УДК 658.51

І.Д. Гаркуша, асп.

Л.Ю. Маноха, канд.техн.наук

ДОСЛІДЖЕННЯ І ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ СТВОРЕННЯ ЦЕНТРІВ ОБРОБКИ ДАНИХ В ОРГАНІЗАЦІЯХ З РОЗГАЛУЖЕНОЮ ІНФРАСТРУКТУРОЮ

Дано визначення центру обробки даних та виділено основні його складові. Проаналізовано функції, які забезпечуватимуться з впровадженням центру. Досліджено і обґрунтовано доцільності створення ЦОД в організаціях з розгалуженою інфраструктурою, приведено приклад архітектури такого центру.

Ключові слова: Цент обробки даних, інженерна інфраструктура, телекомунікаційна система, технічна архітектура, моніторинг

Determination of center of the data processing is given and selected basic his constituents. Functions which will be provided with introduction of center are analysed. It is explored and grounded to expedience of the Data Centers creation in organizations with the ramified infrastructure, resulted the example of architecture of such center.

Key words: Data Center, engineering infrastructure, telecommunication system, technical architecture, monitoring

В організаціях з великою розгалудженою інфраструктурою швидкими темпами росте число серверного та комутаційного обладнання. Консолідація ресурсів і додатків разом зі змінами в серверному парку диктує нові вимоги і підходи до конфігурації інженерних систем. Від нової інфраструктури вимагається мінімізація ризиків внаслідок перебоїв в енергопостачанні, перепадів температури і порушення кліматичних умов, недотримання правил протипожежної безпеки, відключення каналів зв'язку. Поняття технологічних приміщень набуває нових рис, так окреме існування комутаційних та серверних кімнат втрачає будь-який сенс, їм на зміну приходять центри обробки даних (ЦОД).

Центри обробки даних (Data Center) — це комплекс програмних і апаратних компонентів, організаційних процедур і персоналу, що забезпечує автоматизацію діяльності. ЦОД об'єднує велику кількість програмних та апаратних платформ різного типу — серверів, дискових масивів, бібліотек, операційних систем, систем управління навантаження та засобів резервування даних.

Первинна функція ЦОД — це розміщення устаткування для обробки та зберігання інформації, а також допоміжних (інженерних) засобів, що забезпечують його роботу;

На даний час багато підприємств України мають побудовану розгалуджену корпоративну мережу, в якій функціонують дуже важливі для роботи підприємств інформаційні системи, проте мало які організації мають єдиний центр управління такою системою. Тому нині виникає потреба створення єдиного центру обробки даних для розміщення вузла IT (інформаційних технологій) і системи резервування.

Хоча створення інформаційної системи у кожній організації має свою специфіку, існують загальні підходи до формування як усієї інформаційної системи так і інженерної структури.

Структура ЦОД має враховувати специфіку організації, тому склад та конфігурація апаратних та програмних платформ оптимізується у відповідності з обчислювальним навантаженням. Параметр технічних засобів (потужність, ємність сховищ, пропускна здатність каналів передачі даних) мають дозволити створювати високорівневі технічні рішення. Тому характеристики і задачі конкретних серверів, систем і сховищ зберігання даних, телекомунікаційних каналів та програмного забезпечення вибираються та задаються для реального забезпечення неперервності бізнес-процесів підприємства та мінімізації витрат на їх використання.

Серверні обчислювальні платформи є ядром ЦОД, тому вони повинні забезпечувати віртуалізацію обчислювальних ресурсів та виконання гетерогенного програмного забезпечення.

Другою ключовою складовою ЦОД є системи зберігання даних, до яких також висуваються досить високі вимоги. Це, насамперед, забезпечення цілісності та доступності, а також високий ступінь масштабованості та резервування, що забезпечує збереження даних та відмовостійкість системи.

І, нарешті, надійне функціонування ЦОД неможливе без інфраструктури приміщення,

Інженерна інфраструктура ЦОД повинна відповідати наступним вимогам:

— забезпечувати повну фізичну безпеку обладнання з розміщеною на ньому інформацією (захист від пожежі, води і протипожежної рідини, електромагнітного випромінювання, несанкціонованого доступу, пилу, диму, падаючих уламків та вірусних атак);

—забезпечувати безвідмовну працездатність обладнання;

—дотримувати необхідні для функціонування обладнання кліматичні умови;

—забезпечувати проведення сервісних робіт без відключення обладнання;

—розподіляти зони відповідальності в залежності від задач доступу персоналу до різних пристроїв і ресурсів;

—мати можливість масштабованості / перенесеності рішень в цілях нарощування/резервування.

На сьогоднішній день відсутній єдиний стандарт для побудови ЦОД, тому проектувальники користуються американським стандартом EIA/TIA-942 або європейським стандартом EN50173-5. Стандарт TIA визначає ЦОД як будівлю або його частину, призначену насамперед для розміщення обладнання обробки і зберігання даних, функціонування якого забезпечується допоміжними системами. Старий радянський стандарт на організацію і функціонування машинних залів не відповідає сучасним технологіям і суттєво відрізняється від рекомендацій TIA-942. Новий стандарт узагальнює багатолітній досвід створення ЦОД. Дотримання його рекомендацій дозволить максимально наблизитись до рівня захищеності 99, 999% . Ряд вимог варто прийняти в якості постулату. Це твердження відноситься до базової топології ЦОД, яка показана наРис. 1.

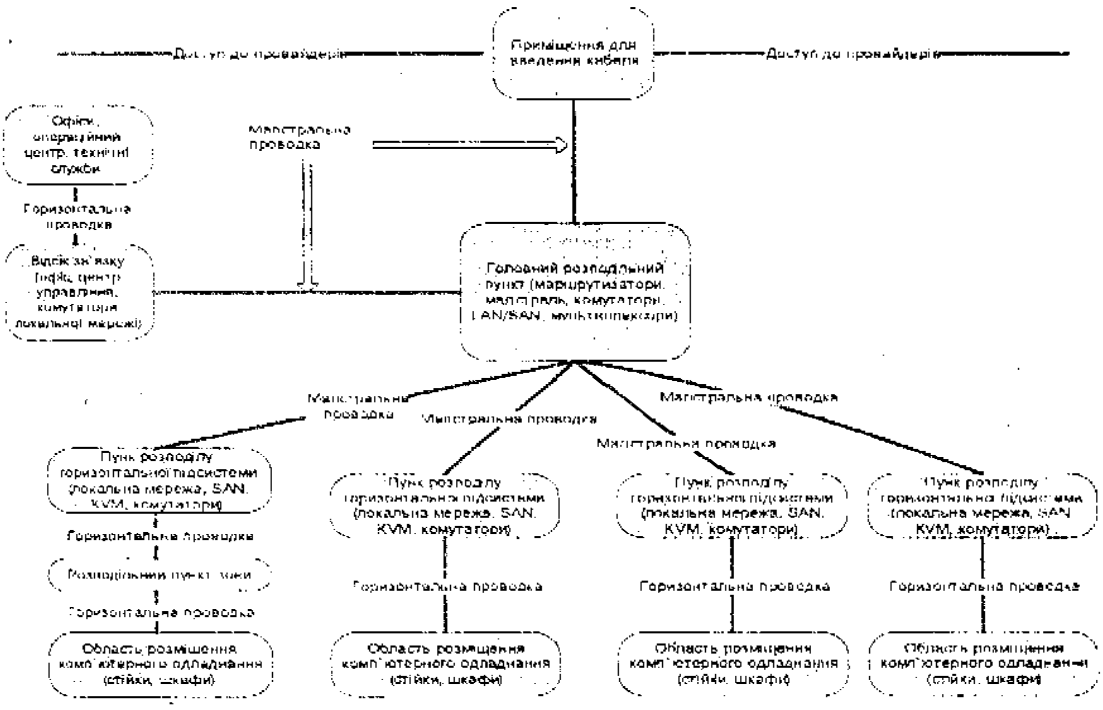

Рис.1 Базова топологія ЦОД згідно ANSI/ EIA/TIA-942.

Вимоги до інженерної інфраструктури визначаються,

зокрема, необхідністю консолідації ресурсів і додатків, що дозволить підвищити рівень керованості, зниження витрат, вищий рівень захисту. Вони стосуються кабельних систем, кондиціювання, електрожив-лення, пожежегасіння, контролю доступу. До їх числа належать підключення до Internet, територіальних і глобальних мереж, забезпечення цілодобового режиму роботи і моніторингу, висока відмовостійкість, над-лишковість, безпека, контролювання параметрів навколишнього середовища, можливість швидкого резервування і зміни конфігурації.

Підхід до створення сучасного центру обробки даних повинен бути комплексним, оскільки необхідний рівень надійності неможливо забезпечити тільки за рахунок побудови ЦОД з якісних елементів. Тому виникає необхідність у впровадженні єдиної системи моніторингу і управління інженерною інфраструктурою ЦОД, яка дозволить досягти бажаного.

Сучасний центр обробки даних є комплексною інженерною спорудою, що забезпечує функціонування бізнес-процесів. Його основу складають три функціональні блоки:

—телекомунікаційна система, що реалізує взаємозв'язок елементів ЦОД, а також прийом/передачу даних між центром і користувачами його сервісів;

—технічна архітектура (сервери доступу, сервери додатків, сервери СУБД, сховища даних), що підтримує функціонування інформаційних систем, доступ користувачів до додатків і зберігання даних;

—інженерна інфраструктура, що забезпечує оптимальні умови для функціонування вищенаведених систем і діяльності обслуговуючого персоналу.

У свою чергу, інженерну інфраструктуру ЦОД можна розділити на підсистему

забезпечення функціонування і підсистему забезпечення безпеки. Перша включає системи загального електропостачання, технологічного кондиціонування, а також монтажні конструктиви.

У підсистему безпеки входять охоронно-пожежна сигналізація, системи автономної газової пожежогасінні і відеоспостереження, контролю і управління доступом.

Проектування архітектури сучасних центрів обробки даних необхідно здійснювати виходячи з розрахунку передбачення можливих відмов устаткування. Сучасні інформаційні системи допускають розпаралелювання процесів збору, обробки, зберігання і надання даних користувачам, а також передбачають механізми захисту від апаратних збоїв. Кластерні рішення і балансування навантаження ще більше підвищують надійність і доступність сервісів ЦОД. Механізми самокорекції, а також розвинені механізми моніторингу стану дозволяють зменшити вплив відмови окремих елементів на систему в цілому.

Огляд факторів, від яких залежить надійність ЦОД показав, що в існуючих комутаційних та серверних кімнатах інженерна інфраструктура часто передбачає лише резервування N + 1, або реалізована взагалі без резервування і не володіє розвиненими системами самодіагностики і раннього виявлення виникачих не-справностей (наприклад, аналогічним SMART). Збій на рівні інженерної інфраструктури приводить до зміни динамічного балансу параметрів навколишнього середовища з їх виходом за допустимі межі. В результаті можлива відмова серверів і іншого устаткування в серверних кімнатах. Вихід з ладу елементів інженерної інфраструктури може викликати як локальну відмову устаткування (перегрів устаткування в одній шафі), так і відмову значної частини обладнання в серверній чи комутаційній кімнаті

(відключення всієї системи кондиціонування).

Більшість апаратних засобів розрахована на роботу при температурі повітря +22±2°С і відносної вогкості 50±10%. Відхилення температури від вказаних параметрів приводить до скорочення терміну служби устаткування (наприклад, акумуляторних батарей), погіршення його характеристик, зниження надійності, збоїв в роботі або навіть повної зупинки (перегріви через високу температуру навколишнього середовища). Низька вологість у приміщенні веде до накопичення статичної електрики, розряд якої здатний вивести з ладу електронні елементи. Внаслідок високої вологості утворюється конденсат, що викликає корозію та може спричинити коротке замикання.

Дослідження Garthner Group встановили, що непередбачені простої інформаційних систем та втрати даних внаслідок збоїв комп'ютерного устаткування чи програмного забезпечення становить лише 25-35% від загального числа збоїв.

Відмова системи електропостачання, перевантаження ліній електроживлення, витік струму, короткі замикання в устаткуванні здатні викликати спрацьовування автоматичних вимикачів. В результаті відбувається знеструмлення тієї або іншої частини устаткуванкя, а несправності важко відшукати внаслідок розгалуженої структури системи і відсутності інформації про стан розподілених пристроїв.

З вищесказаного можна зробити висновок, що збої на рівні інженерної інфраструктури носять масштабніший характер, ніж на рівні додатків і пристроїв, і є причиною збоїв інших елементів архітектури.

Огляд типових проблем інженерної інфраструктури дозволяє встановити, що впровадження високонадійних рішень в різних системах інженерної інфраструктури (наприклад, схеми резервування устаткування 2(N+l)) пов'язано з рядом проблем, що часто зводять

нанівець всі зусилля, вкладені у відмовостійку інженерну інфраструктуру ЦОД:

1) Час реакції на подію. У більшості випадків час реакції на важливі події (протікання рідин, зупинка вентиляторів, пошкодження ізоляції, знеструмлення елементів інженерної інфраструктури, перегрів устаткування) неможливо гарантувати, оскільки такі події: визначаються візуально інженерами чергової зміни під час перевірки серверного приміщення. Як правило, обслуговуючий персонал не має інформації про місцезнаходження джерела виникнення проблеми і причину, що її викликала. Ці фактори значно збільшують терміни усунення аварії.

2) Адекватність реакції. При виникненні аварійних ситуацій або пожежі, реакція співробітників центру, внаслідок стресового стану, може бути неадекватною або неоптимальною. Учбові тривоги і регулярний інструктаж зменшують ризик помилок, але не усувають його.

3)Високе значення людського чинника. Дослідження, проведені організацією The Uptime Institute, довели, що більше ніж 60% відмов інженерної інфраструктури на етапах проектування, монтажу або експлуатації були викликані людським чинником. Більше ніж половина відмов відбувається на етапі експлуатації.

4)Необхідність інтервального регламентного обслуговування. Термін експлуатації інженерної інфраструктури коливається від п'яти до 25 років. Для його збільшення слід періодично проводити регламентне обслуговування, планову заміну окремих комплектуючих з порівняно малим терміном експлуатації і позапланову при закінченні ресурсу або відмові. Досвід експлуатації сучасних ЦОД показує, що контроль (без автоматизованих засобів) і своєчасне обслуговування устаткування виконуються нерегулярно і не в повному обсязі.

5)Внутрішні обмеження інженерних систем серверних та комутаційних кімнат. Доволі часто устаткування інженерної інфраструктури має обмеження за масштабуванням, введенням/виведенням даних, способам управління. Більшість кондиціонерів, наприклад, вимірює температуру «гарячого» потоку повітря і на підставі цього параметра корегує потужність охолоджування повітряного потоку. Локальна температура біля охолоджуваних об'єктів не враховується, і, відповідно, не гарантується підтримка необхідних для роботи устаткування параметрів навколишнього середовища.

6)Відсутність єдиної системи моніторингу стану серверних та комутаційних кімнат. Частина інженерних систем оснащується власними засобами моніторингу і управління, не сумісними один з одним. А у іншої частини іноді їх немає взагалі (системи електроживлення і вентиляції). Повна відсутність інформації про стани всіх інженерних систем ЦОД і параметри навколишнього середовища унеможливлює оперативну оцінку загального стану центру.

7)Неможливість прогнозування / попередження збоїв. Відмова інженерної інфраструктури серверних та комутаційних кімнат веде до відмови рівнів, які розміщені вище. Устаткування інженерної інфраструктури не передбачає моніторингу окремих елементів з необхідним рівнем деталізації. А відсутність інформації про стан і роботу інженерної інфраструктури позбавляє персонал чергової зміни можливості попередження і своєчасного виявлення відмови. Тому існує висока потреба у попередженні відмові ранній діагностиці стану устаткування.

Аналіз архітектурних рішень ЦОД дозволяє зробити висновок, що реалізація системи моніторингу і управління інженерною інфраструктурою ЦОД (рис.2) розв'язує багато

проблем завдяки цілому ряду функціональних можливостей:

1)Практично миттєва реакція на подію. Дані від найкритичніших джерел можна одержувати щомить або частіше, що забезпечує швидку реакцію системи і мінімізує можливі негативні наслідки при виникненні надзвичайних ситуацій.

2)Відсутність людини при ухваленні рішення в екстреній ситуації. Більшість сучасних загроз відома, тому для їх усунення вироблені алгоритми дій, яких необхідно дотримуватись. За рахунок об'єднання всіх інженерних систем в єдину логічну мережу з механізмами ухвалення рішень, вбудованими в контролери автоматизованої системи управління, гарантується належна реакція всієї інженерної інфраструктури ЦОД на надзвичайні ситуації.

3)Зниження значущості людського чинника в рамках експлуатації інженерної інфраструктури. Автоматизована система дозволяє задавати необхідні параметри роботи інженерних систем, контролювати їх дотримання, у безперервному режимі за допомогою незалежних засобів контролю стежити за показниками навколишнього середовища, електроживлення, стану технологічного устаткування. У разі виходу параметрів за задані межі або виявлення відмов черговому персоналу посилаються повідомлення про виникнення інцедентної ситуації, а також видаються рекомендації по її ліквідації.

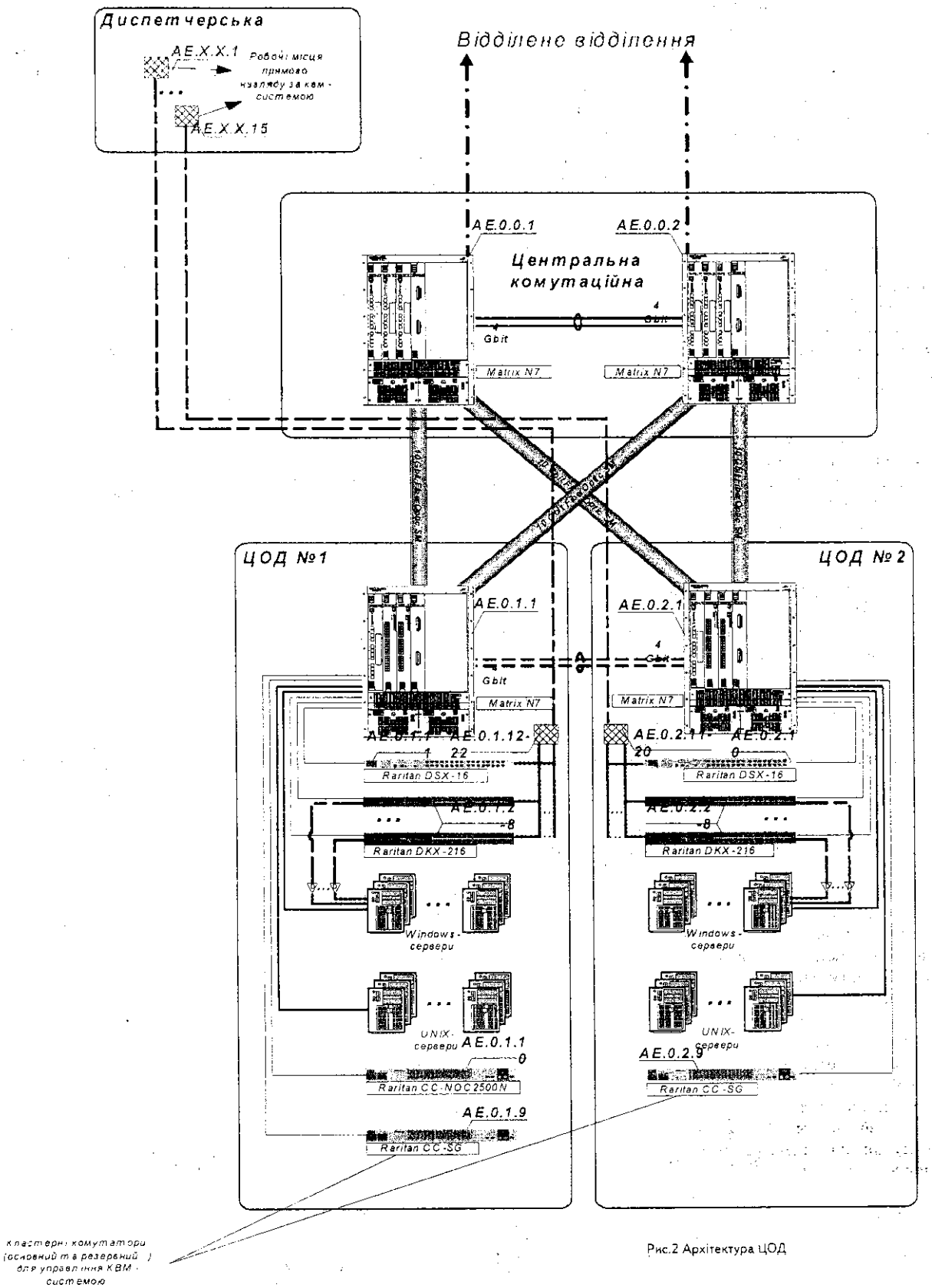

Рис.2 Архітектура ЦОД

4) Розширення можливостей устаткування. На основі температури гарчого повітря, що подається в комутаторів Matrix N7, зв'язок між кондиціонер, але і з якими здійснюється по урахуванням, одержаних з швидкісному і надійному каналу додаткових датчиків (існують основний і резервний встановлених безпосередньо в канали) 10 Gbit FiberOptic SM. місцях надходження повітря у ЦОД№1 і ЦОД№2 мають одне і те ж будь-який пристрій. функціональне призначення і між ними відбуваються реплікації,

5) Єдине середовище ЦОД№2 створено для розподілу моніторингу і управління. навантаження. Щоб забезпечити Чергоий персонал має єдиний резервування даних на віддаленій мнемонічний інтерфейс площадці знаходиться резервний контролю і управління всіма ЦОД, який реплікується з інженерними системами ЦОД. основним. Реалізація ЦОД Це полегшує сприйняття базується на Windows та UNIX інформації персоналом і серверах. дозволяє контролювати всі параметри систем у реальному Windows-серверах часі, своєчасно реагувати на забезпечують наступні задачі: події.

1. Сервіс авторизації;

6) Прогнозування 2. Систему електронного відмов елементів інженерної документообігу всередині інфраструктури. Підключивши організації; додаткові датчики і вимірюючи

3.Інформаційний портал в нестандартні параметри, можна межах організації; вчасно дізнатися про вірогідну

4.Файловий сервіс; аварію.

5.Сервіс друку.

Нарис.2 зображена UNIX-сервера забезпечують архітектура ЦОД. Ядро ЦОД наступні задачі: побудовано на основі потужних

1.Надійну роботу баз даних;

2.Доступ до зовнішніх інформаційних ресурсів;

3.Обмін інформацією з зовнішніми організаціям;

4.Файловий сервіс;

5.Зовнішній інформаційний портал.

Для віддаленого управління такими серверами використовуються кластерні комутатори (основний резервний).

Крім того, впровадження ЦОД забезпечує такі функції як:

— цілодобова автоматична підтримка заданих кліматичних параметрів у будь-якій точці приміщення без участі людини і незалежно від температури зовні будівлі і режимів роботи устаткування з різним рівнем виділення тепла;

— можливість визначення стану системи з робочої станції SCADA за рахунок відображення всіх потрібних параметрів у системі візуалізації. Це звільняє від необхідності візуального контролю параметрів, збудованих в устаткування засобів управління.

— збільшення терміну служби і збереження устаткування при форс-мажорних обставинах. Це забезпечується за рахунок досягнення оптимальних параметрів навколишнього середовища і практично миттєвого часу реакції на події;

— доступ до звітів для аналізу аварійних ситуацій разом з аналізом стану устаткування за певні проміжки часу. Події, що відбуваються в будь – якому з компонентів системи, автоматично реєструються в журналах, структура яких, у свою чергу, дозволяє гнучко і просто аналізувати ситуації;

— протоколювання подій, що відбуваються, і дій персоналу;

—єдиний інтерфейс користувача. Для моніторингу і управління всіма інженерними системами ЦОД потрібен гнучкий і зручний інтерфейс, реалізований відповідно до єдиних принципів. Це забезпечується за рахунок вільної побудови системи візуалізації;

—отримання черговим персоналом довідкової інформації від АСМУ (автоматизованої системи моніторингу та управління).

Надійність інженерних систем безпосередньо впливає на ступінь доступності сервісів центру обробки даних і повинна бути вищою за надійність решти елементів ЦОД. При побудові резервного центру мають бути реалізовані проблемні питання передачі даних, запуску та зупинки додатків, а також організаційні питання — підготовка плану відновлення (Disaster Recovery Plan), що передбачає переведення діяльності з основного ЦОД у резервний та відновлення основного центру.

Для своєчасного реагування або попередження змін, які виникають, та досягнення найкращих виробничих результатів, використовується адаптивний підхід до реалізації ЦОД. Він передбачає поступове нарощування потужності та складу компонентів обчислювального комплексу у відповідності з розвитком технологій та потреб, Розмір IT-кімнатта потужність інженерних комунікацій має розраховуватись для максимальних значень, визначених з урахуванням додавання в ЦОД устаткування, яке підтримує обчислювальні потужності для розвитку інформаційних систем мінімум на 4-5 років.

ЦОД, не обладнаний налагодженою автоматизованою системою управління інженерною інфраструктурою, не в змозі забезпечувати рівень надійності сервісів, який потрібен сучасному бізнесу. Наявність єдиної автоматизованої системи моніторингу і управління інженерною інфраструктурою ЦОД рекомендована для будь-якого рівня його експлуатаційної надійності і є обов'язковою для досягнення надійності вище 99,984% (згідно дослідженням The Uptime Institute і стандарту ANSI-TIA-EIA-942/200 5).

Отже, концепція ЦОД потребує комплексного підходу, який враховує усі складові — будівельні, комп'ютерні, мережеві, інформаційні. Вона визначає методологію створення, технічного обслуговування і модернізації обчислювальних потужностей, що забезпечує мінімізацію ризиків при їх експлуатації.

ЛІТЕРАТУРА

1. Герхарг Унгер Увеличение производительности глобальной сети // Журнал сетевых решений LAN. -2006. — №7 С.38-42

2. *Дирк Трэгер* Хорошая комбинация // Журнал сетевых решений LAN. -2006. — №7 С.48-52

3. *Олександр Мартинюк* Кто должен заниматься управленим проекта строительства ЦОД? // Журнал сетевых решений LAN. -2007. — №2 С.46-49

4. *Туманов О.Е.* Обеспечение непрерывности бизнеса // Финансовый директор. — 2003. — № 9