та вдосконалення конфігурацій мережі. Цей цикл постійних покращень сприяє тому, щоб мережа залишалася адаптованою до змінних вимог бізнесу та технологічних інновацій.

План впровадження мережі повинен бути гнучким та пристосовуватися до конкретних умов та вимог підприємства. Ключовою метою є забезпечення безперебійної роботи мережі та задоволення бізнес-потреб підприємства.

3.2 Система мережевого управління

Система мережевого управління (СМУ) – це ключовий компонент сучасних інформаційних систем, що відповідає за ефективне контролювання та

адміністрування мережевою інфраструктурою. Вона забезпечує іТ-спеціалістам та адміністраторам можливість керування різними аспектами мережі, моніторингу та вдосконалення її продуктивності, а також виявлення та вирішення проблем. Система моніторингу та аналізу продуктивності у мережевому управлінні є критично важливим інструментом для ефективного функціонування інформаційних систем. Однією з ключових функцій цієї системи є надання детальної інформації про роботу мережі, її ресурсів та ефективності в режимі реального часу. Система моніторингу забезпечує постійний збір даних з різних точок мережі. Це може включати в себе інформацію про трафік, завантаження обладнання, використання ресурсів, стан з'єднань та інші параметри, які визначають продуктивність мережі.[53]

Система аналізу даних визначає найбільш важливі та ризиковані аспекти роботи мережі. Алгоритми аналізу допомагають виявляти аномалії, перевищення нормативів чи інші проблеми, що можуть впливати на продуктивність мережі. Система може надсилати автоматичні повідомлення адміністраторам або вживати інших заходів у випадку виявлення критичних або підозрілих подій. Це може включати автоматичне вилучення або перерозподіл обтяжених ресурсів, блокування атак або інші заходи для забезпечення надійності мережі. Система виявляє та аналізує використання пропускної здатності мережі, що дозволяє планувати її оптимізацію. Це може включати в себе виявлення проблемних сегментів, рекомендації щодо підвищення ефективності трафіку та інші заходи для оптимізації роботи мережі. Система забезпечує адміністраторам можливість спостереження за мережею в реальному часі. Це дозволяє оперативно реагувати на зміни, а також вдосконалювати та оптимізовувати роботу мережі в реальному часі. В цілому, система моніторингу та аналізу продуктивності грає ключову роль у забезпеченні ефективності, надійності та безпеки мережі, дозволяючи оперативно реагувати на зміни та удосконалювати інфраструктуру для задоволення потреб бізнесу.

Керування конфігурацією в мережевому управлінні є критично важливою функцією, яка дозволяє забезпечити стабільність та ефективність мережевого середовища. Ця система спрощує та стандартизує процес управління конфігурацією пристроїв, забезпечуючи централізовану контрольованість та безпеку. Система керування конфігурацією дозволяє зберігати та організовувати конфігураційні файли пристроїв у централізованій базі даних. Це робить процес управління конфігурацією більш ефективним та забезпечує можливість відновлення пристроїв до попередніх стабільних станів у випадку виникнення проблем чи збоїв. Адміністратори можуть вносити зміни в конфігурацію пристроїв через централізований інтерфейс, який забезпечує єдинообразний та безпечний спосіб взаємодії з різними типами обладнання. Це уніфікує процес управління конфігурацією та дозволяє уникнути помилок, що можуть виникнути при ручних змінах на пристроях. У випадку збоїв або помилок, система керування конфігурацією надає можливість швидко відновити оптимальні налаштування пристроїв за допомогою збережених конфігурацій. Це робить процес відновлення пристроїв більш швидким та ефективним.[54]

Система здатна вести журнали змін конфігурацій, що дозволяє адміністраторам відстежувати, хто та коли вносив зміни. Це сприяє підвищенню безпеки та дозволяє швидше виявляти та виправляти неправильні зміни чи недоліки в конфігураціях.

Система забезпечує можливість синхронізації конфігурацій між різними пристроями у мережі. Це гарантує, що всі пристрої мають однакові налаштування та працюють в єдинообразному стані, запобігаючи невідповідності та конфлікти. Загалом, система керування конфігурацією в мережевому управлінні є необхідним інструментом для забезпечення стабільності, надійності та ефективності мережевого середовища.

Діагностика та відлагодження в системі мережевого управління (СМУ) відіграють ключову роль у забезпеченні ефективності та надійності мережі. Ця

функція дозволяє оперативно виявляти та вирішувати проблеми, що можуть виникати в ході роботи мережі, забезпечуючи швидке відновлення та уникнення втрат продуктивності. Система мережевого управління використовує різноманітні інструменти діагностики, такі як мережеві сканери, протоколери, аналізатори трафіку та інші. Ці інструменти дозволяють здійснювати моніторинг різних параметрів мережі та виявляти аномалії, помилки або несправності. Система автоматизовано визначає та локалізує проблеми в мережі, використовуючи дані, зібрані з різних пристроїв. Це дозволяє адміністраторам швидко виявляти точку відмови чи конфлікт, що допомагає зберегти час при усуненні несправностей.[29]

Система автоматично здійснює відлагодження, або ж адміністратор може використовувати інтерфейс системи для аналізу причин проблем та вживання заходів для їх усунення. Це може включати перевірку конфігурацій, аналіз журналів подій, ідентифікацію вузьких місць та оптимізацію параметрів мережі. У деяких випадках, СМУ може автоматично реагувати на виявлені проблеми, намагаючись вирішити їх без участі адміністратора. Це може включати перенаправлення трафіку, виключення несправних пристроїв чи автоматичну зміну налаштувань. Система може також включати в себе механізми резервування, які автоматично вводяться в дію в разі виявлення проблеми. Це може бути автоматичне переключення на резервний шлях або використання резервних ресурсів. Діагностика та відлагодження в системі мережевого управління допомагають забезпечити стабільність мережі та зберегти високу продуктивність в умовах змін і викликів.[36]

Автоматизація задач є важливою складовою системи мережевого управління, оскільки дозволяє ефективно виконувати рутинні операції та оптимізувати роботу мережі. Система мережевого управління автоматизує процес резервного копіювання конфігурацій пристроїв в мережі. Це забезпечує зручний спосіб відновлення конфігурацій у випадку втрати даних або несправності обладнання. Автоматичне резервне копіювання може

виконуватися за графіком або при виявленні змін у конфігураціях. Система автоматично виявляє аномалії та атаки в мережі, використовуючи алгоритми моніторингу та аналізу трафіку. Після виявлення аномалії система може автоматично вживати заходів для її усунення або повідомляти адміністратора для подальшого аналізу та втручання.[48]

Мережеве управління може автоматизувати процес внесення змін у конфігурації пристроїв. Це може включати додавання нових пристроїв, зміну налаштувань маршрутизації, оновлення програмного забезпечення та інші операції. Автоматичні зміни можуть виконуватися згідно попередньо заданих сценаріїв або за умови певних подій. Система мережевого управління може автоматично оптимізувати використання ресурсів в мережі. Це включає в себе автоматичне балансування навантаження, налаштування параметрів маршрутизації та інші операції, спрямовані на підвищення ефективності роботи мережі. Система може автоматично керувати обладнанням, включаючи введення нових пристроїв, зміни конфігурацій, відключення несправного обладнання та інші операції. Це спрощує рутинні завдання адміністрування та дозволяє ефективно впоратися із зростаючим обсягом роботи. Автоматизація задач в мережевому управлінні забезпечує швидке реагування на зміни у мережі, покращує продуктивність та дозволяє адміністраторам ефективно використовувати свій час для вирішення стратегічних завдань.[10]

Безпека мережі в контексті системи мережевого управління (СМУ) є критичним аспектом для забезпечення інтегритети, конфіденційності та доступності даних і ресурсів в мережі. СМУ використовує системи виявлення інтрузій (IDS) та інші механізми для виявлення аномального або зловмисного трафіку в мережі.

Це може включати виявлення атак, спроб несанкціонованого доступу, вразливостей у конфігураціях та інші потенційні загрози. Система мережевого управління встановлює правила та політики безпеки для запобігання різноманітним атакам. Це може включати налаштування брандмауерів,

фільтрацію трафіку, контроль доступу та інші заходи, спрямовані на захист мережі від несанкціонованого доступу та атак.[55]

СМУ керує правами доступу користувачів до мережевих ресурсів. Це включає в себе аутентифікацію та авторизацію користувачів, обмеження прав доступу в залежності від ролей та обов'язків. Управління доступом допомагає уникнути несанкціонованого використання чутливої інформації та ресурсів.

Система мережевого управління забезпечує можливість шифрування даних, які передаються по мережі. Це допомагає захистити конфіденційну інформацію від несанкціонованого перегляду чи зміни під час передачі через відкриті мережі. СМУ веде журнали подій та аудиту для реєстрації подій в мережі. Це включає в себе виявлення та реагування на важливі події, виявлення порушень безпеки та реєстрацію взаємодій користувачів з мережевим обладнанням. Система мережевого управління регулярно оновлюється для врахування нових загроз і вразливостей. Це включає в себе оновлення програмного забезпечення, встановлення патчів безпеки та інші заходи, спрямовані на підтримання високого рівня безпеки. Безпека мережі через систему мережевого управління стає основним аспектом для захисту даних та забезпечення стійкості мережевого середовища.[24]

Масштабованість та оптимізація у контексті системи мережевого управління (СМУ) представляють собою важливі аспекти для забезпечення ефективності та відповідності мережевої інфраструктури зростаючим вимогам бізнесу. СМУ надає засоби для легкого масштабування мережевої інфраструктури відповідно до росту бізнес-потреб. Це може включати в себе додавання нових пристроїв, розширення пропускної здатності та інші масштабувальні заходи, які дозволяють мережі розвиватися разом з компанією. СМУ використовує різні механізми для оптимізації використання ресурсів мережі. Це може включати в себе розподіл ресурсів в залежності від завдань, використання технологій віртуалізації та інші методи для забезпечення ефективного використання доступних потужностей.[21]

Система мережевого управління забезпечує аналіз трафіку в мережі, що дозволяє ідентифікувати обсяги та напрямки трафіку. На основі цього аналізу можна впроваджувати оптимізації, такі як балансування навантаження, підтримка резервних шляхів та інші заходи для покращення продуктивності мережі. Софтверно-визначена мережа (SDN) та функції мережі, віртуалізовані на функції (NFV), використовуються для створення більш гнучких та ефективних мережевих середовищ. Це дозволяє швидше впровадження нових сервісів та адаптацію мережі до змін у бізнес-вимогах. СМУ використовує автоматизацію для виконання рутинних операцій, таких як налаштування, моніторинг та управління мережевим обладнанням. Це допомагає прискорити відповідь на змінні умови та заощаджує час та ресурси IT-персоналу. Система мережевого управління дозволяє встановлювати та контролювати параметри якості обслуговування для різних видів трафіку. Це дозволяє надавати пріоритети для різних видів даних, що забезпечує ефективніше використання мережевих ресурсів. Загалом, система мережевого управління грає важливу роль у створенні масштабованих, гнучких та оптимізованих мережевих інфраструктур, які можуть ефективно відповідати потребам сучасного бізнесу.
Зменшення часу відгуку є важливим аспектом управління мережею. Для досягнення цієї мети використовуються різні стратегії та функції систем мережевого управління.[23]

Система мережевого управління (СМУ) забезпечує моніторинг та аналіз продуктивності, що дозволяє оперативно виявляти та реагувати на проблеми в мережі. Автоматизація виявлення проблем та аналіз дозволяють визначати аномалії та реагувати на них без значного втручання адміністраторів. Керування конфігурацією є ще однією важливою функцією. Система мережевого управління дозволяє тримати під контролем конфігурації всіх пристроїв в мережі, що сприяє швидкому відновленню оптимальних налаштувань у випадку виникнення проблем. Діагностика та відлагодження є невід'ємною частиною забезпечення швидкого відгуку. СМУ допомагає

ідентифікувати та локалізувати проблеми в мережі, використовуючи інструменти діагностики та відлагодження.

Автоматизація задач є ефективним засобом зменшення часу відгуку. Це включає в себе автоматизоване резервне копіювання конфігурацій, виявлення та усунення аномалій, а також виконання змін у конфігурації пристроїв. Безпека мережі є ключовим аспектом. СМУ дозволяє виявляти потенційні загрози та вживати заходів для їх запобігання. Це включає в себе моніторинг та управління правами доступу до різних ресурсів. Масштабованість та оптимізація мережі є важливими аспектами забезпечення швидкого реагування на змінні потреби бізнесу. Система мережевого управління дозволяє ефективно масштабувати і оптимізувати мережеву інфраструктуру. Загальний підхід до зменшення часу відгуку полягає у використанні інструментів моніторингу, автоматизації та ефективного управління мережею для швидкого виявлення, відладження та вирішення проблем.[45]

Підвищення продуктивності мережі є важливою метою для багатьох організацій, оскільки це безпосередньо впливає на швидкодію, доступність та загальну ефективність бізнес-процесів. Система мережевого управління відіграє ключову роль у досягненні цієї мети, надаючи комплексний підхід до контролю, аналізу та оптимізації мережевої інфраструктури.

Ефективне управління ресурсами включає в себе раціональне використання обладнання, пропускної здатності та інших мережевих ресурсів. Система моніторингу та аналізу продуктивності дозволяє оперативно виявляти та вирішувати ефективність проблем, уникати перевантажень та оптимізувати роботу мережі для максимальної продуктивності.

Швидке виявлення та усунення несправностей є ще однією ключовою складовою підвищення продуктивності. Система мережевого управління забезпечує постійний моніторинг стану мережі та оперативну реакцію на будь-які аномалії чи проблеми. Це дозволяє уникнути відмов, покращити надійність мережі та забезпечити стабільну роботу бізнес-процесів. Загально кажучи,

система мережевого управління є важливим інструментом для забезпечення оптимальної ефективності мережі та відповіді на виклики, які можуть виникнути у сучасному інформаційному середовищі.[39]

Підвищення безпеки є однією з найбільш критичних аспектів управління мережею, оскільки у сучасному світі загрози кібербезпеки постійно зростають як за складністю, так і за частотою. Система мережевого управління грає ключову роль у забезпеченні безпеки мережі, надаючи інструменти для виявлення, аналізу та реагування на потенційні загрози. Забезпечення виявлення загроз включає в себе постійний моніторинг мережі на предмет аномалій, невідповідностей та незвичайної активності. Система мережевого управління використовує різноманітні методи та алгоритми, щоб виявити потенційні загрози та надати оперативну інформацію для прийняття рішень. Реакція на загрози включає в себе ряд заходів, таких як автоматичне відключення від мережі компрометованих пристроїв, відправлення повідомлень адміністраторам про інциденти безпеки, а також ізоляцію частини мережі для запобігання подальшому розповсюдженню загроз. Загалом, підвищення безпеки мережі завдяки системі мережевого управління допомагає зменшити ризики, пов'язані з кіберзагрозами, та забезпечує надійний захист конфіденційності, цілісності та доступності даних у мережі.

Оптимізація конфігурацій через автоматизоване управління стає стратегічним рішенням для сучасних мереж. Цей підхід спрощує та ускладнює адміністрування мережі, роблячи її більш гнучкою та ефективною.

Забезпечуючи автоматичні зміни та уніфікацію конфігурацій, система мережевого управління забезпечує надійність, швидкість та високу стійкість всієї інфраструктури. Автоматизоване управління конфігураціями не лише полегшує завдання адміністраторів, але і впливає на безпеку мережі. Заходи безпеки можуть бути легко впроваджені та моніторені, забезпечуючи вчасне реагування на потенційні загрози. Також, цей підхід дозволяє ефективно керувати змінами та вдосконалювати роботу мережі відповідно до бізнес-

потреб. Відсутність ручного втручання сприяє уникненню помилок та забезпеченню стабільності операцій. У підсумку, оптимізація конфігурацій через автоматизоване управління стає ключовим аспектом для забезпечення ефективності, безпеки та адаптивності мережі до зростаючих вимог у світі інформаційних технологій.[37]

Підтримка масштабованості в системі мережевого управління є ключовою для сучасних організацій, які стикаються з постійним зростанням обсягів даних та розширенням своєї інфраструктури. Системи мережевого управління надають необхідні інструменти для ефективного справляння з цими викликами.

Однією з ключових переваг є здатність швидко виявляти та інтегрувати нові пристрої та компоненти в мережу. Це дозволяє організаціям легко розширювати свою інфраструктуру, додаючи нові ресурси та технології для відповіді на зростання потреб. Крім того, системи мережевого управління надають засоби для ефективного розподілу ресурсів та оптимізації роботи мережі при збільшенні навантаження. Це включає в себе розподіл пропускної здатності, оптимізацію маршрутів та інші стратегії, що дозволяють підтримувати ефективність мережі при змінних обсягах даних.

Забезпечення масштабованості також включає в себе планування на майбутнє та визначення стратегій розвитку мережі. Системи мережевого управління допомагають аналізувати потреби та прогнозувати зростання, щоб забезпечити стабільність та гнучкість в обличчі змін. Загалом, СМУ виступає як невід'ємна складова для ефективного та безпечного управління сучасною мережею.

Методи мережевого аналізу та управління є важливими для розробки нових продуктів і технологій як у традиційних галузях, де зазвичай відбуваються поетапні інновації, так і в нових, швидко розвиваючихся сферах. Мережеве співробітництво виступає ключовим інструментом як для мобілізації ресурсів, так і для більш ефективного використання існуючих.

На практиці, застосування мережевого підходу в логістиці дозволяє використовувати графічні методи планування, поєднуючи їх з елементами імовірнісних моделей для прогнозування тривалості окремих етапів робіт.

Система мережевого планування і управління (СПУ) є набором науково обґрунтованих принципів організації та управління виробництвом, що ґрунтується на моделюванні процесів за допомогою мережевого графіка, використовуючи теорію графів, теорію ймовірностей і комп'ютерні технології.

Система СПУ дозволяє створювати календарний план для складного комплексу робіт, визначати та мобілізувати резерви часу, попереджати можливі зриви в ході робіт і здійснювати оперативне коригування планів.

Спочатку розробка СПУ була обумовлена потребою обгрунтованого прогнозу терміну завершення великих бізнес-проектів, проте з розвитком цих систем і комп'ютерних технологій вони стали використовуватися для рішення різноманітних завдань. Як засіб ефективного планування та управління, мережеві методи вирізняються своєю простотою і доступністю, що сприяло їх швидкому впровадженню на практиці. Зараз СПУ може застосовуватися як у формі одноразового використання мережевих методів і моделей, так і як постійна система, яка є складовою більш складних систем управління. У цьому випадку методи СПУ поєднуються з економіко-математичними методами, особливо в тих випадках, коли використання мережевих моделей є особливо ефективним (наприклад, в теорії масового обслуговування).

Переваги СПУ є значущими, оскільки ця система дозволяє:

- Створювати календарний план для складних бізнес-проектів.

- Визначати та мобілізувати резерви часу та ресурсів.

- Забезпечувати точне виконання проекту в узгоджені терміни.

- Реалізовувати логістичний принцип "точно в термін" з попередженням можливих зривів.

- Здійснювати оперативне впровадження бізнес-проекту.

- Підвищувати ефективність менеджменту через чітку розподіл відповідальності та делегування повноважень.

Особливістю методів СПУ є моделювання всього комплексу робіт, виявлення критичних точок, що найбільше впливають на виконання проекту, та оптимізація управління роботами.

Основним компонентом у системі СПУ є мережева модель, що деталізує план виконання взаємопов'язаних робіт на різних рівнях, виражаючи його у специфічній формі мережі. Мережевий графік надає наочне відображення послідовності та взаємозв'язку всіх робіт, що виконуються у процесі розробки, і результатів, які досягаються до завершення.

Системи СПУ можуть бути здійснені з використанням детермінованих чи імовірнісних моделей. У всіх моделях застосовуються загальні принципи:

- Для кожного об'єкта створюються мережеві графіки, які є умовними економіко-математичними моделями, відображаючи хід виконання робіт від початку до завершення.

- Терміни виконання робіт на окремих етапах визначаються з урахуванням кінцевого терміну.

- При створенні мережевого графіка використовуються такі вихідні матеріали, як завдання на проектування, проектно-конструкторська документація, проекти виконання робіт, активні технологічні процеси, графіки поставок ресурсів, обладнання та документації.

Основними елементами мережевого графіка є поняття події та роботи. Термін "робота" охоплює набір дій, необхідних для виконання завдання чи досягнення мети. Робота поділяється на роботу-дію, роботу-очікування та залежність (фіктивну роботу).

- Робота-дія - це процес, що відбувається в часі і вимагає ресурсних витрат. Кожна робота-дія конкретна, визначена та має відповідального виконавця. Вона переносить подію в іншу і зображується суцільною лінією зі стрілкою на мережевому графіку.

- Робота-очікування - це процес, що відбувається в часі, але не потребує ресурсних витрат. Вона також переносить подію в часі і зображується суцільною лінією зі стрілкою.

- Залежність (фіктивна робота) вказує на логічний зв'язок між подіями, не вимагаючи ресурсів, але показує, що можливість початку однієї роботи безпосередньо залежить від результатів іншої.

Поняття "подія" відображає результат, стан чи момент завершення процесу, яким закінчується конкретна робота. Подія відображає етап виконання комплексу робіт, і цей результат має бути достатнім для початку наступної роботи. Подія відображається як моментальна, безтривала, і визначається результатами всіх безпосередньо попередніх робіт.

Події можуть бути розподілені на прості та складні. Проста подія визначається результатом виконання лише однієї роботи, у той час як складна подія включає в себе результати двох чи більше робіт. Серед подій виокремлюють вихідні та завершальні. Початкова подія не має попередніх робіт і подій, що відносяться до відображеного в мережевій моделі комплексу робіт. Завершальна подія, навпаки, не має наступних робіт і подій.

У випадку відсутності числових оцінок в мережевій моделі, вона вважається структурною. Однак у більшості випадків використовуються мережі, в яких визначені тривалості робіт (виражені у годинах, тижнях, місяцях тощо над відповідними стрілками), а також оцінки інших параметрів (трудомісткість, вартість).

Орієнтація та розміри стрілок (топологія мережі) не мають принципового значення, так само як і масштаб мережевого графіка. При побудові мережевого графіка слід дотримуватися кількох загальноприйнятих правил:

1) Тільки вихідні події не повинні мати вхідних стрілок, що означає, що жодна подія (за винятком вихідної) не повинна бути безпосередньо передумовою жодної роботи.

2) Тільки завершальні події не повинні мати вихідних стрілок, тобто не повинно бути подій, з яких не виходить жодна робота, за винятком завершальної.

3) Кожна робота повинна мати попередню і наступну події.

4) Не повинно бути контурів та петель, які з'єднують події з ними ж самими, оскільки це вказує на те, що умовою початку деякої роботи є її ж закінчення.

5) Будь-які дві події повинні бути безпосередньо пов'язані не більше ніж однією роботою. Порушення цієї умови призводить до появи паралельних робіт на мережевому графіку, які можуть суттєво відрізнятися за використаними ресурсами. Для усунення цього порушення вводиться фіктивна подія, фіктивна робота, і одна з паралельних робіт замикатиметься на цю фіктивну подію.

Таблиця 3.1 Комплекс робіт підготовки виробництва та виготовлення виробу

Номер події	**Цифри робіт**	**Тривалість робіт, тижнів**	**Найменування і зміст робіт**
1	1	-	0
2	2	1-2	Розробка технічного проекту
3	3	3 січня	6
4	3	2-3	Розробка робочого проекту
5	4	1-4	Розробка та узгодження технічних умов
6	4	2-4	Підтвердження погодження технічних умов
7	5	2-5	Експериментальні роботи
8	6	4-6	Розробка інструкцій з експлуатації виробу
9	6	5 (12	Аналіз підсумків експериментальних

			робіт
10	7	2-7	Матеріальне забезпечення виробництва
11	7	3-7	Розробка технологічних процесів
12	7	5-7	Підтвердження замовлень від покупців
13	8	6-8	Навчання персоналу експлуатації і вироби
14	8	7-8	Заготівельні операції та обробка
15	3 вересня	9	Забезпечення контрагентскіх поставок
16	9	7-9	Виготовлення штатних запчастин
17	9	8-9	Загальна збірка і відвантаження вироби замовнику

Виділяючи певні події та пов'язуючи їх роботами, необхідно створити та організувати мережевий графік. З переліку робіт випливає, що подія 1 є вихідною для мережевого графіка, оскільки до неї не має жодних попередніх робіт, а завершальною є подія 9, оскільки за нею не слідує жодна робота.

Зазвичай на мережевих графіках часовий прогрес відображається зліва направо. Таким чином, розмістимо подію 1 ліворуч на графіку, а подію 9 - праворуч. Між ними розташуємо проміжні події в порядку їх номерів.

Впорядкування мережевого графіка передбачає таке розташування подій та робіт, при якому для будь-якої роботи попередню подію розташовано ліворуч та має менший номер порівняно з завершальною подією для цієї роботи. Усі роботи спрямовані зліва направо, від подій із меншими номерами до подій із більшими номерами.

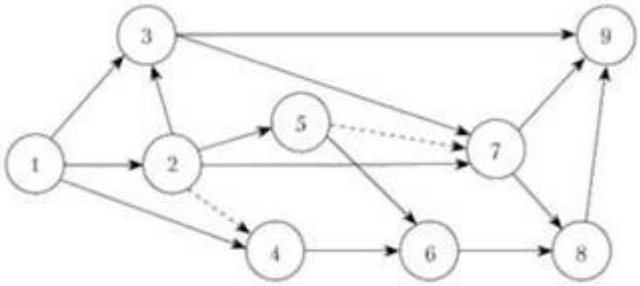

Рис.3.1 Початковий варіант мережного графіка

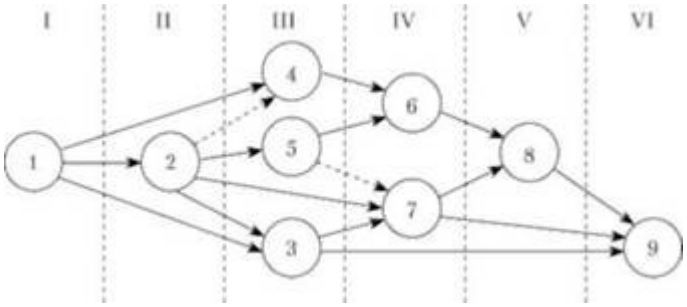

Рис.3.2 Процес упорядкування мережного графіка

Розмістивши початкову подію 1 в шарі I, припустимо, що ми викреслюємо цю подію на рисунку 4.6 та проводимо стрілки виходу з неї. Після цього залишається подія 2 без вхідних стрілок, і ми розмістимо її в шарі II. Виключивши подію 2 з виходом відповідних робіт, ми виявимо, що без вхідних стрілок залишаються події 3, 4, 5, які утворять шар III. Проведемо подальші операції видалення подій 3, 4, 5 із відповідними роботами, і отже, в шарі IV виявляться події 6 і 7. Після вилучення останніх без вхідних стрілок з'явиться подія 8 в шарі V. Після аналогічних дій у шарі VI ми досягнемо завершальної події 9. Тепер ми можемо легко зобразити остаточний вигляд графіка, вказавши тривалість всіх робіт.

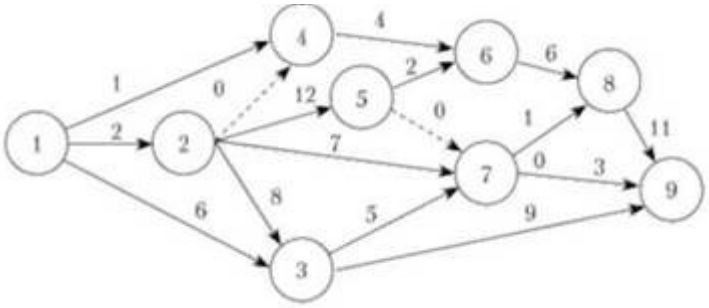

Рис.3.3 Упорядкований мережевий графік

Важливо відзначити, що впорядкований графік інтуїтивно і чітко відображає послідовність подій і робіт. У складних мережах впорядкування графіка стає обов'язковою умовою для подальшого аналізу. Грамотно структурований графік завжди може бути упорядкованим, що не можна сказати про графік, який містить петлі та контури.

Люба тривалість робіт, яка починається з початкової події і завершується кінцевою подією, отримує назву "шлях". Довжина (тривалість) будь-якого шляху дорівнює сумі тривалостей всіх входящих робіт. У мережі всі шляхи необхідні для досягнення кінцевої мети, оскільки всі роботи, які знаходяться на цих шляхах, повинні бути виконані.

Шлях, що виявляється найбільш тривалим у мережевому графіку, називається критичним. У нашому випадку цей критичний шлях включає події 1-2 - 3 - 7 - 8 - 9. Також події та роботи, що розташовані на цьому критичному шляху, отримують назву критичних. Шляхи, тривалість яких приблизно рівна тривалості критичного шляху, називають підкритичними, тоді як інші шляхи вважаються ненапруженими.

Критичний шлях є ключовим поняттям у системі планування та управління проектами. Основною метою аналізу мережевого графіка за часовим критерієм є визначення загальної тривалості всього комплексу робіт. Загальна тривалість визначається не всіма роботами мережі, а лише тими, які знаходяться на критичному шляху. Збільшення тривалості чи затримка

виконання будь-якої критичної роботи веде до затримки завершення всього комплексу робіт. Тому важливо приділяти особливу увагу своєчасному виконанню критичних робіт та забезпеченню їх необхідними ресурсами для витримки планового графіку. Якщо критичний шлях за вихідним графіком виявляється довшим за плановий термін, необхідно шукати можливості скорочення саме критичних робіт для виправлення ситуації. Це і є суть логістики в методології управління проектами.

У випадку, коли тривалість робіт не є фіксованою, кожна робота оцінюється за оптимістичною (мінімально можливий термін), песимістичною (максимально можливий термін), найбільш ймовірною тривалістю (час виконання в нормальних умовах) та очікуваною тривалістю (визначається на основі попередніх оцінок).

Вихідна інформація мережевої моделі включає:

- Мережу з початковою подією 1 та завершальною подією 9, яка є єдиним цільовим елементом моделі;

- Тривалість кожної з робіт, що представлені в мережі, де фіктивним роботам відповідає нульова тривалість.

Крім того, вихідна інформація включає момент початку виконання комплексу робіт (момент початкової події) та планований термін завершення всіх робіт (момент завершальної події).

Будь-який план чітко визначає момент завершення комплексу робіт. Якщо заданий плановий термін, то критичний шлях не повинен перевищувати цей термін. Якщо тривалість критичного шляху не перевищує плановий термін або якщо ця інформація відсутня, то такий план є прийнятним і його виконання реально. При цьому моменти початку та завершення робіт можуть варіюватися в певних межах, і при аналізі мережевого графіка визначаються параметри, які обмежують ці варіації.

Для кожної події визначаються:

- Тривалість раннього настання (Тр) - найраніший можливий момент настання події при заданих тривалості роботи і початковому моменті без урахування планового терміну завершення комплексу робіт. Ранній термін настання визначається тривалістю максимального шляху, що передує даній події;

- Тривалість пізнього настання (Тп) - найпізніший можливий момент настання події, за якого ще можливе виконання всіх наступних робіт з дотриманням планового терміну завершення комплексу робіт. Пізній термін настання визначається різницею між тривалістю критичного шляху та тривалістю наступного шляху, який веде до завершальної події мережі;

- Резерв часу (К) - можливий часовий інтервал, на який можна затримати подію без збільшення тривалості всього комплексу робіт. Резерв часу визначається як різниця між пізнім і раннім термінами настання події.

Таблиця 3.2 Тимчасові параметри подій

Подія	**Ранній термін (Тр)**	**Пізній термін (Тп)**	**Резерв часу (R)**
1	0	0	0
2	2	3	1
3	10	10	0
4	2	15	13
5	11	15	4
6	16	19	3
7	-	15	0
8	25	25	0
9	36	36	0

Для кожної роботи встановлюються наступні параметри:

- Ранній термін початку роботи (Тр) - найменший можливий момент початку роботи при визначених тривалості та початковому моменті. Тр збігається з раннім терміном настання початкової події роботи.

- Ранній термін закінчення роботи (Тз) - найменший можливий момент завершення роботи при визначених тривалості та початковому моменті. Цей термін перевищує ранній термін початку роботи на тривалість роботи.

- Пізній термін початку роботи (Тпп) - найбільший з можливих моментів початку роботи, при якому ще можливе виконання всіх наступних робіт з дотриманням планованого терміну завершення всього комплексу робіт. Цей термін менший від пізнього терміну закінчення роботи на тривалість роботи.

- Пізній термін закінчення роботи (Тпз) - найбільший з допустимих моментів завершення роботи, при якому ще можливе виконання всіх наступних робіт з дотриманням планованого терміну завершення всього комплексу робіт. Цей термін збігається з пізнім терміном настання кінцевої події роботи.

- Загальний (повний) резерв часу роботи (R) - максимальний час, на який можна відкласти початок чи збільшити тривалість роботи, не змінюючи планований термін завершення всього комплексу робіт. R дорівнює резерву найбільшого із шляхів, які проходять через цю роботу. Цей повний резерв може бути використаний при виконанні роботи, якщо початкова подія роботи відбувається в ранній термін і може дозволити настання кінцевої події в її пізньому терміні.

- Приватний (вільний) резерв часу роботи (R) - максимальний час, на який можна відкласти початок чи збільшити тривалість роботи за умови, що всі події мережі наступають у свої ранні терміни. Цей приватний резерв може бути використаний, якщо закінчення попередньої роботи відбулося в пізній допустимий термін, а наступні роботи хочуть виконати в ранні терміни.

Якщо планований термін співпадає із отриманою тривалістю критичного шляху, то завершення процесу складання мережевого графіка та розрахунку його параметрів можна вважати завершеним. У випадку, коли отриманий

термін перевищує планований, необхідно вжити заходів для скорочення критичного шляху та внести корективи або провести оптимізацію мережевого графіка.

Аналіз мережевого графіка направлений на виявлення можливостей скорочення загального терміну виконання всього комплексу робіт шляхом зменшення тривалості робіт на критичному шляху. При цьому тривалість критичних робіт, які мають резерв часу, може бути збільшена без впливу на загальний термін виконання робіт.

Слід відзначити, що сама величина резерву часу не є достатньою для повного визначення впливу конкретної роботи некритичного шляху на загальний термін виконання. Важливо враховувати послідовність виконання цих робіт. Ступінь складності виконання у строк кожної роботи некритичного шляху визначається коефіцієнтом напруженості роботи (К"), який визначає співвідношення тривалості різних відрізків шляху, один з яких є максимально тривалим, а інший - критичним:

\[К" = \frac{Є_max}{Є_{кр}}\]

де \(Є_max\) - тривалість максимального шляху, що проходить через дану роботу; \(Є_{кр}\) - тривалість критичного шляху; \(Є'_кр\) - тривалість відрізку розглянутого шляху, який співпадає з критичним шляхом.\

Коефіцієнт напруженості робіт (К ") - це відносна величина, яка може варіюватися навіть при однаковому загальному резерві часу. Різні роботи можуть мати різні коефіцієнти напруженості, навіть якщо їхні загальні резерви часу однакові, і навпаки, різні роботи можуть мати однакові коефіцієнти напруженості при різних загальних резервах часу. Значення коефіцієнта напруженості лежить в інтервалі від 0 до 1, де найвищий коефіцієнт напруженості (К "= 1) відноситься до робіт, які знаходяться на критичному шляху. Чим ближче коефіцієнт напруженості до 1, тим складніше виконати цю роботу в установлені терміни, і тим більше уваги слід приділити цій роботі в процесі організації та проведення робіт.

Розраховані коефіцієнти напруженості дозволяють класифікувати роботи за такими рівнями напруженості:

- Критична напруженість (від 1 до 0,8): роботи 1-2, 2-3, 2-5, 5-6, 3-7, 5-7, 6-8, 7-8, 8-9;

- Підкритична напруженість (від 0,8 до 0,6): робота 1-3;

- Резервна напруженість (менше 0,6): роботи 1-4, 2-4, 4-6, 2-7, 3-9, 7-9.

Оптимізація мережевого графіка представляє собою процес поліпшення організації виконання комплексу робіт з урахуванням терміну його виконання. Оптимізація графіка проводиться з метою скорочення тривалості критичного шляху, вирівнювання коефіцієнтів напруженості робіт та раціонального використання наявного ресурсного потенціалу. Для скорочення тривалості робіт на критичному шляху застосовуються комплекс заходів, включаючи перерозподіл різних ресурсів (тимчасових, матеріальних, трудових, фінансових) з некритичних шляхів на роботи критичного шляху. Додаткові заходи включають зниження трудомісткості робіт критичного шляху, виконання трудомістких робіт паралельно та перегляд структури мережі і складу робіт.

Теоретично, кінцевим результатом оптимізації мережевого графіка є рівність будь-якого повного шляху новому критичному шляху, що визначає рівну напруженість всіх робіт, хоча практично досягти цього завдання не завжди вдається.

3.3 Технічна підтримка та навчання персоналу

Технічна підтримка та навчання персоналу є ключовими елементами ефективного управління інформаційно-комунікаційною інфраструктурою в сучасних організаціях. Ці аспекти важливі для забезпечення безперебійної роботи систем та збереження високого рівня компетентності персоналу. Технічна підтримка включає в себе комплекс заходів, спрямованих на

забезпечення ефективного функціонування інформаційно-комунікаційних систем та надання необхідної допомоги користувачам. Однією з ключових мет цього напрямку є спрощення вирішення проблем та забезпечення якісної технічної підтримки для всіх користувачів.

Перш за все, ефективність технічної підтримки полягає в забезпеченні доступної та оперативної допомоги. Користувачі повинні мати можливість легко звертатися за допомогою та отримувати відповіді на свої запитання чи вирішення проблем. Використання систем відстеження та управління заявками є важливим елементом управління та контролю над цим процесом, що дозволяє ефективно взаємодіяти з користувачами та оперативно реагувати на їхні потреби. Крім того, забезпечення чіткого зв'язку між технічним персоналом та користувачами важливо для успішного розв'язання проблем. Відкритий та зрозумілий обмін інформацією дозволяє не тільки вирішувати конкретні проблеми, а й створювати позитивний досвід взаємодії з іТ-сервісом. Окрім цього, система технічної підтримки повинна враховувати можливість постійного вдосконалення. Аналіз виниклих проблем дозволяє виявляти кореневі причини та розробляти стратегії для їхнього уникнення у майбутньому. Впровадження нових інструментів та практик спрямоване на постійне підвищення якості технічної підтримки та задоволення потреб користувачів. Такий підхід до технічної підтримки дозволяє створювати надійне та ефективне середовище для користувачів, в якому вони можуть отримати необхідну допомогу та вирішити свої питання чи проблеми.

Вдала комунікація є ключовим елементом успішної технічної підтримки, сприяючи якісному вирішенню проблем та створенню позитивного враження у користувачів. Перш за все, важливо забезпечити чіткий зв'язок між технічним персоналом та користувачами під час виникнення проблем. Це може включати в себе швидке та доступне спілкування через різні канали зв'язку, такі як телефон, електронна пошта чи онлайн-чат. Розуміння та врахування особливостей комунікації кожного користувача допомагає забезпечити

ефективний обмін інформацією. Крім того, передача інформації про рішення проблем є важливим етапом взаємодії. Технічний персонал повинен надавати користувачам зрозумілі та повні відповіді на їхні питання, а також наділяти їх знаннями та інструкціями щодо усунення проблем. Це може включати в себе як особистий підхід до роз'яснення складних технічних аспектів, так і надання документації чи посилань на ресурси для самостійного розв'язання проблем. Забезпечення ефективної комунікації також включає в себе ретельне інформування користувачів про процеси обслуговування. Якщо на вирішення проблеми потрібно більше часу, ніж очікувалося, або якщо виникають затримки, важливо чесно та вчасно сповістити користувача про ситуацію та надати відповідні пояснення. Такий підхід до комунікації сприяє побудові довіри між технічним персоналом та користувачами, а також забезпечує позитивний досвід взаємодії з сервісом технічної підтримки.

Постійне вдосконалення в області технічної підтримки є ключовим аспектом, спрямованим на підвищення якості послуг та задоволення потреб користувачів. Аналіз виниклих проблем грає важливу роль у вдосконаленні технічної підтримки. Це включає в себе глибокий розгляд кожної ситуації, визначення кореневих причин проблем та розробку ефективних стратегій для їх вирішення. Важливо розуміти, чому проблема виникла та як можна уникнути подібних ситуацій у майбутньому. Впровадження нових інструментів та практик є необхідним етапом у процесі постійного вдосконалення. Це може включати в себе впровадження нових систем відстеження заявок, удосконалення процесів автоматизації вирішення проблем, а також навчання персоналу новим технікам та стратегіям. Застосування передових технологій та методів допомагає зробити технічну підтримку більш швидкою, ефективною та адаптованою до змін у технологічному середовищі. Постійне вдосконалення також включає в себе навчання персоналу. Співпраця зі спеціалізованими тренерами, організація внутрішніх семінарів та впровадження програм навчання допомагають технічному персоналу підтримувати актуальність своїх

знань та навичок. Всі ці заходи спрямовані на створення найкращих умов для користувачів, забезпечуючи їм високоякісну та ефективну технічну підтримку.

Організація тренінгів є важливим елементом стратегії навчання персоналу в галузі ІТ. Регулярні тренінги дозволяють удосконалювати навички та знання персоналу, щоб вони могли ефективно впроваджувати нові технології та оптимізувати свою роботу. Семінари створюють можливість для обміну досвідом між членами команди та вивчення передових практик в галузі ІТ. Вони сприяють формуванню спільної бази знань та покращують комунікацію в команді. Ознайомлення з новими технологіями та інструментами є невід'ємною частиною тренінгів. ІТ-спеціалісти повинні бути в курсі останніх тенденцій та можливостей, які можуть покращити ефективність роботи. Також важливо розуміти, як нові технології можуть вплинути на бізнес-процеси та як їхнє впровадження може призвести до покращення результативності. Тренінги знову-таки стають невід'ємною частиною стратегії розвитку персоналу, допомагаючи ІТ-спеціалістам залишатися конкурентоспроможними в постійно змінюючомуся світі технологій.

Створення та підтримка навчальних матеріалів є ключовим аспектом стратегії навчання персоналу в галузі ІТ. Це може включати в себе розробку навчальних посібників, презентацій, відеоуроків та інших матеріалів, які сприятимуть ефективному передаванню інформації. Створення онлайн-ресурсів та документації для самонавчання є іншим важливим елементом. Це дозволяє членам команди вивчати новий матеріал у зручний для них час і темп. Онлайн-ресурси можуть включати в себе відеоуроки, інтерактивні тести, статті та інші матеріали, які сприяють розвитку навичок та знань. Важливою частиною цього процесу є постійна актуалізація та оновлення матеріалів, оскільки галузь ІТ швидко розвивається, і нові технології та методи часто виникають. Такий підхід дозволяє персоналу залишатися інформованим про останні тенденції та технічні нововведення.

Залучення персоналу до сертифікаційних програм є важливим етапом в їхньому професійному розвитку. Сертифікація дозволяє персоналу підтвердити свої навички та знання в конкретних областях інформаційних технологій. Це може включати в себе отримання сертифікатів від провідних виробників програмного та апаратного забезпечення, а також сертифікації в галузевих стандартах та методологіях. Проведення регулярних оцінок компетентності також є важливим елементом стратегії навчання. Це дозволяє визначити потреби персоналу у додатковому навчанні, а також оцінити ефективність навчальних програм. Оцінки можуть бути спрямовані на визначення рівня знань та вмінь персоналу в конкретних областях, а також їхню готовність до викликів, які можуть виникнути в процесі роботи. Такий підхід допомагає створити ефективну систему навчання, спрямовану на постійне підвищення кваліфікації персоналу та відповідь на змінні вимоги галузі ІТ.

Підтримка кар'єрного росту є важливим елементом управління персоналом, особливо в галузі інформаційних технологій. Розробка планів кар'єрного росту допомагає співробітникам уявити свій шлях розвитку в організації та досягнення поставлених цілей. Створення індивідуальних планів кар'єрного росту може включати в себе такі етапи, як оцінка поточних навичок та знань, визначення цілей кар'єрного росту, ідентифікація можливостей для професійного розвитку та розробка конкретних кроків для досягнення цих цілей. Забезпечення можливостей для отримання нових ролей та відповідальностей в сфері ІТ є важливою складовою такого підходу. Це може включати в себе участь у проектах з впровадження нових технологій, керівництво малими командами, участь у професійних конференціях та подіях. Такий підхід не тільки сприяє задоволенню персоналу, але і підтримує постійне вдосконалення знань та навичок, що є важливим для ефективного функціонування в галузі інформаційних технологій.

Ефективна технічна підтримка та постійне навчання персоналу є важливими елементами стратегії управління IT, спрямованими на підтримання високого рівня функціональності та безпеки мережевих систем.

ВИСНОВКИ

У контексті реалізації мережевого проекту, висновки виявляються ключовим етапом в успішному розвитку та оптимізації інфраструктури. Визначення бізнес-вимог, оцінка масштабованості, технічні вимоги, топологія мережі, засоби безпеки, масштабування та резервування, план впровадження, система мережевого управління, технічна підтримка та навчання персоналу — це складові, що взаємодіють для створення інфраструктури, що відповідає вимогам сучасного бізнесу.

Професійно впроваджений проект, забезпечений необхідними заходами безпеки та високою масштабованістю, формує основу для стійкої та ефективної мережі. Його успішна реалізація сприяє оптимізації бізнес-процесів, розширенню можливостей та забезпеченню конкурентоспроможності.

Велика увага, надана системі мережевого управління та технічній підтримці, забезпечує необхідний рівень контролю, ефективного виявлення та вирішення проблем, а також навчання персоналу для відповідності сучасним стандартам та викликам галузі IT.

У великому висновку, правильно реалізований мережевий проект — це не тільки технічне вдосконалення, але й стратегічний крок вперед у високотехнологічному бізнес-середовищі, що сприяє необхідному прискоренню розвитку та успішності організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Михайловська О.В. (2008) Операційний менеджмент: навч. посіб. для вузів. Київ: Кондор, 549 с.
2. Капінос Г.І., Бабій І.В. (2013) Операційний менеджмент: навч. посіб. Київ: Центр учбової літератури, 352 с.
3. Jacobs R. and Chase R. (2012) Operations and Supply Chain Management: The Core. McGraw-Hill Education; 3 edition, 552 p.
4. Koren Y. (2006) General RMS Characteristics. Comparison with Dedicated and Flexible Systems. Reconfigurable Manufacturing Systems and Transformable Factories, 27-45.
5. Mahadevan B. (2010) Operations Management: Theory and Practice. Pearson Education India, 650 p.
6. Putnik G. et al. (2013) Scalability in manufacturing systems design and operation: State-of-the-art and future developments roadmap. CIRP Annals - Manufacturing Technology, 62, 751-774.
7. Ray Wild (2002) Operations Management. Cengage Learning EMEA, 870 p.
8. Sarabjeet Singh (2012) Unit 3: Production System. Available at http://www.slideshare.net/SarabjeetSingh9/operations-management-production-system?from_action=save
9. Waters, D. (2003) Logistics: An Introduction to Supply Chain Management. Palgrave Macmillan, 364 p.
10. Кунинець А.І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній / А.І. Кунинець, Ю.І. Грицюк 257 // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.2. – С. 352-360.
11. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. [Електронний ресурс]. –

Доступний з http://nbuv.gov.ua/portal / Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

12. Чудінова Н.В. Особливості використання мережі Інтернет для отримання конфіденційної інформації / Н.В. Чудінова, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.- техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.3. – С. 337-346.
13. Nicholas Rosasco and David Larochelle. How and Why More Secure Technologies Succeed in Legacy Markets: Lessons from the Success of SSH. Quoting Barrett and Silverman, SSH, the Secure Shell: The Definitive Guide, O'Reilly & Associates . Dept. of Computer Science, Univ. of Virginia. Архів оригіналу за 2013-06-25.
14. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7
15. Стрихалюк Б. М. Теорія побудови та протоколи інфокомунікаційних мереж: Конспект лекцій. – Львів: Львівська політехніка, 2017. – 121 с
16. Кулаков Ю. О., Луцький Г. М. Комп'ютерні мережі: Підручник / За ред. Ю. С. Ковтанюка. – К.: Юніор, 2003. – 400 с.
17. Основи інформаційних систем: Навч. Посібник. – Вид. 2-ге, перероб. і доп. / В.Ф. Ситник, Т.А. Писаревська, Н.В. Єрьоміна, О.С. Краєва; За ред. В.Ф. Ситника. – К.: КНЕУ, 2001. – 420 с.
18. Стеклов В.К., Беркман Л.Н. Нові інформаційні технології: транспортні мережі телекомунікацій. – К.: Техніка, 2004.
19. Валецька Т.М. Комп’ютерні мережі: Апаратні засоби. Навч. посібник. – К.: Ельга, 2004.
20. Жураковский Б. Ю. Комп’ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім.

Ігоря Сікорського. – 2020. – 336 с. – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/36615.

21. Жураковський Б. Ю. Комп'ютерні мережі. Частина 2 Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 372 с. – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/36641
22. Zhurakovskiy B. Assessment. Technique and Selection of Interconnecting Line of Information Networks [Електронний ресурс] / B. Zhurakovskiy, N. Tsopa // 3rd International Conference on Advanced Information and Communications Technologies (AICT). – 2019. – Режим доступу до ресурсу: DOI: 10.1109/AIACT.2019.8847726. Proceedings (2019) 71-75
23. Методи аналізу та моделювання безпеки розподілених інформаційних систем: навч. посіб. / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. – Чернігів: Чернігівський національний технологічний університет, 2016. – 254 с.
24. Taqqu M., Willinger W., Sherman R. Proof of a fundamental result in self–similar traffic modeling / M. Taqqu, W. Willinger, R. Sherman // Computer Communication Review. – 1997. – Vol. 27(2). – p. 5 – 23.
25. Leland W., Taqqu M., Willinger W., Wilson D. On the self–similar nature of Ethernet traffic / W. Leland, M. Taqqu, W. Willinger, D. Wilson // IEEE/ACM Transactions on Networking. – 1994. – Vol. 2(1). – p. 1 – 15.
26. Paxon V., Floyd S. Wide-area traffic: The failure of Poisson modeling. / V. Paxon, S. Floyd // IEEE/ACM Transactions on Networking. – 1995. – Vol. 3. – p. 226 – 244.
27. Feldmann A., Gilbert A.C., Willinger W. Data Networks as Cascades: Investigating the multifractal nature of Internet WAN traffic. / A. Feldmann, A.C. Gilbert, W. Willinger // ACM SIGCOM. – 1998. – p. 42 – 55.
28. Добровольский Е.В., Нечипорук О.Л. Имитационное моделирование источников нагрузки в сетях передачи данных с коммутацией пакетов /

Е.В. Добровольский, О.Л. Нечипорук // Наукові праці ОНАЗ ім. О.С. Попова. – 2000. – № 3. – С. 19 – 23.

29. Добровольский Е.В., Нечипорук О.Л. Моделирование сетевого трафика с использованием контекстных методов / Е.В. Добровольский, О.Л. Нечипорук // Наукові праці ОНАЗ ім. О.С. Попова. – 2005. – № 1. – С. 24 –
30. Зоріна Т.І. Системи виявлення і запобігання атак в комп'ютерних мережах / Т.І. Зоріна // Вісник східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15 (204) ч.1. – С. 48 – 54.
31. Субач І.Ю., Фесьоха В.В. Модель виявлення аномалій в інформаційно – телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу / І.Ю. Субач, В.В. Фесьоха // Збірник наукових праць ВІТІ. – 2017. – № 3. – С. 21 – 24.
32. TCPDUMP/LIBPCAP public repository [Інтернет-ресурс] / Web-сайт: tcpdump; Режим доступу http://www.tcpdump.org, вільний.
33. Snort [Інтернет-ресурс] / Web-сайт: snort; Режим доступу http://www.snort.org, вільний.
34. Wireshark [Інтернет-ресурс] / Web-сайт: wireshark; Режим доступу http://www.wireshark.org, вільний.
35. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 12 с.
36. Вишневський, В. М. Теоретичні основи проектування комп'ютерних мереж / В. М. Вишневський М .: Техносфера, 2014 г. 512 с.
37. Кузин, А.В. Комп'ютерні мережі / А. В. Кузін М .: 2015 г. 256 с.

38. Корріган, П. Основи проектування мережі / П. Корріган // Lan. 1997. № 2. С. 3-7.
39. Казаков, С.І. Основи мережевих технологій / С.І. Казаков, С. Г. Харін. М .:Видавництво Мікроінформ, 2005. 162 с.
40. Фомінов О.С. Мережеві стандарти і застосування // Мережі. 1995. №9. – 202 с.
41. Коломоєць Г.П. Організація комп'ютерних мереж: навчальний посібник. Запоріжжя: КПУ, 2012. 156 с.
42. Шиндер, Л.Д. Основи комп'ютерних мереж / Л.Д. Шиндер М .: 2015 г. 152 с.
43. Семенов, А. Б. волоконна оптика в локальних і корпоративних мережах / А.Б. Семенов М .: Айті-Пресс, 2016 г. 327 с.
44. П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко ТЕЛЕКОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ МЕРЕЖІ Розділ 3.5. Компоненти і моделі фізичної структури мереж.
45. Телекомунікаційні системи та мережі. Том 1. Структура й основні функції. Автори: Поповський В.В, Лемешко О.В.; Ковальчук В.К.; Плотніков М.Д.; Картушин Ю.П.; Попонін О.М.; Агєєв Д.В.; Сабурова С.О., Олійник В.Ф., Персиков А.В.; Лошаков В.А. Селіванов К.О. Розділ 4. Лінії зв’язку. Друге видання. Виправлено та доповнено. 2018.
46. П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко ТЕЛЕКОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ МЕРЕЖІ Розділ 3.5. Компоненти і моделі фізичної структури мереж.
47. Остапов С. Е. Євсеєв С. П. Король О. Г. ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ Навчальний посібник Харків. Вид. ХНЕУ, 2013. – 120 с.
48. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, Г. М. Гулак, В. Б. Толубко. – К.: ДУТ, 2015. – 449 с.
49. Mueller S. Upgrading and Repairing Networks / S. Mueller. – Que, 2002.

50. Lekkas P. C. Network Processors / P. C. Lekkas. – The McGraw-Hill Companies, 2003.
51. Богуш В. М. Основи інформаційної безпеки держави / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005 – 432 с.
52. Богуш В. М. Інформаційна безпека від А до Я: 3000 термінів і понять / В. М. Богуш, А. М. Кудін. – К.: МОУ, 1999. – 456 с.