УДК 004.047

О.В.Копійка

ПРИНЦИПИ ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ ПРИ ФОРМУВАННІ СИСТЕМНИХ ВИМОГ ДО ІНФОРМАЦІЙНОЇ АРХІТЕКТУРИ ЦЕНТІВ ОБРОБКИ ДАНИХ

Розглядається задача побудови інформаційної архітектури Центрів обробки даних, яка складається з: мережної інфраструктури; служби активного каталогу; системи збереження даних; програмно-апаратного забезпечення прикладних сервісів; служби управління даними; резервного копіювання та відновлення; моніторингу та контролю працездатності систем; безпеки та технічного захисту інформації. Дослідження проводились на прикладі IT-інфраструктури ПАТ «Укртелеком».

Ключові слова: центр обробки даних, збереження інформації, безпека та технічний захист інформації.

Введення та постановка задачі

Основною метою досліджень є: надійне збереження інформації; стандартизація і консолідація IT-служб; зниження витрат, пов'язаних з управлінням IT-ресурсами; розробка основних елементів уніфікації програмно-апаратних систем [1-7].

Дослідження проводились на прикладі IT-інфраструктури ПАТ «Укртелеком».

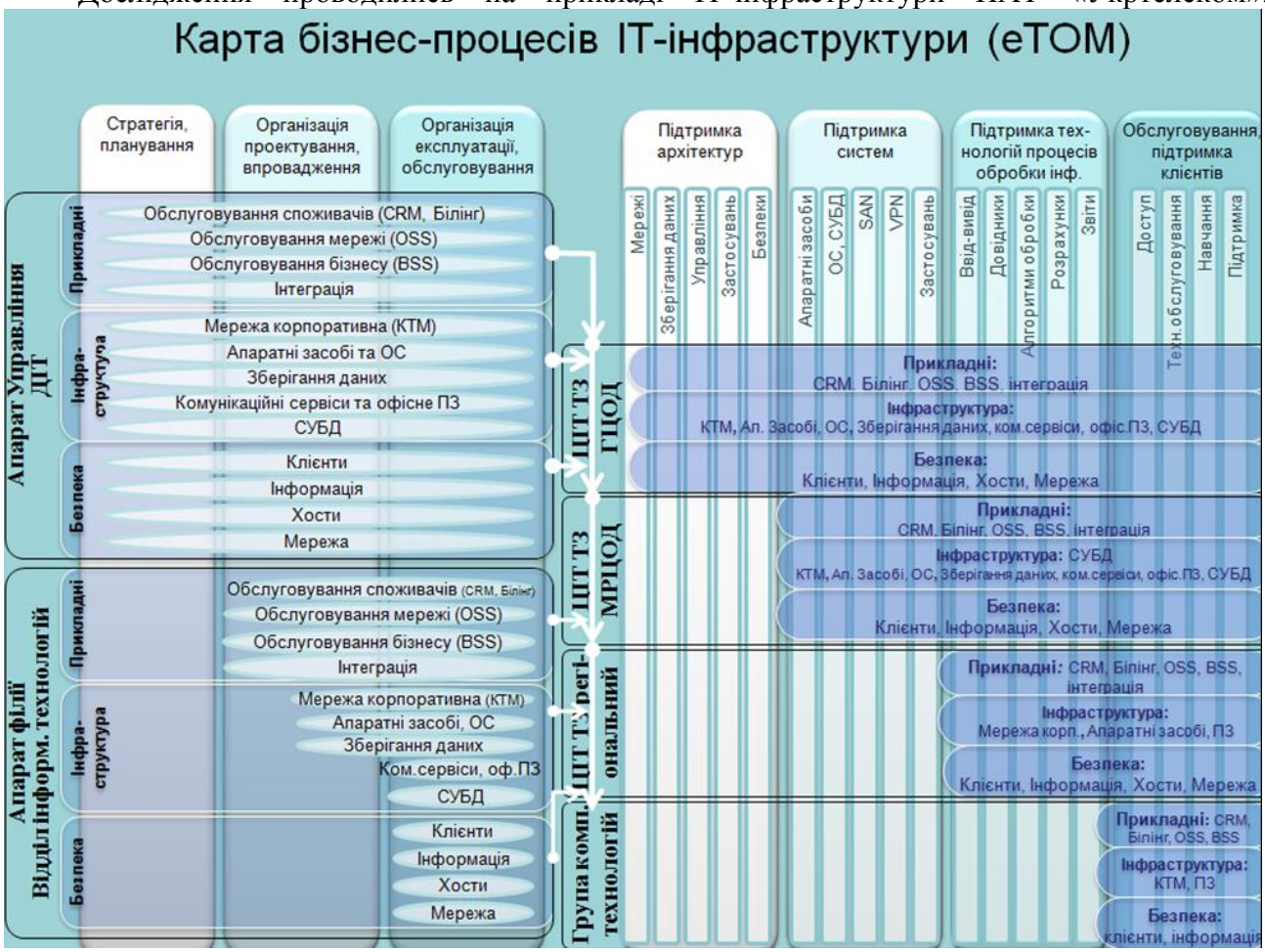

Рис.1 Карта бізнес-процесів IT-інфраструктури

До основних елементів інформаційної архітектури Центрів обробки даних відноситься:

- Мережна інфраструктура Центрів обробки даних.
- Служба Активного Каталогу (AD).
- Система збереження даних.
- Програмно-апаратне забезпечення прикладних сервісів.

– Служба управління даними.
– Резервне копіювання та відновлення.
– Моніторинг та контроль працездатності систем.
– Безпека та технічний захист інформації.

Основна частина

1. Мережна інфраструктура Центрів обробки даних

Основними елементами мережної інфраструктури Центрів обробки даних є:

- Локальна мережа Центру обробки даних.
- Модуль забезпечення балансування трафіку до серверних ферм.
- Мережевий екран (Firewall).

Локальна мережа Центру обробки даних.

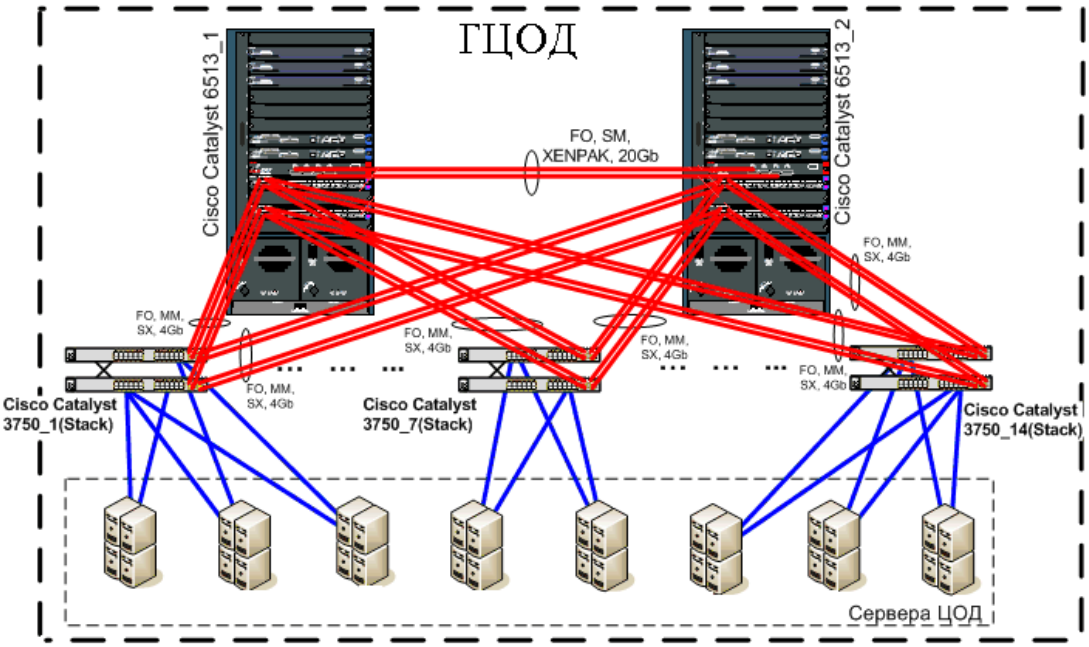

Рис. 2 Мережна інфраструктура Центрів обробки даних

У якості ядра мережі виступають комутатори Cisco Catalyst 6500 серії, комутатори доступу Cisco Catalyst 3750 з підтримкою стикування. Між комутаторами ядра та доступу, побудована багаторівнева відмовостійка схема фізичних лінків, логічних з'єднань, а також розподілення по живленню. Фізичні з'єднання представлені на рис. 2, логічні настройки виконані згідно рекомендацій Cisco System 2007 документ BRKDCT-2002-DC рис. 3 [8,9].

Сервери на рівні доступу повинні підключатися двома спареними інтерфейсами (Teaming) в два комутатори в стеку.

Модуль забезпечення балансування трафіку до серверних ферм.

Модуль забезпечення балансування трафіку до серверних ферм Load Balancer Cisco Content Switching Module (WS-X6066-SLB-APC), мережних екранів, пристроям SSL та VPN. Content Switching Module (CSM) дає можливість одночасно обробляти до 1 млн з'єднань TCP з швидкість встановлення 200 тис з'єднань в секунду. Забезпечує балансування на рівнях від 4 до 7 моделі OSI.

В ПАТ «Укртелеком» було встановлено версію: hardware ver.1.9 , software ver.4.1(2).

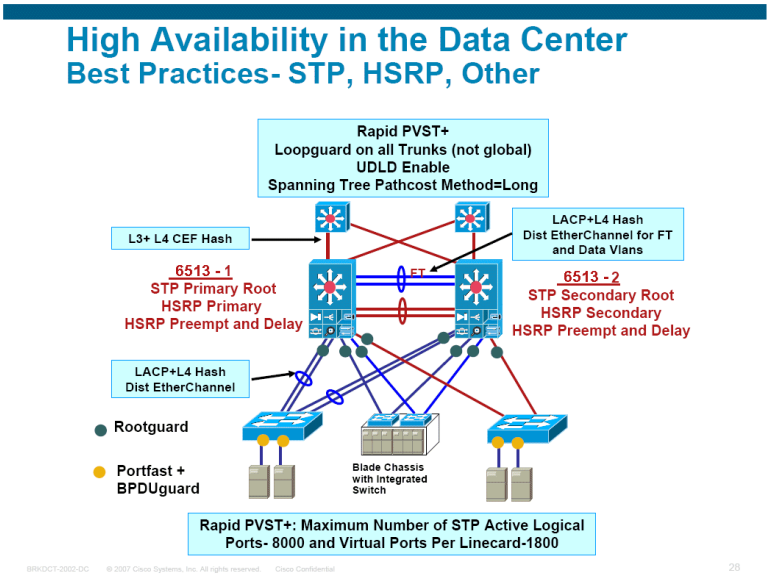

Рис.3 Модуль забезпечення балансування трафіку

Мережевий екран (Firewall).

Мережевий екран (Firewall) Cisco Firewall Services Module (WS-SVC-FWM-1-K9) представляє собою високопродуктивний мережевий екран, який може забезпечувати високу пропускну спроможність до 5 Гбіт/с, з швидкістю встановлення з'єднань до 100000 CPS та 1 млн. одночасних з'єднань. FWSM належить до родини Cisco PIX Firewall та забезпечує такий же рівень захисту, функціональності та надійності, як інші мережні екрани. Забезпечує інспектування трафіку на рівнях 4-7 моделі OSI (рис. 4).

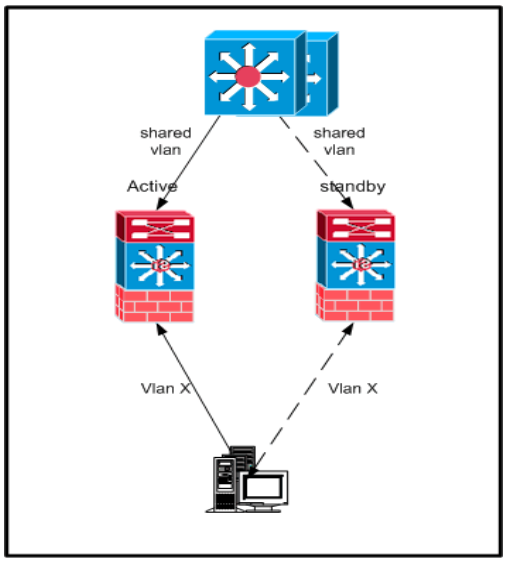

Рис. 4 Високопродуктивний мережевий екран

В ПАТ «Укртелеком» було встановлено версію: hardware ver. 3.0 software ver. 3.2, multi-context mode.

2. Служба Активного Каталогу (AD)

Служба Активного Каталогу забезпечує централізоване керування IT — інфраструктури підприємства. Розгорнута на 4-х серверах головного ЦОД (2 контролера кореневого домену, 2

контролера основного домену, в якому зосереджені основні сервіси та мережні ресурси). Кожен з п'яти регіональних ЦОД містить 2 контролера основного домену.

До складу Служба Активного Каталогу входять:

- Типова апаратна та програмна платформа для контролера домену.
- Логічна структура служби та топологія сайтів.
- Аутентифікація в домені.

Типова апаратна та програмна платформа для контролера домену.

- сервер HP DL380G4;
- операційна система Microsoft Windows Server R2 Enterprise Edition.

Логічна структура служби та топологія сайтів (рис. 5).

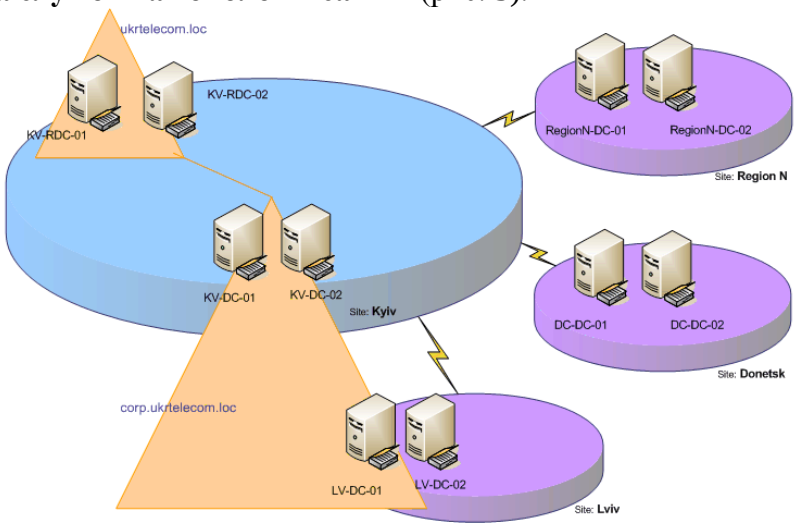

Рис. 5. Логічна структура служби та топологія сайтів

Аутентифікація в домені

Kerberos

В службі АК застосовується системна служба розподілення ключів Kerberos (KDC). Користувачі можуть входити до мережі за допомогою протоколу перевірки автентичності Kerberos 5. Служба перевірки випускає білети на видачу білетів (TGT), а служба видачі білетів – на отримання доступу до ресурсу домену (TGS).

Прикладний протокол	Протокол	Порти
Kerberos;	TCP	88
Kerberos;	UDP	88

Net Logon

На комп'ютерах у складі домену служба Net Logon використовує віддалених виклик процедур (RPC) по іменованим каналам. На контролерах домену використовується віддалених виклик процедур (RPC) по іменованим каналам, віддалених виклик процедур (RPC) по протоколу TCP/IP, слоти повідомлень (mailslot), та протокол доступу до каталогів LDAP.

Прикладний протокол	Протокол	Порти
Служба датаграмм NetBIOS	UDP	138
Разрешение имен NetBIOS	UDP	137
Служба сеансов NetBIOS	TCP	139
SMB	TCP	445
LDAP	TCP	389

3. Система збереження даних

До складу системи збереження даних входять:

- Мережна технологія Fibre Channel (SAN).
- Дискові масиви.
- Логічна діаграма систем збереження даних.

Мережна технологія Fibre Channel (SAN).

Апаратним забезпеченням домену керування SAN виступають директори Fibre Channel 9509, 9506 та FC адаптери HBA Emulex LP9802, Qlogic QLA2XXX.

Директори та комутатори Connectrix серії MDS та FC-адаптери укомплектовані відповідним програмним забезпеченням керування. Схема SAN наведена на рис. 6.

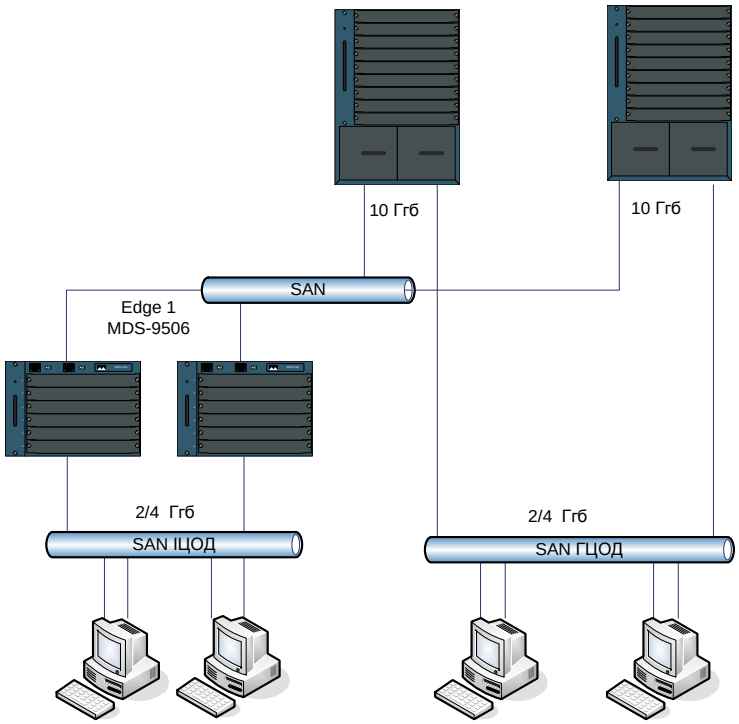

Рис. 6 Схема SAN

Дискові масиви

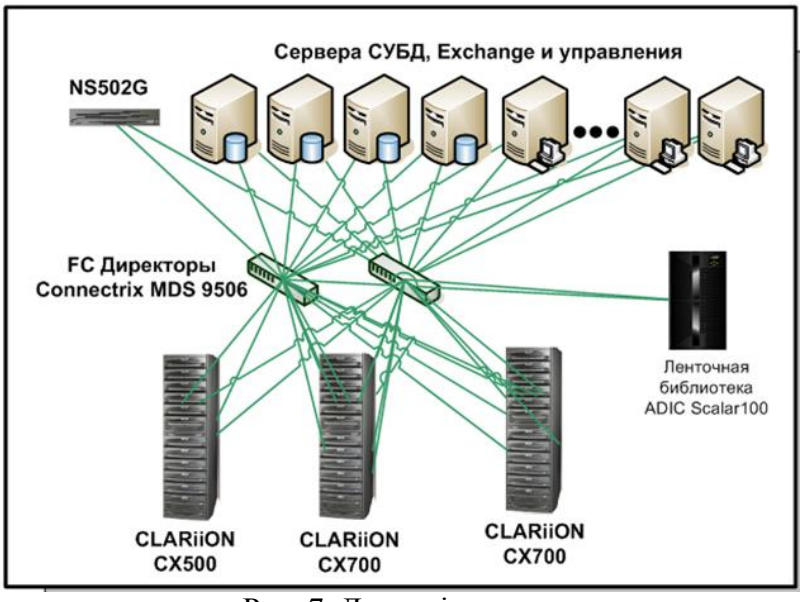

Рис. 7. Дискові масиви

Апаратним забезпеченням домену керування дисковими системами виступають дискові масиви EMC CLARiiON сімейства CX та робочі станції адміністраторів систем збереження даних.

Програмним забезпеченням домену керування дисковими системами виступає ПЗ управління EMC Navisphere Manager, PowerPath та AccessLogix

Системи збереження даних EMC:

- EMC Cellera NS502G NAS;
- EMC CLARiiON CX700;
- EMC CLARiiON CX500;
- EMC CLARiiON CX3-80.

Логічна діаграма систем збереження даних (рисунок 7).

4. Програмно-апаратне забезпечення прикладних сервісів

До програмно-апаратного забезпечення прикладних сервісів відноситься:

- Апаратне забезпечення.
- Програмне забезпечення.

Апаратне забезпечення

- Апаратного забезпечення Hewlett-Packard:
  - HP DL380;
  - HP rx2620;
  - HP rx4640.
- Апаратного забезпечення IBM (Шасі для серверів - IBM BladeCenter™ H)
  - Сервера , що базуються на процесорах Intel

Програмне забезпечення

- Microsoft Windows Server R2 Enterprise Edition English.
- Microsoft Windows Server R2 IA64 Enterprise Edition English.
- HP-UX 11i v2 .
- Linux RedHat (у виключних випадках).

5. Служба управління даними

5.1 Microsoft.SQL Failover кластер

Microsoft. SQL Failover кластер використовується для централізованого управління базами даних, та також для сервісів, які використовують SQL бази даних,

5.1.1. Топологія рішення (рис. 8, 9).

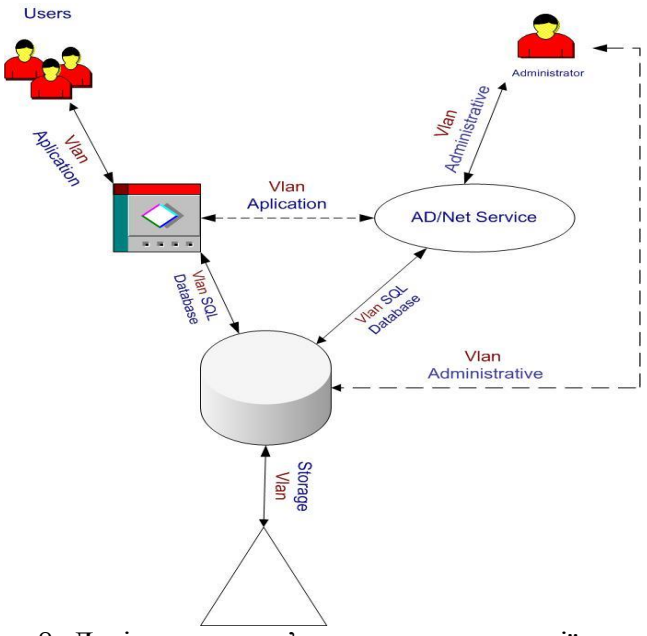

Рис. 8. Логічна схема з'єднання та взаємодії

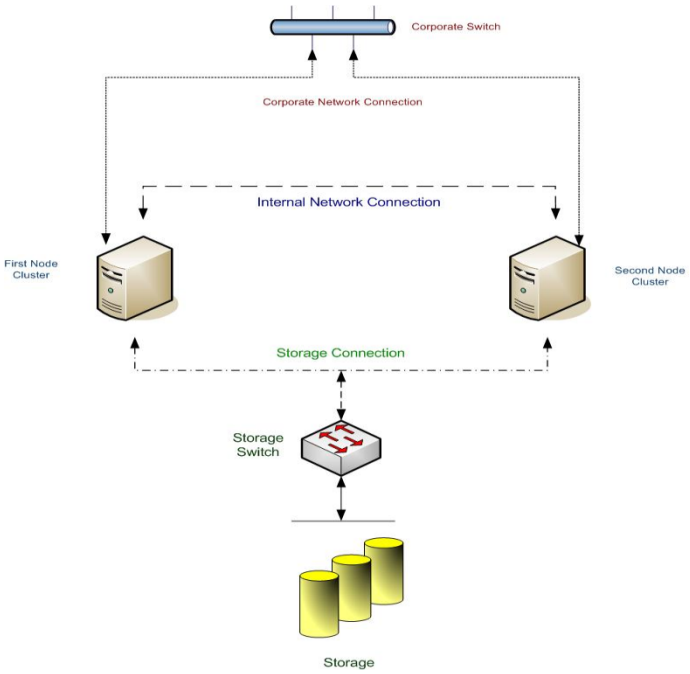

Рис. 9. Схема SQL Failover Cluster

5.1.2. Апаратне забезпечення SQL Failover Cluster
- Hewlett-Packard RX2620, 2 CPU x 1.6 GHz, HDD 2x 36 Gb (RAID 1), 16 GB RAM

5.1.3. Програмне забезпечення
- Microsoft Windows Server with Enterprise Edition IA64
- Microsoft SQL Server with Enterprise Edition 64-bit

5.2. СУБД Oracle

Бази даних розгорнуті на кластерному рішенні Oracle RAC, Oracle 10g

5.2.1. Апаратне забезпечення
- Hewlett-Packard RX4640: 4 CPU, 16GB RAM, 2x72GB HDD, 2 HBA

5.2.2. Програмне забезпечення
- HP-UX 11.0
- Oracle 10g

6. Резервне копіювання та відновлення

6.1. Логічна архітектура сервісу резервного копіювання та відновлення (РКВ)

Сервіс РКВ є робочим елементом для сервісу всієї IT інфраструктури ПАТ «Укртелеком», який, в свою чергу, є метасервісом для сервісу РКВ.

Сервіс РКВ складається із наступних компонентів (рис. 10):
- робочі елементи сервісу;
- система управління сервісу;
- інтерфейси сервісу.

6.2. Апаратне забезпечення
- стрічкова бібліотека ADIC Scalar 100;
- дискові масиви сімейства EMC CLARiiON CX.

6.3. Програмне забезпечення
- програмне забезпечення управління дисковими масивами EMC Navisphere;
- програмне забезпечення створення локальних реплік EMC SnapView (для CLARiiON);
- програмне забезпечення створення локальних реплік EMC SnapSure (для Celerra);
- програмне забезпечення управління системою РКВ EMC Legato Networker;
- спеціалізовані модулі ПО EMC Legato Networker для проведення резервного копіювання та відновлення даних Exchange, MS SQL Server, Oracle;

- мережа збереження даних на базі директорів та комутаторів Cisco;
- сервера розгортання ПО управління РКВ.
- програмне забезпечення централізованого моніторингу та управління системою РКВ на рівні всього ПАТ "Укртелеком" EMC Legato Networker Management Console.

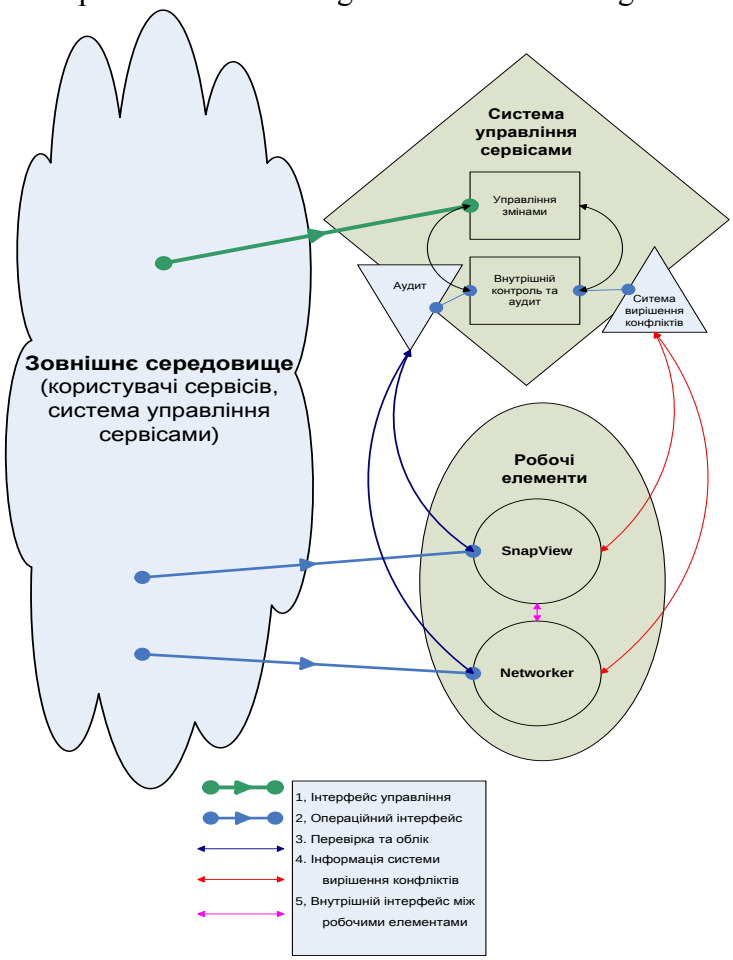

Рис. 10. Сервіс резервного копіювання та відновлення

7. Моніторинг та контроль працездатності систем

Моніторинг та контроль працездатності обладнання та систем ЦОД проводиться за допомогою сервісу Microsoft Operation Manager (MOM). З цією метою на обладнанні, що моніториться, встановлюються агенти MOM, а на сервері MOM – MANAGEMENT PACK, що містить процедури контролю та тестування.

8. Вимоги до безпеки та технічного захисту інформації

Ключові питання захисту систем, що відповідають вимогам Закону України "Про зв'язок":

- Захист та резервне копіювання баз даних (алгоритм та графік).
- Ведення журналів звернень до БД (тривалість – мінімум місяць). Особливу увагу звернути на ведення журналу звернень до БД, що містить особові дані про клієнтів компанії.
- Розподілення доступу до системи (особливо серверних частин) та ведення журналів доступу (хто і коли звертався до яких підсистем Контакт-центру, тривалість звернення).
- Забезпечити контроль (або часткову заборону) використання пристроїв копіювання даних (DVD, FDD, USB, таке інше) на серверах, активному обладнанні та робочих місцях фахівців.
- Створити перелік портів та сервісів контакт-центру, які будуть взаємодіяти з IP-платформою ВАТ “Укртелеком” через вказані на схемі міжмережні екрани (FW).

- Керування сервісами та обладнанням контакт-центру повинно здійснюватись тільки з локальних, розташованих у мережі контакт-центру, терміналів з погодженими для цього IP – адресами (MAC – адресами).
- Оновлення програмного забезпечення контакт-центру, у тому числі й операційних систем.
- Антивірусний захист (у разі використання зовнішніх носіїв).

Висновки

Враховуючи вище сказане, при впровадженні окремих систем в Центрах обробки даних ПАТ «Укртелеком», слід використовувати наявну інфраструктуру, яка складається з наступних елементів:

1. Мережна інфраструктура ЦОД базуються на апаратно-програмних рішеннях компанії Cisco
2. Апаратні платформи рівня СУБД: HP (Серія RX).
3. Апаратні платформи прикладного рівня: HP (серія DL380), IBM (BladeCenter серія H)
4. Апаратні платформи рівня збереження даних: EMC CLARiiON сімейства CX.
5. Програмні платформи рівня СУБД: Windows Server 2003 SP2 with Enterprise Edition IA64 (SQL), HP-UX (Oracle 10g).
6. Програмні платформи прикладного рівня: Windows Server 2003 SP2, HP-UX
7. Резервне копіювання та відновлення: програмне забезпечення EMC Legato Networker
8. Розгортання робочих місць, та оновлення клієнтського ПЗ проводиться за допомогою сервісу System Management Server.
9. Моніторинг працездатності систем проводиться за допомогою сервісу MOM, Cisco Info Center.

Література

1. Информационные технологии – практические правила управления информационной безопасностью // ISO/IEC 17799 МЕЖДУНАРОДНЫЙ СТАНДАРТ - Первое издание 2000-12-01-87 с.

2. Еталонні архітектури MSA. – К.: Майкрософт Україна; К.: Видавнича група BHN, 2005. – 352 с.

3. http://www.tiaonline.org/standards/

4. Jew, Jonathan. BICSI Data Center Standard: A Resource for Today's Data Center Operators and Designers // BICSI News Magazine, May/June 2010- page 28.

5. Niles, Susan. Standardization and Modularity in Data Center Physical Infrastructure // 2011, Schneider Electric – page 4.

6. Telecommunications Infrastructure Standard for Data Centers//TIA STANDARD TIA-942. TELECOMMUNICATIONS INDUSTRY ASSOCIATION - April 2005. - p. 135

7. ANSI/BICSI 002-2011 Data Center Design and Implementation Best Practices// Committee Approval - January 2011 First Published: March 2011 - p. 367

8. Копійка О.В. Архітектура мережі в сучасних дата-центах /О.В.Копійка// Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – № 2(30). – С.34 – 41.

9. Копейка О.В. Сетевые службы и службы сетевых устройств в Дата-центрах/О.В. Копейка//Системи управління, навігації та зв'язку: наукове періодичне видання. – 2013. – Випуск 4 (28). – С. 98-104

Надійшла 01.06.2015 р. Рецензент: д.т.н., проф. Кравченко Ю.В.