УДК 004

С.Мороз, магістр гр. КІ-23Мз
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ГІПЕРЦОД

У статті розроблено програмне забезпечення, яке призначено для системи управління гіперЦОД. Метою розробки є дослідження та програмна реалізація системи управління гіперЦОД. Об'єктом дослідження є процес управління гіперЦОД. Предметом дослідження є методи управління гіперЦОД. Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи управління гіперЦОД. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Загальна ефективність – це саме те, що потрібно в ЦОД. ГіперЦОД концентруються саме на підвищенні ефективності. Економія засобів у перерахуванні на одиницю встаткування дозволяє встановити більше встаткування й забезпечити більше якісні сервіси.

Зміни, що відбуваються в галузі, численні й різноманітні. Можливо, провиною всьому криза, а може бути, наполегливе бажання змінити екосистему – у кожному разі зміни неможливо не помітити.

Зміни торкаються людей, що перетворюють інновації в життя, компанії – як лідерів, так і аутсайдерів – і потреби тих і інших. Потоки даних перемінили обчислювальні операції як типове навантаження для ІТ-устаткування, ПЗ стало відкритим, код абстрагується від процесорної архітектури. Приватні й корпоративні користувачі повстають проти застарілих методів, консервативних вендорів, що втратили свою ефективність бізнес-моделей. Зовсім змінилися ті принципи, відповідно до яких реалізується фундаментальна системна архітектура й взаємодіють між собою процесори.

Отже, якщо ви – системний архітектор, вас не може не захоплювати, які можливості відкриваються для інновацій, для створення нових або трансформації наявних видів бізнесу! Але інновації – це найчастіше реалізація абсолютно нових підходів до тому, як робляться справи. Ще не всі зміни перетворені в життя. Ми тільки на початку шляху.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи управління гіперЦОД.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи управління гіперЦОД.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем управління гіперЦОД.
– Дослідження системи управління гіперЦОД.
– Програмна реалізація системи управління гіперЦОД.

Об'єктом дослідження є процес управління гіперЦОД.

Предметом дослідження є методи управління гіперЦОД.

Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Рекомендації з керування ІТ інфраструктурою

Оцінка необхідності змін в ІТ-інфраструктурі

При організації діяльності ІТ-служби Замовника рекомендується використовувати сервісний підхід, основи якого викладені в «Стандарті надання послуг в області інформаційних технологій". Відповідно до сервісного підходу діяльність ІТ-служби – це надання якісних і надійних послуг, що задовольняють вимогам інших підрозділів компанії. За допомогою сервісного підходу здійснюється:

– організація ІТ відповідно до вимог бізнес-процесів;
– використання описів ІТ-послуг (сервісів) мовою, зрозумілому їхнім користувачам;
– керування ІТ у термінах надаваних послуг (сервісів);
– керування витратами на використання надаваних послуг (сервісів);
– вимірність результатів інвестицій в ІТ і оптимізація сукупної вартості володіння (ТСО) послугами (сервісами).

При рішенні завдань керування ІТ-інфраструктурою важливе значення мають процеси, пов'язані зі змінами ІТ-інфраструктури. Технічні рішення, пов'язані зі змінами ІТ-інфраструктури, повинні бути обґрунтовані, у тому числі, з урахуванням оцінки їхнього впливу на вартість і якість послуг, надаваних ІТ-службою, і реалізовані з урахуванням наступних рекомендацій по внесенню змін і плануванню ІТ-інфраструктури.

Рекомендації із проведення змін в ІТ інфраструктурі

Процес по проведенню змін в ІТ-інфраструктурі – це процес використання стандартизованих методів і процедур для ефективного й своєчасного проведення змін в ІТ-інфраструктурі з мінімальними негативними наслідками для бізнес-процесів.

При зміні ІТ-інфраструктури необхідно враховувати наступні вимоги:

– Загальні вимоги до тестування й приймання змін.
– Вимог «розумного консерватизму» при впровадженні нових версій ІТ-компонентів.
– Вимог автоматизації тиражування відновлень ПЗ.
– Обов'язкове документування внесених змін.

Загальні вимоги до тестування й приймання змін

Процес тестування й приймання змін ІТ-інфраструктури повинен задовольняти наступним загальним вимогам:

– Рішення про проведення змін повинні прийматися Службою замовника за узгодженням з функціональними замовниками. Служба замовника вправі розробити спрощений порядок прийняття рішень про проведення некритичних для бізнес-процесів змін.
– Перед введенням змін в експлуатацію необхідно розробити й протестувати план внесення змін з обов'язковою вказівкою контрольних точок ухвалення рішення про відмову від внесених змін і поверненні системи в попередній стан. Тестування плану внесення змін необхідно робити в середовищі, аналогічної виробничої.
– Тестування й приймання змін необхідно робити в середовищі, аналогічної виробничої.
– Введення змін в експлуатацію випереджається резервним копіюванням всіх елементів системи, які підверглись зміні.

Вимоги «розумного консерватизму»

При впровадженні, модернізації, відновленні ІТ-компонентів повинні бути дотримані наступні загальні вимоги «розумного консерватизму»:

– впровадження нових версій ПЗ повинне мати обґрунтовані переваги перед використовуваними версіями ПЗ й не повинне погіршувати поточного стану справ;
– для критично важливих бізнес-процесів неприпустиме впровадження останніх версій промислового ПЗ й/або його компонентів, за винятком використовуваних у схожому

промисловому середовищі більше 2 років і, що мають при цьому не менш 2 коригувальних відновлень від виробника (релізів, патчів, сервіс-паків, відновлень ПЗ й т.п.);

– неприпустиме використання тестових версій ІТ-компонентів (альфа, бета версії ПЗ й т.п.) у режимі промислової експлуатації;

– при плануванні впровадження нових версій ПЗ рекомендується враховувати довгострокові плани виробника по випуску нових версій/релізів;

– перед впровадженням нових версій ПЗ в промислову експлуатацію обов'язково ретельне тестування функціонування відповідної системи, з висновками відповідних ключових фахівців.

Автоматизація тиражування відновлень ПЗ

Автоматизація тиражування відновлень ПЗ повинна виконуватися з обліком наступних загальних вимог і рекомендацій:

– при виборі ПЗ, при інших рівних функціональних характеристиках, перевага варто віддавати системам, що мають служби централізованого керування й відновлення;

– створення й впровадження рішення по автоматизації тиражування відновлень ПЗ повинне вироблятися в рамках окремих проектів ІТ-служби й з використанням власної серверної системи тиражування відновлень; Відновлення ПЗ безпосередньо з Інтернет-порталу виробника не допускається;

– функціональні можливості автоматизованої системи тиражування відновлень повинні дозволяти реалізацію повного й спрощеного циклів керування змінами, проводити автоматичну перевірку (аудит) тиражування відновлень;

– тиражування відновлень в області безпеки критичних для підприємства систем (відновлення операційних систем, ПЗ з безпосереднім доступом у зовнішні мережі / Інтернет, антивірусні системи й т.п.) підлягає обов'язковій автоматизації;

– тиражування відновлень в області безпеки й функціональних відновлень на робочі станції й інфраструктурні ІТ-компоненти (домен – контролери, DNS / DHCP – сервера й т.п.) у частині системного й офісного ПЗ підлягає обов'язковій автоматизації;

– відновлення інфраструктурного ПЗ (домен-контролери, DNS/DHCP/ mail-сервера), що включає зміну функціональності (крім відновлень в області безпеки), підвищення major-версії необхідно проводити під контролем відповідного фахівця, попередньо провівши тестування в тестовому середовищі, аналогічної виробничої;

– рекомендується автоматизація тиражування відновлень клієнтської частини бізнес-додатків;

– перед масштабним тиражуванням відновлень необхідно провести тестування в локальному тестовому середовищі.

Рекомендації із планування ІТ-інфраструктури

При плануванні ІТ-інфраструктури повинен бути забезпечений економічно обґрунтований рівень відповідності ресурсів ІТ-інфраструктури поточній і майбутній потребам споживачів. Для ефективного планування ІТ-інфраструктури необхідно враховувати прогноз розвитку основної діяльності споживача й технічного розвитку ІТ. Тому, для кожного споживача, важливе значення має вибір обріїв планування для різних ІТ-додатків і визначення базової методики розрахунку продуктивності й обсягу збереженої інформації для ІТ-систем.

Рекомендації з вибору обріїв планування для ІТ-додатків

Вибір обріїв планування ІТ-додатків повинен визначатися обрієм планування споживача. При цьому обрій планування ІТ-інфраструктури повинен бути менше, ніж обрій планування ІТ-додатків.

Рекомендується виходити з наступних обріїв планування ІТ-додатків:

– 8-9 років для додатків класу ERP і додатків керування ІТ, критичних для бізнесу;

– 5-6 років для бізнес-додатків і систем операційного керування ІТ;

– 3-5 років для офісних і системних додатків.

При цьому для відповідних елементів ІТ інфраструктури рекомендується встановити наступні обрії планування:

– 5-6 років для додатків класу ERP і додатків керування ІТ, критичних для бізнесу;
– 3-4 роки для бізнес-додатків і систем операційного керування ІТ;
– 2-3 роки для офісних і системних додатків.

Рекомендації з розрахунку продуктивності й обсягу збереженої інформації для ІТ-систем (масштабування ІТ-систем)

Розрахунок продуктивності ІТ-систем повинен вироблятися в термінах ІТ-послуг, виходячи із планованих строків використання (обрію планування), обсягів, значень показників рівня надання й продуктивності послуг.

При розрахунку продуктивності підлягають обліку навантажувальні можливості всіх задіяних у наданні ІТ-послуг компонентів: ІТ-послуг, ІТ-систем, компонентів інфраструктури й систем інформаційної безпеки, включаючи клієнтські робітники станції.

При розрахунку продуктивності ІТ-систем обов'язковий облік як середніх, так і пікових показників навантаження. Рекомендується для розрахунку продуктивності використовувати надаваний виробником інструментарій – навантажувальні криві й розроблені кращі методики (bestpractices).

У загальному випадку, у ході розрахунку рекомендується проводити оцінку завантаження по наступних компонентах:

– сервер додатків;
– сервер баз даних;
– серверні засоби інформаційної безпеки (антивірусне забезпечення, програмний міжмережний екран, криптографічні системи й т.п.);
– компоненти моніторингу (агенти й т.п.);
– системне ПЗ;
– апаратна платформа (процесори, оперативна пам'ять, дискова підсистема, мережний інтерфейс);
– мережі зберігання даних (SAN, NAS);
– мережі передачі даних, включаючи активні пристрої (міжмережні екрани, маршрутизатори й т.п.);
– мережні сервіси (сервіси каталогу, DNS, DHCP і т.п.);
– клієнтські робочі станції в апаратній і програмній частині.

Для оцінки обсягу збереженої інформації рекомендується використовувати власні статистичні дані по обсягах і динаміці зміни даних за тривалі (від 1 місяця) періоди й максимальні значення в пікові періоди. При відсутності власних даних припустиме використання статистики схожих підприємств або експертних оцінок. При впровадженні нових сервісів варто дотримуватися інформації, що вказується виробником, як в області початкових вимог, так і в прогнозованих обсягах збільшення інформації. Останній показник варто коректувати в ході наступної експлуатації систем.

При оцінці обсягу збереженої інформації обов'язковий облік не тільки корисного обсягу, але й обсягів системної й службової інформації (системи шифрування, файли логування, файли журналів транзакцій і т.п.).

Каталогізація й класифікація елементів ІТ-інфраструктури

Типізація елементів ІТ-інфраструктури

Уніфікація й типізація елементів ІТ-інфраструктури здатна значно знизити витрати й полегшити впровадження нових ІТ-рішень, знизити витрати на підготовку ІТ-персоналу, спростити супровід і обслуговування цих рішень у майбутньому й, в остаточному підсумку, значно знизити загальну вартість володіння ІТ-інфраструктурою в цілому.

Під типізацією розуміється зниження номенклатури й підвищення якості ІТ-елементів і конфігурацій, впроваджуваних в органах державної влади.

Дана технічна політика висуває вимоги до наступних категорій ІТ інфраструктури:

– робочим місцям користувачів (ПК, периферійне встаткування);
– мультисервісної мережі (корпоративна мережа, зовнішні канали зв'язку);
– прикладного ПЗ;
– інфраструктурі центрів обробки даних (системи зберігання й резервування, сервери).

Класифікація за рівнем використання

При побудові сучасної ІТ-інфраструктури для визначення місця установки (розміщення) ІТ-рішення необхідно провести класифікацію даного рішення залежно від сукупності наступних параметрів: состава користувачів даної системи, ступеня агрегації інформації, зберігання й обробки даних. розв'язуваних задач. рівня складності й т.д.

З погляду даної класифікації рекомендується виділити наступні класи або рівні інфраструктури для розміщення ІТ-систем:

– Центр обробки даних – ЦОД І рівня, (рівень Уряду) – забезпечує централізоване зберігання й обробку даних на рівні Уряду. Ресурси даного ЦОД використовуються для консолідації інформації з нижчележачих рівнів, забезпечення інформаційної взаємодії органів державної влади й надання ІТ-сервісів всім організаціям, фінансованим з республіканського бюджету.
– Центр обробки даних – ЦОД ІІ рівня, основний центр зберігання й обробки даних у рамках одного органа державної влади.

Класифікація за рівнем необхідної безперервності обслуговування й важливості для бізнесу

Багато критичних управлінських і технологічних процесів опираються на комп'ютерні системи обробки й зберігання даних і не можуть функціонувати без їхнього використання. Тому, забезпечення безперервності обслуговування й доступності ІТ-рішень є найважливішим показником безперервності державного керування в цілому, і важливим фактором, що класифікує, для елементів ІТ-інфраструктури. Виходячи із пропонованих вимог до надійності окремих елементів і конфігурацій ІТ-систем у цілому і їхньому відновленні після збоїв і відмови встаткування, ПЗ або інфраструктурних елементів, сучасні ІТ-технології надають різні архітектурні й конфігураційні рішення, що забезпечують дані вимоги. З погляду забезпечення безперервності обслуговування управлінських і технологічних користувачів і процесів, а також вимог до відказостійкості, можна запропонувати наступну класифікацію ІТ-рішень:

– **Mission Critical-системи**, що працюють у режимі «бойового чергування». До таких систем ставляться: гостро критичні з погляду державного керування або зовнішніх факторів – наприклад екології, додатки, а також технологічні додатки, що працюють у режимі реального часу. Вихід з ладу цих систем спричиняє непоправні втрати для керування, у т.ч. загрозу життю й здоров'ю персоналу й населення. Рекомендований час відновлення подібних систем після відмови менш 10 хвилин. Для таких систем повинні використовуватися спеціалізовані серверні платформи й інфраструктурні рівні з повним багаторазовим резервуванням всіх компонентів, у тому числі з використанням резервних віддалених ЦОД.
– **Business Critical-системи**, критичні для керування, з режимом роботи 24x7x365. Вихід з ладу цих систем спричиняє значні бізнес втрати для органів державної влади. Рекомендований час відновлення подібних систем після відмови менш 2 годин. Для таких систем повинні використовуватися кластерні рішення й інфраструктурні рівні із частковим резервуванням використовуваних інфраструктурних компонентів.
– **Business Operational** – звичайні бізнес-додатки – системи, не потребуючі роботи в реальному часі, з режимом роботи 8x5. Рекомендований час відновлення подібних систем після відмови 4-6 години. Для таких систем рекомендується використовувати резервування зберігання даних і електроживлення.

– **Office Production** – не критичні для управління додатка, персональні дані. Рекомендований час відновлення подібних систем після відмови 1-2 робочих дня.

Необхідно враховувати, що загальна безперервність і відказостійкість IT-конфігурацій визначається відповідною безперервністю й відказостійкістю її окремих елементів: апаратних, програмних засобів і інфраструктури, необхідної для її успішного функціонування – каналів зв'язку, системи електроживлення й т.д. і, в остаточному підсумку, залежить від рівня безперервності й відказостійкості його найслабшого компонента (принцип «слабкої ланки»). Класифікація систем з погляду забезпечення безперервності й відказостійкості повинна бути одним з вирішальних факторів при виборі рівня інфраструктури (ЦОД) для розміщення IT-систем.

Принципи створення КРК

Необхідно розробити й впровадити каталог рекомендованих конфігурацій (КРК) для побудови IT-рішень. Даний каталог повинен містити перелік типових елементів IT-інфраструктури, рекомендованих до використання в органах державної влади, державних установ.

Основна мета створення КРК – провести уніфікацію використовуваного встаткування й програмного забезпечення й забезпечити цілісність і керованість IT-інфраструктури органів державної влади, державних установ.

При побудові й розвитку своєї IT-інфраструктури всі органи державної влади, державні установи повинні закуповувати й впроваджувати тільки внесені в каталог IT-конфігурації. Закупівля конфігурацій, які не входять у даний список, можлива в тільки виді виключення.

Уніфікація IT-рішень, використовуваних у рамках конкретного органа державної влади дозволить домогтися зниження загального ТСО, що має на увазі зниження витрат на закупівлі, впровадження й експлуатацію елементів IT-інфраструктури.

Каталог створюється в кожному органі державної влади й повинен містити наступний мінімальний набір даних про рекомендовану конфігурацію:

– назва конфігурації;

– клас об'єкта (функціональний розділ каталогу) відповідно до «Класифікатора об'єктів»;

– клас конфігурації за рівнем використання;

– клас конфігурації за рівнем безперервності;

– набір апаратних засобів, що рекомендується, для даної конфігурації;

– набір програмних засобів, що рекомендується, для даної конфігурації.

– Кількість уніфікованого встаткування й ПЗ в кожному функціональному розділі каталогу повинне бути мінімально.

– Рекомендується використовувати стандартне встаткування й ПЗ сЪебеебе, що зарекомендував, на ринку виробника в даній області, що постійно розвиває й удосконалює свій модельний ряд.

– Каталог повинен регулярно (не рідше чим раз у рік) переглядатися й обновлятися.

– Рекомендується використовувати складне апаратно-програмне забезпечення різного призначення того самого виробника. Таке рішення спрощує керування IT-інфраструктурою, дозволяє знизити експлуатаційні витрати, а також вартість знову апаратно-програмного забезпечення, що здобувається.

– Для масових, стандартних IT-конфігурацій і їхніх елементів рекомендується включати в каталог рішення не менш чим двох альтернативних виробників.

Вимоги до постачальників, виробникам і проведенню конкурсів

У справжньому розділі викладені основні вимоги, що стосуються вибору постачальників програмно-апаратних комплексів і послуг, виробників програмно-апаратних комплексів, а так само системних інтеграторів, що здійснюють розгортання IT-інфраструктури.

Органи державної влади вправі при виборі постачальників і виробників орієнтуватися на більше високі вимоги, чим це передбачено в справжньому документі.

Загальні вимоги

До постачальників і виробників пред'являються наступні загальні вимоги:

– Діяльність постачальників і виробників повинна бути ліцензована, якщо таке передбачає Українське законодавство.

– При підведенні підсумків конкурсу, за інших рівних умов, перевагу мають ті компанії, виробництво яких відповідає вимогам стандарту системи менеджменту якості ISO 9001:2000. Причому в додатку до сертифіката повинна бути зазначена саме та діяльність, на надання якої претендує дана компанія.

– За останні три роки учасник конкурсу повинен успішно завершити два аналогічних контракти на поставку послуг, якщо він претендує на постачальника послуг, або розробку, інсталяцію, забезпечення технічної підтримки для IT-систем, якщо він претендує на поставку програмно-апаратного забезпечення, аналогічних конкурсній пропозиції по параметрах і порівнянних по масштабі.

– Мінімально прийнятний середньорічний оберт постачальника за останні три роки не повинен бути менше, ніж сума договору на поставку послуг або встаткування, помножена на 5.

– Ключові керівники постачальника повинні мати досвід успішної реалізації, як мінімум, двох контрактів порівнянного масштабу, з яких мінімум один контракт реалізований в України.

Вимоги до постачальників і виробників устаткування

До постачальників і виробників програмно-апаратного забезпечення пред'являються наступні вимоги:

– Виробник апаратного забезпечення повинен мати сертифікат, виданий визнаним органом по сертифікації, на відповідність своєї системи менеджменту якості вимогам ISO 9001:2000.

– Перевага повинне віддаватися тим постачальникам апаратного забезпечення які мають сертифікат, виданий визнаним органом по сертифікації, на відповідність своєї системи менеджменту якості вимогам ISO 9001:2000.

– Апаратна платформа й програмне забезпечення повинні бути стандартизовані й сертифіковані на відповідність стандартам, що вважаються загальноприйнятими в предметній області даного програмно-апаратного забезпечення, мати гнучку й масштабовану архітектуру.

– Пропоноване постачальником устаткування повинне бути комерційно доступно протягом не менш трьох місяців, а програмне забезпечення не менш шести місяців.

– Постачальники складного програмно-апаратного забезпечення повинні вчасно одержувати сертифікати відповідності на всю гаму встаткування, що поставляється, і ПЗ відповідно до діючих технічних вимог у повному обсязі, а також обновляти сертифікати з появою нових версій програмного й апаратного забезпечення поставляється продукції, що.

– У випадку поставки встаткування, постачальник повинен мати власний склад.

– Постачальник повинен бути авторизований виробником на той перелік послуг, які постачальник буде робити замовникові. При цьому перевага повинне віддаватися постачальникам, що мають більше високий статус (рівень) відносин з виробником.

– Постачальник повинен здійснювати страхування вантажу при доставці.

– Постачальник повинен мати сертифікований технічний персонал на ту предметну область, у якій постачальник буде робити замовникові послуги.

– Перевага повинне віддаватися виробникам, що поставляють устаткування й ПЗ, адаптоване для використання в України, якщо така адаптація можлива.

– Перевага повинне віддаватися постачальникам, що надають документацію на встаткування й ПЗ українською мовою й на електронних носіях (в електронному виді).

– Постачальники повинні здійснювати гарантійну підтримку поставленого встаткування й ПЗ згідно з вимогами до послуг з експлуатації й супроводу, наведеним нижче.

– Гарантійний строк на програмно-апаратне забезпечення починається з моменту приймання ПЗ або встаткування в експлуатацію й повинен тривати не менш 12 місяців для апаратного забезпечення й 6 місяців для ПЗ.

– Постачальники програмно-апаратного забезпечення повинні організувати на території України центри навчання з метою первинного навчання фахівців, що експлуатують програмно-апаратне забезпечення, їхньої перепідготовки при впровадженні нових версій і типів устаткування й ПЗ, або мати договір зі стороннім центром навчання на надання послуг з навчання, гарантуючи при цьому, що навчання на навчальних курсах даного центра буде досить для експлуатації програмно-апаратного забезпечення.

Вимоги до постачальників послуг

Загальні вимоги до постачальників послуг

До постачальників послуг пред'являються наступні вимоги:

– Перевага повинне обдаватися компаніям, що надають послуги відповідно до міжнародних стандартів, прийнятими для даного типу послуг. Дана відповідність рекомендується документально підтверджувати або наявністю відповідного сертифіката, або вибірковою перевіркою нормативних і робочих документів.

– Постачальник послуг повинен мати сертифікованих фахівців, як по функціоналі надаваних послуг, так і з погляду процесної організації надання послуг. Зокрема, рекомендується враховувати відповідність бізнес-процесів постачальника рекомендаціям ITIL і COBIT по наданню послуг.

– При наданні послуг системної інтеграції рекомендується, щоб постачальник мав впроваджену в себе на виробництві систему керування проектами на основі кращих світових практик, таких як рекомендації PMI і IPMA. Також перевага повинне віддаватися компаніям, що мають сертифікованих керівників проектів, наприклад, по системі PMI.

Вимоги до постачальників послугам з експлуатації й супроводу

Постачальники послуг по технічній підтримці (супроводу) і учасники конкурсів, проведених Компаніями для поставки програмно-апаратного забезпечення, повинні задовольнити наступні мінімальні вимоги до організації підтримай і експлуатації:

– Сервіс-центр повинен перебувати в прийнятній далекості від замовника, щоб мати можливість усунути несправність із виїздом до замовника в строки, установлені відповідними регламентами взаємодії, які, у свою чергу, повинні опиратися на вимоги безперервності, готовності й доступності IT-елементів IT-інфраструктури.

– Експлуатація складного програмно-апаратного забезпечення, гарантійний строк на яке минув, повинна здійснюватися на основі контракту на післягарантійне обслуговування. Зазначений контракт повинен полягати сервісом-центром, розташованим на території України й забезпечуючий післягарантійне обслуговування програмно-апаратного забезпечення даного типу. У випадках, коли програмно-апаратне забезпечення застосовується в обмежених обсягах і сервіс-центр на території України відсутній, контракт на післягарантійне обслуговування полягає безпосередньо з фірмою – постачальником або її представництвом.

– Експлуатація складного програмно-апаратного забезпечення, що перебуває поза гарантійним строком, без укладеного контракту на післягарантійне обслуговування або без наявності в Замовника сервіс-центра, не допускається.

– В окремих випадках допускається здійснювати післягарантійне обслуговування силами сервіс-центра, при наявності фахівців, що пройшли відповідне навчання (що підтверджується сертифікатами постачальника), необхідного оснащення, запасних частин і оформлених належним чином взаємин із системою сервісної підтримки фірми-постачальника або виробника.

– Постачальник послуг з експлуатації й супроводу встаткування повинен мати власний склад запасних частин, що повинен перебувати в прийнятній далекості від місця установки встаткування.

– Постачальник послуг з експлуатації й супроводу повинен бути авторизований виробником на ці види діяльності. При цьому перевага повинне віддаватися постачальникам, що мають більше високий статус (рівень) відносин з виробником.

– Постачальник послуг з експлуатації й супроводу повинен мати сертифікований технічний персонал.

– Постачальники складного програмно-апаратного забезпечення повинні силами сервіс-центрів, розташованих на території України, здійснювати модернізацію програмно-апаратного забезпечення, що перебуває в експлуатації, з метою підтримки його на сучасному технічному рівні й впровадження нових сучасних функцій і послуг.

– Обслуговування й модернізація повинні здійснюватися для всіх установлених типів устаткування й ПЗ даного постачальника й для всіх версій зазначеного встаткування, у тому числі тих, поставки яких закінчилися до набрання чинності справжнім документом.

Сервіс-центри постачальника послуг з експлуатації й супроводу повинні забезпечувати:

– Підтримку користувачів, відповідно до вимог безперервності, по телефоні й за допомогою електронної пошти.

– Рішення проблем, що виникають при роботі програмно-апаратного забезпечення в обсязі, покладеному на даний сервіс-центр.

– Можливість внесення оперативних корекцій у програмне забезпечення, що перебуває в експлуатації з використанням сучасних засобів передачі інформації (мереж передачі даних і ін.).

– Можливість виїзду фахівців для усунення несправностей відповідно до встановленого регламенту. Рекомендується використовувати наступні вимоги для екстреного виїзду фахівців: виїзд фахівця протягом не більше 12 годин і із прибуттям на місце протягом не більше 24 годин з моменту обігу (без обліку транспортних затримок, що не залежать від сервіс-центра).

– Не допускається несанкціоноване керівником ІТ втручання (у тому числі дистанційне) сервіс-центрів у роботу програмно-апаратного забезпечення, що перебуває в експлуатації.

– Строк ремонту або заміни сервісом-центром несправних вузлів устаткування не повинен перевищувати двох тижнів з моменту передачі вузла на сервіс-центр. Для цього сервіс-центр повинен мати необхідний комплект запасних вузлів, а також, при необхідності – ремонтні встаткування й служби.

Вимоги до постачальників послуг з навчання

Постачальники послуг повинні задовольняти наступним мінімальним вимогам до навчання співробітників замовника:

– Рівень навчання повинен бути достатнім для самостійної експлуатації програмно-апаратного забезпечення в типових ситуаціях, що виникають у процесі експлуатації. Кваліфікація тих, яких навчають, повинна підтверджуватися відповідними сертифікатами, що дають право на експлуатацію програмно-апаратного забезпечення даного типу.

– Пропускна здатність центрів навчання повинна бути достатньої для того, щоб забезпечувати підготовку й перепідготовку персоналу для всього діючого й знову програмно-апаратного забезпечення, що вводиться, даного типу.

Вимоги до проведення конкурсів

Учасники конкурсів, проведених Службою Замовника для поставки програмно-апаратного забезпечення й/або послуг, повинні відповідати всім додатковим вимогам, зазначеним для постачальників і виробників у даному документі, а також відповідати всім

основним вимогам, які пред'являє Система стандартів по організації закупівельної діяльності.

Розробка структурної схеми

Технічні вимоги до елементів ІТ-інфраструктури

Дані технічні вимоги розглядаються в розрізі кращих світових практик по створенню ІТ-інфраструктури для сучасних корпорацій. Окремі вимоги пред'являються до наступних категорій інфраструктурних елементів:

- Робочі місця користувачів:
- Персональні комп'ютери.
- Системне ПЗ робочих місць користувачів.
- Периферійні пристрої.
- Прикладне ПЗ.

Мультисервісна мережа:

- Корпоративна розподілена мультисервісна мережа.
- Зовнішні канали зв'язку.

Інфраструктура центрів обробки даних:

- Системи обробки й зберігання даних.
- Приміщення й інженерні системи.
- Інформаційна безпека.
- Безперервність надання ІТ-послуг.
- Системи керування й моніторингу.

Вимоги до робочих місць користувачів

Вимоги до персональних комп'ютерів

Даний розділ розглядає загальні технічні вимоги до парку персональних комп'ютерів, експлуатованих в органах державної влади, державних установах.

Загальні вимоги

При розвитку парку персональних комп'ютерів і виборі закуповуваних моделей ПК ІТ-служби органів державної влади, державних установ України повинні керуватися наступними положеннями:

- Апаратна платформа й програмне забезпечення персональних комп'ютерів повинні бути стандартизовані й сертифіковані, мати гнучку й масштабовану архітектуру.
- Апаратні характеристики ПК повинні відповідати, або перевершувати мінімальні системні вимоги використовуваного ПЗ.
- Для забезпечення загального рівня послуг, керування даними всіх ПК повинне бути уніфіковане, тобто для ПК повинне бути організоване централізоване поширення програмного забезпечення за допомогою єдиного інструмента поширення відновлень програмного забезпечення.
- ПК повинен мати апаратну або програмну систему віддаленого керування.
- Для підвищення якості й швидкості адміністрування кількість різних програмно-апаратних конфігурацій персональних комп'ютерів повинне бути обмежене. Рекомендується використання не більше 4 типових конфігурацій.

Для специфікації технічних вимог виділяються наступні ключові параметри ПК:

- Продуктивність. Продуктивність персональних комп'ютерів повинна забезпечуватися за рахунок:
- Параметрів швидкодії процесора.
- Необхідного й достатнього обсягу оперативної пам'яті.
- Швидкості внутрішніх шин передачі даних.
- Якості й швидкодії графічної підсистеми.
- Пристроїв введення/виводу.

– Надійність. Надійність повинна забезпечуватися за рахунок апаратних засобів і програмного забезпечення й визначатися виходячи із середнього часу безвідмовної роботи (MTBF).

– Масштабованість. Масштабованість повинна забезпечуватися архітектурою й конструкцією персонального комп'ютера за рахунок можливості нарощування:

– Числа й потужності процесорів.

– Обсягів оперативної й зовнішньої пам'яті.

Вимоги до типізації конфігурацій

Весь парк ПК в органах державної влади, державних установах пропонується розділити на наступні типові конфігурації:

– Персональний комп'ютер для роботи з бізнес-орієнтованим прикладним ПЗ (офісні системи, фінансові системи, СЕД і т.п.).

– Персональний комп'ютер підвищеної потужності для роботи із графічними пакетами, пакетами ПЗ моделювання, САПР, АСУЕИ, АСУТП та ін. Використовується для додатків з розвитий графікою, високими вимогами до продуктивності процесора й обсягам оперативної пам'яті.

– Тонкий клієнт. Малопотужний персональний комп'ютер для роботи з додатками в термінальному середовищі, або із програмами-тонкими клієнтами в клієнт-серверній архітектурі. При такій роботі основні ресурсномісткі операції виробляються на сервері.

– Ноутбук для роботи мобільних користувачів. Припустимо окремо виділити ноутбук для VIP користувачів.

Вимоги до системного ПЗ робочих місць користувачів

ОС офісного призначення повинні:

– Відповідати по типі клієнтським ОС.

– Підтримувати всі мережні сервіси, що забезпечують функціонування корпоративної мережі.

– Забезпечувати необхідний рівень інформаційної безпеки, відповідати вимогам «Політики інформаційної безпеки».

– Бути сумісними з корпоративним стандартом використовуваного офісного ПЗ.

Вимоги до периферійних пристроїв

Справжній розділ викладає основні технічні вимоги до застосовуваним і закуповуваним для служб Замовника периферійним пристроям, що входять в IT інфраструктуру.

Розглядаються вимоги до наступних класів периферійних пристроїв:

– Пристрою друку (принтери):

– Монохромні принтери (персональні й групові використання).

– Кольорові принтери (персональні й групові використання) для офісної й фотографічного друку.

– Кольорові рулонні принтери для дизайну, картографії (персональні й групові використання).

– Пристрою сканування:

– Сканери персональні.

– Сканери фотографічні й дизайнерські.

– Сканери широкоформатні.

– Потокові сканери.

– Багатофункціональні пристрої:

– Персональні БФП.

– БФП групового й корпоративного використання.

– Пристрою копіювання паперових документів:

– Персональні копіри.

– Копіри групового використання.
– Копіри корпоративні – міні друкарні.
– Факсимільні апарати.

Вимоги до спеціалізованих пристроїв, що мають вузьке технологічне застосування (термопринтери, принтери штрих-кодів, наклейок, друкарні й т.д.), не розглядаються. Використання спеціалізованого встаткування приймається на основі конкретних технічних вимог технологічного процесу.

Для опису мінімальних вимог до периферійного встаткування використовується наступна класифікація пристроїв:

– Персональний пристрій – перебуває в постійному використанні одним співробітником.
– Груповий пристрій – використовується в режимі поділу ресурсів групою співробітників.
– Корпоративний пристрій – використовується в складі гіперЦОД I або II рівнів.

Загальні вимоги

У даному розділі викладаються загальні вимоги, які необхідно застосовувати при виборі й закупівлі нового периферійного обладнання з метою розвитку IT Замовника. Периферійне встаткування повинне відповідати наступним основним вимогам:

– Продуктивність. Периферійне встаткування повинне забезпечувати потреби бізнес-процесів і задовольняти вимогам, певним у кількісних показниках (наприклад, кількість копій у мінуту, дозвіл скануємого зображення й т.д.).
– Надійність. Периферійне встаткування повинне дозволяти забезпечувати безперервність бізнес-процесів і задовольняти вимогам, певним у кількісних показниках (MTBF).
– Функціональність. У тому випадку, якщо робоче місце співробітника повинне бути обладнане декількома видами периферійного встаткування, варто віддавати перевагу при закупівлі багатофункціонального пристрою (БФП), що повинне підтримувати всі або частково всі наступні функції:
– друкованого пристрою;
– скануючого пристрою;
– копіювального пристрою;
– факсимільного пристрою.
– Сумісність. Периферійне встаткування повинне технічно й програмно сполучатися з персональними комп'ютерами (у випадку використання групового або корпоративного пристрою – із серверами) незалежно від типу процесора й операційної системи.
– Безпека. Вихід з ладу якого-небудь периферійного пристрою не повинен впливати на усталену роботу персональних комп'ютерів (у випадку використання групового або корпоративного пристрою – серверів) з іншим периферійним устаткуванням.
– Керованість. Підключення й керування персональним периферійним устаткуванням по можливості повинні бути простими й не вимагати оперативного використання інструкцій і описів роботи пристроїв.
– Низька ТСО. Запчастини й видаткові матеріали для периферійного встаткування повинні бути легко доступні й мати невисоку вартість.
– Низький рівень створюваного акустичного шуму. Периферійним устаткування в процесі роботи не повинне створювати перешкод навколишньої. Рівень шуму не повинен перевищувати 55 дб [А]. Для експлуатації гучного встаткування повинні бути передбачені спеціально виділені приміщення.
– Низьке енергоспоживання. Рекомендується придбання встаткування, що має режим зниженого енергоспоживання (режим очікування).

– Варто віддавати перевагу тим периферійним пристроям, які в штатному режимі мають можливість обміну інформацією через локальну мережу.

– Ті периферійні пристрої, які мають можливість підключатися як до ПК, так і до локальної мережі варто підключати до локальної мережі.

Вимоги до групових і корпоративних пристроїв

Для групових і корпоративних пристроїв повинні застосовуватися більше тверді вимоги, ніж до персональних пристроїв. При виборі групових і корпоративних пристроїв необхідно виходити з оцінки кількості користувачів, які будуть експлуатувати дані пристрої.

Крім зазначених вище загальних вимог, для групових і корпоративних пристроїв необхідно розглянути наявність наступного функціонала (застосовно до відповідних пристроїв):

– Наявність клієнтського додатка для ПК для прийому й розсилання факсів, а також для сканування документів.

– Підтримка формату А3.

– Потокове сканування документів з автоматичним перетворенням у потрібний формат з підтримкою мережного збереження файлів.

– Автоматична факсова розсилання.

БФП повинні проходити періодичне технічне обслуговування, що буде сприяти більше високій доступності пристрою й знизить ТСО. Періодичність даного обслуговування необхідно визначати з технічних вимог по експлуатації кожного конкретного пристрою.

Вимоги до мультисервісної мережі

Вимоги до розподіленої мультисервісної мережі

Загальні вимоги

Основні стратегічні положення й підходи до організації корпоративної розподіленої мультисервісної мережі: орієнтація на архітектуру мереж наступного покоління (NGN).

Дана архітектура називається також архітектура softswitch (softswitch – пакетний комутатор для мереж нового покоління, є носієм інтелектуальних можливостей мережі, координує керування обслуговуванням викликів, сигналізацію й функції, що забезпечують установлення з'єднання через одну або кілька мереж). Дана архітектура дозволяє, міняючи версії ПЗ на Softswitch-ах і самі Softswitch-і, розширювати функціональні можливості, не міняючи встаткування доступу. Крім цього, відповідно до архітектури IMS (Interactive Multimedia Subsystem), стандартизується протокол надання сервісів, що дозволяє, без доробки інтерфейсів взаємодії, підключати будь-які послуги від будь-яких сервіс-провайдерів.

Телефонія, аудіоконференцзв’язок, відеоконференцзв’язок і передача даних повинні ґрунтуватися на єдиної конвергентної мультисервісної мережі, що дозволяє надавати зазначені сервіси, забезпечуючи необхідний і достатній рівень QoS.

NGN-мережа побудована на наступних принципах:

– Розподілена корпоративна архітектура, що забезпечує QoS.

– Висока доступність і надійність мережі.

– Продуктивність, керованість і масштабованість мережі.

– Мультисервісна мережа повинна проектуватися з урахуванням вимог інформаційної безпеки.

Весь трафік повинен бути класифікований на наступні класи, що визначають пріоритет обслуговування:

– Трафік реального часу (телефонний, аудіо й відео).

– Трафік передачі користувальницьких даних.

– Технологічний трафік.

Якщо технологічне встаткування вимагає найвищого класу обслуговування, то його трафіку повинен бути відданий найвищий пріоритет. Після цього повинен іти трафік реального часу, після якого треба трафік користувальницьких додатків. Причому пропускна

здатність мережі й активне мережне встаткування повинні завжди забезпечувати якість для трафіку реального часу.

При аварійних ситуаціях ресурси мережі повинні віддаватися технологічному трафіку й частини трафіку реального часу й користувальницького трафіку в тому обсязі, у якому це необхідно для забезпечення безперебійної роботи основного технологічного встаткування й обслуговуючого його персоналу. Даного правила повинні бути реалізовані в настроюваннях устаткування й набувати чинності автоматично при настанні аварійної ситуації.

Вимоги до архітектури мережі

Архітектура мультисервісної мережі повинна бути заснована на наступних принципах:

– Будуватися на трирівневої моделі.
– Мати резервування по встаткуванню й каналам.
– Підтримувати VLAN.
– Архітектурно розбиватися на демілітаризовані зони (ДМЗ).
– Мережа повинна забезпечувати необхідну для рішення завдань продуктивність.
– Мережа повинна забезпечувати QoS для різних класів трафіку.

Мультисервісна мережа для всіх гіперЦОД повинна проектуватися, виходячи із трирівневої моделі комутації:

– Рівень доступу (Access Layer) – комутатори 2-го рівні моделі OSI з інтелектуальністю 3– 4-го рівнів моделі OSI (з метою забезпечення вимог до мережної безпеки, QoS і т.д.).
– Рівень розподілу (Distribution Layer) – комутатори 3– 4-го рівнів моделі OSI.
– Магістральний рівень / рівень ядра (Core Layer) – комутатори 3- 4-го рівнів моделі OSI.

У випадках, коли використання виділених комутаторів рівня розподілу в якому-небудь сегменті мережі недоцільно через зниження продуктивності мережної інфраструктури, зниження надійності або в силу інших причин, допускається переносити функції комутаторів рівня розподілу на комутатори рівня ядра.

Структурна схема зазначеної трирівневої моделі гіперЦОД наведена на рисунку 1.

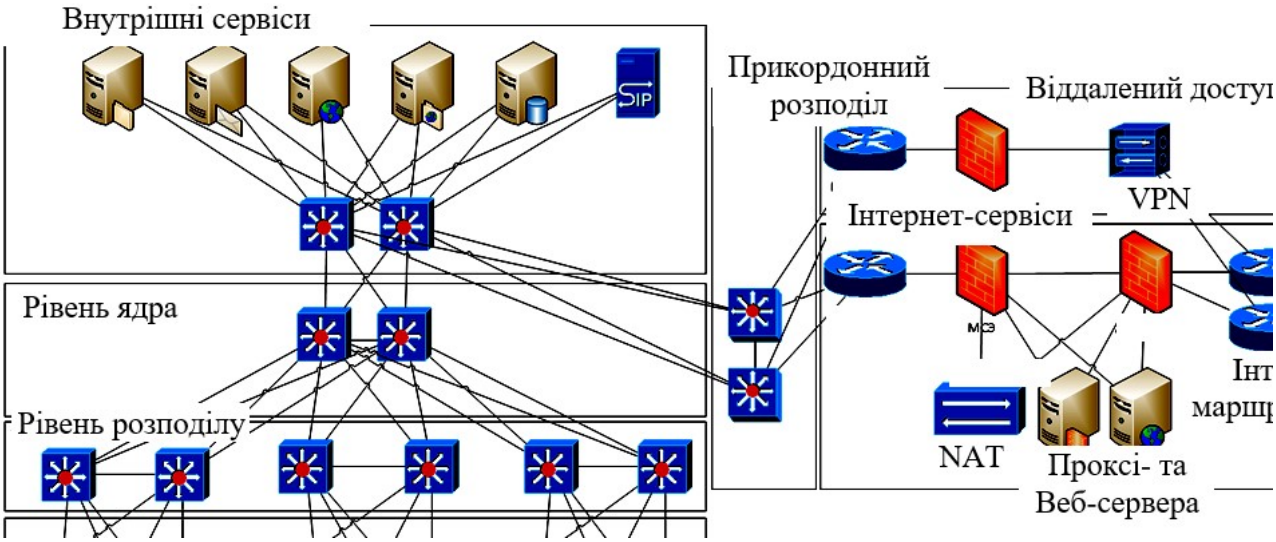

Рисунок 1 – Структурна схема системи

Обрана архітектура мережі повинна дозволяти нарощувати мережу шляхом додавання нових блоків, забезпечувати високий детермінізм поводження мережі, вимагати мінімальних зусиль і засобів для пошуку й усунення несправностей. Інтелектуальні сервіси 3-го рівні моделі OSI (у тому числі протоколи маршрутазації) повинні забезпечувати скорочення області, що зачіпається при виникненні різноманітних проблем з несправним або невірно

настроєним устаткуванням, а також балансування навантаження між/усередині рівнями ієрархії й швидку збіжність.

Повинні бути дотримані загальні правила проектування трирівневої структури:

– Будь-які проблеми з устаткуванням і каналами зв'язку на нижчележачих рівнях не повинні позначатися на верхніх рівнях.

– Транзитні резервні маршрути певного рівня не повинні проходити через нижчележачі рівні.

– Класифікація трафіку повинні відбуватися тільки на рівні доступу. Пріоритизація трафіку повинна підтримуватися всіма рівнями мережі. Рівень розподілу повинен тільки агрегувати трафік. Ядро мережі повинне тільки здійснювати швидку комутацію й маршрутизацію пакетів.

– Час збіжності таблиць маршрутизації і їхній обсяг повинні бути оптимізовані для кожного рівня за допомогою вибору оптимальної схеми резервування.

– Віддалені користувачі й зовнішні канали зв'язку не повинні приєднуватися прямо до ядра мережі. Необхідно використовувати комутатори доступу для запобігання лавиноподібних налаштувань таблиць маршрутизації всієї мережі.

– Забороняється використання некерованих комутаторів. Мінімально припустимий комутатор у мережі – керований комутатор рівня 2.

Резервування для гіперЦОД I рівня повинне, а для гіперЦОД II рівня рекомендується організовувати в такий спосіб:

– У мережі повинне бути не менш двох комутаторів рівня ядра, зв'язаних між собою по 10 (або вище) GigabitEthernet, або об'єднаних в відказостійкий стек з еквівалентною пропускною здатністю.

– Кожний комутатор рівня доступу повинен мати з'єднання каналами Gigabit Ethernet із двома комутаторами рівня розподілу.

– Кожний комутатор рівня розподілу повинен мати з'єднання каналами Gigabit Ethernet (або вище) із двома комутаторами рівня ядра.

– Для забезпечення відказостійкості в мережі повинне бути два прикордонних маршрутизатори. Маршрутизатори підключаються кожний до не менш чим двох різних інтернет-провайдерам і здійснюють маршрутизацію пакетів по протоколі BGP. Кожний прикордонний маршрутизатор повинен бути пов'язаний із двома пристроями, що забезпечують функціональність міжмережного екрана (MME) або IDS/IPS.

– Для забезпечення незалежності від інтернет-провайдерів повинна використовуватися автономна системи (AS) із власним пулом ip-адрес (не менш /22).

Продуктивність мережі повинна бути забезпечена в такий спосіб:

– Поетажні комутатори (комутатори доступу) повинні з'єднуватися з комутаторами рівня розподілу по GigabitEthernet або 10 GigabitEthernet.

– Сервери повинні з'єднуватися з комутаторами рівня розподілу по GigabitEthernet або 10 GigabitEthernet. При необхідності допускається підключення серверів до комутаторів рівня ядра.

– Комутатори рівня розподілу і ядра повинні бути обрані відповідної продуктивності. При виборі рівня продуктивності, необхідно враховувати вимогу підтримки всіх необхідних протоколів з необхідним рівнем QoS.

– Між двома будинками рекомендується прокладати оптичні канали. При більших відстанях, необхідності пропуску великого обсягу трафіку й більших швидкостей передачі даних рекомендується організовувати канали зв'язку на основі технології оптичного ущільнення (xWDM) і агрегації каналів.

Надійність мережі повинна бути забезпечена за допомогою виконання наступних правил:

– Устаткування магістрального рівня повинне мати резервування всіх компонентів.

– Мережа повинна бути спроектована з урахуванням вимог інформаційної безпеки відповідно до вимог «Політики інформаційної безпеки».

– У мережі повинні використовуватися VLAN. VLAN повинні в обов'язковому порядку захищатися всі ресурси мережі й користувачів, які мають підвищену захищеність згідно «Політиці інформаційної безпеки».

Підтримка масштабованості мережі повинна бути забезпечена в такий спосіб:

– За рахунок правильного впровадження трирівневої моделі комутації.

– За рахунок масштабованості комутаторів, що повинна досягатися за рахунок об'єднання комутаторів у групи (стеки). Причому кожний комутатор у стеці повинен працювати у двох режимах – як головний комутатор стека і як процесор комутації пакетів. Повинна забезпечуватися відказостійкість системи за схемою 1:N (при виході з ладу одного з комутаторів стека, незалежно від виконуваної їм функції, інші будуть продовжувати виконання своїх функцій без зупинки роботи всієї мережі).

– Рекомендується використовувати динамічний протокол внутрішньої маршрутизації OSPF як володіє гарною масштабованістю, швидкою збіжністю, що враховує якість каналів зв'язку й займає мінімальну смугу каналу.

Система IP-адресації мережі повинна забезпечувати:

– Поділ адресного простору на службовий блок (мережі, що зв'язують маршрутизатори, віртуальні інтерфейси й т.п.) і блок адрес локальної мережі. Такий поділ дозволяє ефективно будувати правила доступу до мережних пристроїв.

– Розподіл адресного простору локальної мережі блоками відповідно до територіального розташування. Такий поділ дозволяє робити агрегування адрес, що приводить до зменшення таблиць маршрутизації й спрощує керування мережею.

Для здійснення автентифікації на рівні доступу для всіх пристроїв, що забезпечують функціонування мережі, і при доступі до консолі керування всіма пристроями, мережа повинна мати наступні можливості:

– Безпека портів, тобто повинна бути можливість використання порту комутатора з попередньо заданими фізичними адресами користувальницьких ПК (MAC-адреси). При спробі підключення неавторизованого пристрою повинне вироблятися відключення цього порту й повідомлення системи керування мережею.

– Автоматичне конфігурування портів комутаторів, тобто повинна бути автоматизація зміни конфігурації порту на основі логічного підключення користувача до мережі.

– Автентифікація адміністративного доступу на Radius сервері, тобто повинна бути ідентифікація, авторизація й облік при доступі до командного рядка пристрою.

– Обмеження доступу по IP адресах, з урахуванням обмеження на доступ до командного рядка пристрою й системної консолі, а також SNMP трафіку.

– Повинна бути автоматична фільтрація трафіку невикористовуваних протоколів на портах комутаторів.

Для забезпечення високої доступності мережі рекомендується використовувати наступну функціональність:

– Підтримка протоколу RSTP/MSTP або інших протоколів резервування другого рівня.

– Підтримка можливості поєднувати в єдиний логічний канал кілька фізичних з'єднань між комутаторами.

– Функції автоматичного перемикання з основного маршрутизатора на резервний у випадку відмови основного.

– Балансування навантаження між резервуємими маршрутизаторами.

– Функції внутрішнього програмного забезпечення для поліпшення часу збіжності протоколів маршрутизації й балансування навантаження через рівноцінні маршрути.

Для підтримки додатків, заснованих на технології багатоадресного розсилання IP Multicast, від мереж потрібне наявність наступних можливостей:

– На рівні доступу/розподілу – передача пакетів IP Multicast на канальному рівні на швидкості фізичного каналу, динамічна реєстрація за допомогою протоколів IGMP і PIM.

– Магістральний рівень – передача пакетів IP Multicast на канальному й мережному рівнях на швидкості фізичного каналу, масштабовані протоколи маршрутизації трафіку IP Multicast.

Вимоги до телефонії, аудіо- і відео-конференцзв'язку

Основний протокол передачі аудіо- і відеоінформації – IP. Допускається використання традиційної аналогової телефонії в наступних випадках:

– Успадковані існуючі телефонні станції.

– Економічна доцільність. Дане виключення діє до моменту, коли вартість VoIP телефонів стане порівнянна із ціною аналогового телефону.

VoIP переважно повинна впроваджуватися за технологією SIP, тому що дана технологія, у порівнянні з H.323, використовується в мережах наступного покоління й має більшу функціональність. При цьому необхідно звертати увагу на сумісність реалізації протоколу SIP між прикінцевими пристроями й програмно-апаратним комплексом, що забезпечує функціональність телефонної станції. Дана сумісність повинна виражатися в підтримці основного функціонала по обробці вступників дзвінків з прикінцевих пристроїв. З метою недопущення проблем, пов'язаних з несумісністю реалізації протоколу SIP, рекомендується встановлювати прикінцеві пристрою (телефони) і програмно-апаратні комплекси, що забезпечують функціональність телефонної станції, одного виробника, або проводити ретельне лабораторне тестування сумісності апаратури різних виробників.

Системи відеоконферензв'язку повинні підтримувати Web-конференції й інтегруватися з офісними додатками.

Сервера аудіоконференцзв'язку повинні підтримувати або мати можливість розширення для підтримки відеоконференцзв'язку.

Відеоконференцзв'язок повинен організовуватися на технології IP з використанням стандартів H.323/H.264.

При пакетної передачі за еталон якості мови повинен бути прийнятий рівень якості, рівний 4 балам по шкалі MOS/PAMS (Mean Opinion Score, суб'єктивний метод оцінки відповідно до рекомендації P.800). Рекомендується використовувати кодек G.729 (MOS = 4.07). Вимоги до параметрів якості пакетної передачі: затримка пакетів – до 150 мс, джиттер – до 50 мс.

При наявності двох і більше провайдерів, включаючи традиційну телефонію й VoIP, рекомендується використовувати LCR – вибір провайдеру по найменшій вартості. При цьому встаткування VoIP повинне забезпечувати моніторинг якості каналу зв'язку.

Вимоги до встаткування

Устаткування рівня доступу повинне мати можливість класифікації трафіку (Traffic Classification), тобто повинна бути забезпечена можливість класифікувати трафік по типах додатків, фізичним і мережним адресам джерел і одержувачів, портам комутаторів. Класифікований трафік повинен одержувати мітку, що позначає призначений пакетам рівень пріоритету, тим самим даючи можливість пристроям мережі відповідним чином обслуговувати цей трафік. Повинна бути забезпечена рекласифікація пакетів на основі заданій адміністратором політики якості обслуговування. Наприклад, користувач призначає високий пріоритет своєму трафіку й передає його в мережу. Цей пріоритет може потім бути знижений відповідно до мережної політики, а не на основі вимог користувача. Даний механізм повинен бути ключовим у забезпеченні якості обслуговування в рамках всієї мережі.

Устаткування магістрального рівня повинне мати наступну функціональність:

– Запобігання й керування перевантаженнями, тобто повинна бути забезпечена можливість управляти поводженням мережі при перевантаженнях, відкидаючи певні пакети

на основі класифікації або політики в моменти перевантаження мережі й безлічі черг на інтерфейсах. Адміністратор повинен установлювати граничні значення для різних рівнів пріоритету.

– Планування, тобто повинна бути забезпечена можливість здійснювати пріоритетну передачу пакетів, засновану на класифікації або політику якості обслуговування, за допомогою декількох черг.

– Резервування основних вузлів, до яких може ставитися: блок живлення, блок вентиляторів, процесорний модуль.

– Надавати можливість поглибленого аналізу потоків мережного й транспортного рівнів за допомогою протоколу IPFIX (RFC 3917), Netflow, J-Flow або іншого протоколу надання агрегованої статистики по ip-потоках.

У гіперЦОД I і II рівня крім забезпечення резервування основних вузлів устаткування магістрального рівня, рекомендується забезпечити таке ж резервування для встаткування рівня розподілу.

У всьому активному мережному встаткуванні повинні бути засобу моніторингу політики якості обслуговування й безпеки, планування мережі й сервісів:

– Повинна бути забезпечена можливість збору статистики з точністю до порту мережі для аналізу продуктивності й виявлення вузьких місць мережі.

– Повинна бути забезпечена можливість перенаправляти трафік окремих портів, груп портів і віртуальних портів на аналізатор протоколів для детального аналізу.

– Повинна бути забезпечена можливість розширеного моніторингу подій у реальному часі для розширення можливостей діагностики, крім зовнішніх аналізаторів.

– Повинна бути забезпечена можливість збору й збереження інформації про істотні мережні події, включаючи зміни конфігурацій пристроїв, зміни топології, програмні й апаратні помилки за технологією syslog.

– Повинна бути забезпечена можливість доступу до інтерфейсу керування пристроєм і звітам через стандартний WEB-Браузер з використанням протоколу HTTPS.

– Повинна бути можливість підключення до пристрою для його настроювання з використанням протоколу ssh.

– Повинна бути забезпечена можливість автоматичної конфігурації Fast/Gigabit Ethernet портів, віртуальних мереж, транків VLAN.

– Повинна бути забезпечена можливість автоматичного розпізнавання топології мережі за допомогою агентів розпізнавання топології.

– З метою забезпечення продуктивності локальної мережі, її масштабованості, задоволення вимогам інформаційної безпеки й забезпечення якості обслуговування мультисервісного трафіку, забороняється використовувати концентратори (hub). Замість них повинні використовувати тільки комутатори (switch).

Все активне встаткування повинне мати конструктивне 19” стоечне виконання.

Вимоги до зовнішніх каналів зв'язку

Даний розділ розглядає технічні вимоги до зовнішніх каналів зв'язку, які надаються сторонніми операторами зв'язку.

Загальні положення

З метою уніфікації необхідно виділити наступні використовувані види каналів зв'язку:

– Телефонні цифрові потоки E1 PRI.

– Виділені канали передачі даних із шириною від 64 кбіт/с до 2 Мбіт/с і вище.

– Орендовані канали мережі передачі даних.

При виборі виду каналу зв'язку перевага необхідно віддавати каналам зв'язку, які підключаються до мережі MPLS оператора, тому що тільки мережі MPLS у цей час ефективне забезпечують QoS для мультисервісного трафіку при прийнятній вартості послуги. Інтерфейс підключення, що рекомендується – Ethernet, точка-точка.

Канали зв'язку для з'єднань точка-точка або точка-багатоточка між гіперЦОД I і II рівнів повинні організовуватися за допомогою технології MPLS або іншої технології, що забезпечує виконання необхідних вимог по пропускній здатності каналу і якості надання послуги, що підтримує оператор зв'язку. При цьому повинен бути укладений договір, що передбачає забезпечення QoS для аудіо- і відеоданих, якщо такі є. Вимоги повинні бути зазначені у відповідному SLA.

При підключенні гіперЦОД I і II рівнів оператор зв'язку повинен забезпечити цілодобову службу технічної підтримки, що у будь-який час доби не тільки приймає заявки, але й усуває інциденти.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління гіперЦОД.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем управління гіперЦОД.
– Досліджена система управління гіперЦОД.
– На основі отриманих результатів досліджень створена програмна реалізація системи управління гіперЦОД.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання управління гіперЦОД. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
2. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
3. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
4. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
5. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
6. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
7. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
8. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
9. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
10. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
11. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
12. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.

13. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
14. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
15. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
16. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
17. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
18. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
19. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
20. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
21. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
22. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
23. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
24. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.