

В.О. Юхимець, В.Г. Терентюк, В.А. Науринський, В.В. Куц, В.В. Яровий,
А.С. Єршоміна, О.Л. Мельник, О.С. Лісневич

АВТОМАТИЗОВАНА МЕДИЧНА ІНФОРМАЦІЙНА СИСТЕМА. ВПРОВАДЖЕННЯ ТА ОПТИМАЛЬНІ ТЕХНІЧНІ РІШЕННЯ

ЧАСТИНА 2

ДУ «Національний інститут фтизіатрії і пульмонології ім. Ф.Г. Яновського
НАМН України»
ТОВ «АЛТ Україна Лтд.»

В **1-й частині** статті були наведені визначення АМІС, завдання, які вона вирішує в ЛПЗ, призначення та область її використання, основні застосовані нами технічні рішення, зокрема, архітектура та склад основних підсистем, логічна та функціональна архітектура системи в цілому, рішення щодо захисту інформації. В 2-й частині висвітлені питання технічного та базового програмного забезпечення і структури управління АМІС.

4.4. Технічне та базове програмне забезпечення АМІС.

Для забезпечення роботи програмно-апаратного комплексу «Автоматизована медична інформаційна система» (АМІС), у відповідність до вимог розробленого Технічного завдання, нами було встановлено та використовується відповідне програмно-апаратне середовище, яке включає в себе декілька підсистем. Частина цих підсистем була побудована на базі існуючого обладнання та інфраструктури ЛОМ інституту, частина підсистем була поставлена як складова АМІС:

- підсистема керування локальною мережею, користувачами й серверами, у тому числі серверами й користувачами АМІС (ця підсистема існувала в інституті до початку впровадження):

- контролери домену з операційною системою MS Windows Server 2000/2003, робочі станції відділу інформаційно-комп'ютерних технологій з ОС MS Windows XP і вище, прикладним ПЗ для керування мережею та ін.;

- відмовостійка підсистема обробки транзакцій і збереження даних, що включає сервер БД і дисковий масив із розподілом дисків на декілька окремих відмовостійких масивів (RAID 5, 6, 10):

- дисковий масив DELL PowerVault MD3620f DC + 2 порти 8Gb Fibre Channel
- дисковий масив DELL PowerVault MD1200 + 2 порти 8Gb Fibre Channel

- диски типу 300GB 2.5in 15K 6Gb SAS, 600GB 2.5in 10K 6Gb SAS та 3TB 3.5in 7.2K rpm 6Gb NL SAS;

- блейд-шасі Dell PE M1000e Blade Enclosure;
- шафа DELL PE 4220 42U + Dell UPS Network Management Card;
- джерело безперебійного живлення DELL UPS Rack 5600W 4U 32A 1phase;
- комутатор DELL PowerConnect M6220 Switch 20 Port 3Y;
- комутатор DELL Brocade M5424 FC8 Switch 12 Ports with 2x 8Gb SFPs 3Y;
- комутатор HP-V1905-24;

- сервери DELL PowerEdge M520 2xE5-2407 64GB 0ME2572 DRAG Ent 3Y (2 процесори Intel® Xeon® E5-2407 2.20GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W + 8 модулів 8GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x4 Data Width + On-Board Broadcom 5720 2x Dual Port 1GBE + Qlogic QME2572 8Gbps Fibre Channel I/O Mezz Card for M-Series Blades (сервери термінального доступу);

- сервер DELL PowerEdge M520 2xE5-2420 16GB QME2572 iDRAC Ent 3Y (2 процесори Intel Xeon 6C Processor Model E5-2420 95W 1.9GHz/1333MHz/15MB + 2 модулі 8GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x4 Data Width + On-Board Broadcom 5720 2x Dual Port 1GBE + Qlogic QME2572 8Gbps Fibre Channel I/O Mezz Card for M-Series Blades (сервер АМІС);

- сервер DELL PowerEdge M520 2xE5-2440 64GB QME2572 iDRAC Ent 3Y (2 процесори Intel Xeon E5-2440 2.40GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W + 8 модулів 8GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x4 Data Width + On-Board Broadcom 5720 2x Dual Port 1GBE + Qlogic QME2572 8Gbps Fibre Channel I/O Mezz Card for M-Series Blades (сервер БД SQL);

- сервер DELL PowerEdge M520 2xE5-2420 16GB QME2572 iDRAC Ent 3Y (2 процесори Intel® Xeon® E5-2407 2.20GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W + 2 модулі 8GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x4 Data Width + On-Board Broadcom 5720 2x Dual Port 1GBE + Qlogic QME2572 8Gbps Fibre Channel I/O Mezz Card for M-Series Blades (сервер PACS).

На наведених серверах встановлене таке ліцензійне базове ПЗ:

- Microsoft Windows Server Standard 2012 R2;
- Microsoft SQL-Server Standard 2012;
- сервер підключень тонких клієнтів SysElegance Application Server,

та серверна частина ПЗ АМІС;

- підсистема створення резервних копій і відновлення даних (окремий сервер, змонтований в окремій стандартній шафі):

- сервер DELL PowerVault NX400 4x3TB 7.2K 3Y (2 процесори Intel Xeon 4C Processor Model E5-2403 80W 1.8GHz/1066MHz/10MB, 2 модулі 4GB (1x4GB, 1Rx4, 1.35V) PC3L-10600 CL9 ECC DDR3 1333MHz LP RDIMM, On-Board Dual Gigabit Network Adapter, операційна система Windows Storage Server 2012 Standard Edition OEM, 3TB 7.2K RPM Near-Line SAS 6Gbps 3.5in Hot-plug Hard Drive + RAID 5 for H710/H310 (3-8 HDDs) з пристроєм безперебійного живлення APC Smart-UPS 1500VA USB;

- підсистема захисту від вторгнення на серверні підсистеми та клієнтські автоматизовані робочі місця (АРМ):

- система комплексного антивірусного захисту ESET;
- інші засоби обмеження доступу, контролю прав доступу й реєстрації спроб несанкціонованого доступу, механізми виявлення сканування портів і захисту від різних типів мережових атак на сайт та інше ПЗ, що функціонувало в інституті до початку впровадження АМІС;

- інфраструктура ЛОМ (мережні пристрої та лінії зв'язку):

- комутаційні вузли, що існували в інституті, у складі шаф для комутаторів 12U, керованих комутаторів HP ProCurve Switch та пристроїв безперебійного живлення APC Back-UPS CS 500VA;

- персональні комп'ютери, принтери, сканери та інше обладнання для організації АРМ користувачів системи – медичних працівників:

- настільні комп'ютери на платформах x86 та x64 різних виробників, придбані інститутом у різний час, під управлінням операційних систем MS Windows 2000/XP/7/8 із пристроями безперебійного живлення APC Back-UPS CS 500VA;

- «тонкі» клієнти LuxS TC-117-AC;

- принтери для друку документів HP LaserJet P1606dn;

- пристрої друку штрих-кодів ZEBRA LP/TLP 2824;

- пристрої зчитування штрих-кодів Zebex Z-3100.

4.4.1. Рішення щодо взаємодії основних підсистем та забезпечення сумісності.

4.4.1.1. Підсистеми керування.

ПАК АМІС складається з комплексу підсистем керування на програмному та апаратному рівні, які забезпечують виконання наступних завдань:

- планування й керування доступом до мережних ресурсів, зокрема, до серверів керування мережею (що вже існувало в інституті) та серверів, що поставляються в складі ПАК АМІС, у тому числі для користувачів, які здійснюють доступ до мережі та ПАК за допомогою термінальних сесій;
- реєстрація й призначення прав доступу користувачам;
- організація роботи користувачів у рамках єдиного програмного комплексу;
- адміністрування та діагностика серверу БД;
- адміністрування та діагностика серверу програмних додатків та підключень;
- адміністрування та діагностика серверу додатків для роботи з діагностичним та лабораторним обладнанням, збереження даних про медичні цифрові файли (PACS);
- адміністрування та діагностика серверу термінальних підключень;
- адміністрування та діагностика систем збереження даних, основної та резервної;
- налаштування і контроль продуктивності серверів і мережі;
- адміністрування та діагностика ПЗ АМІС;
- надійне зберігання інформації, що виникає в процесі роботи ЛПЗ, а саме: медична, статистична, управлінська, персональні дані пацієнтів, медичні цифрові файли як результати досліджень та діагностики, тощо.

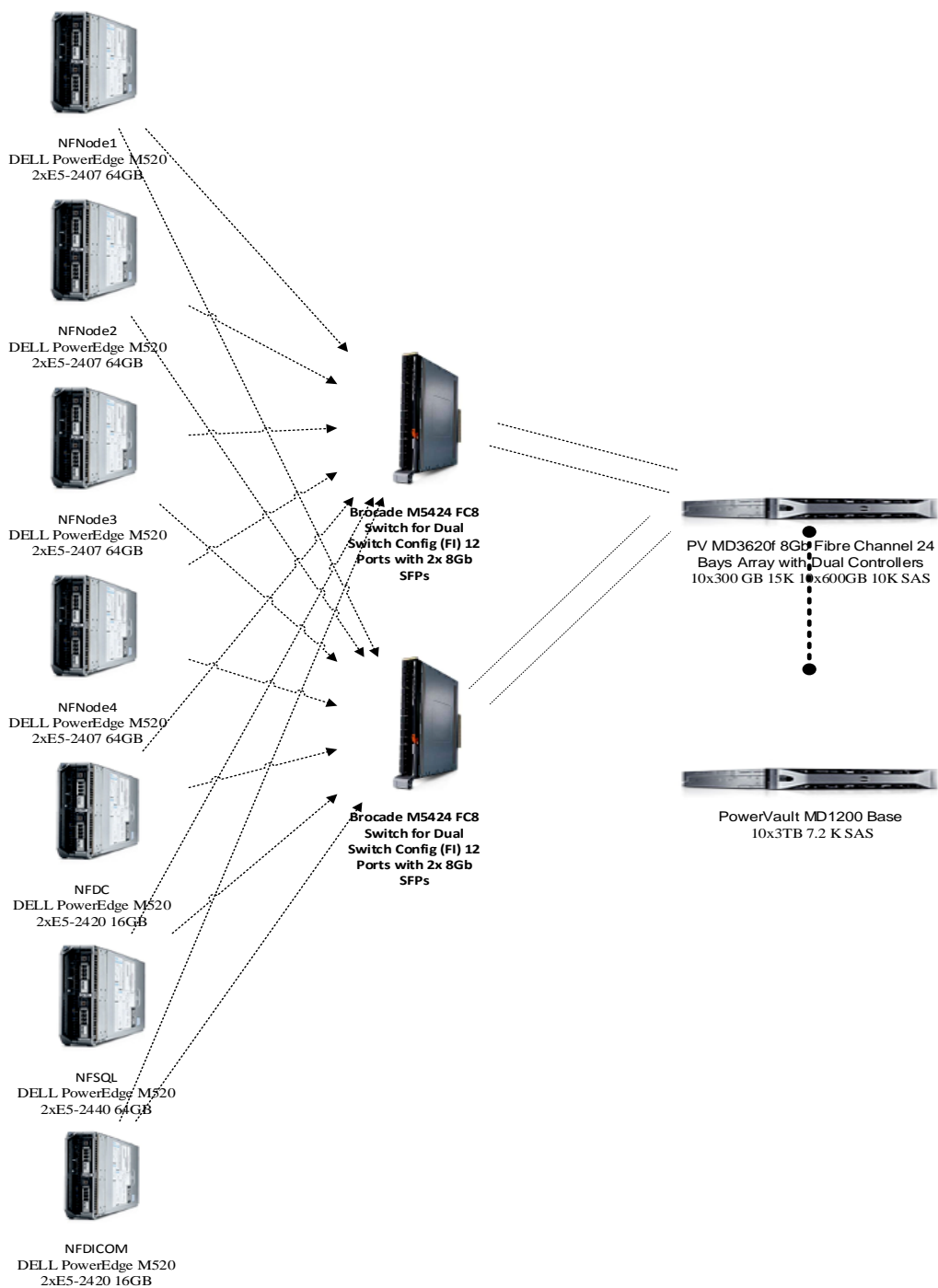
4.4.1.2. Взаємодія серверних підсистем. Взаємодія серверних підсистем схематично зображена на малюнку 3.

Далі наведене призначення кожного сервера, що входить до цієї підсистеми.

4.4.1.3. Сервер програмних додатків та підключень.

Сервер програмних додатків для внутрішніх клієнтів, клієнтів Інтранету (в т.ч. сервер WEB-додатків) забезпечує взаємозв'язок між програмними компонентами ПЗ АМІС й організовує роботу користувачів у рамках єдиного програмного комплексу, у т.ч. виконує наступні функції:

- одержання запитів і контроль вхідних даних Користувачів за допомогою серверних сценаріїв;
- реалізація бізнес-логіки обробки запитів за допомогою активних серверних об'єктів: сторінок ASPX, HTML, серверів COM+, елементів керування ActiveX та інше;
- передача запитів до СУБД (підсистеми обробки транзакцій);



Малюнок 3. Схема серверної підсистеми

- формування результатів запитів (наборів даних та вихідних WEB-сторінок із результатами запиту, що відправляються клієнту);
- здійснення кодування даних, що передаються до СУБД та декодування даних, що передаються до клієнтських АРМ;

- виконання функцій серверу лабораторних пристроїв;
- підтримання функцій резервного принт-серверу ПАК АМІС.

Сервер програмних додатків реалізований як окреме сервер-лезо в складі комплексної серверної підсистеми ПАК АМІС.

4.4.1.4. Сервер керування БД.

Сервер керування БД забезпечує реалізацію наступних завдань:

- оптимальна організація зберігання й обробки великих об'ємів інформації (медичної, управлінської та інше) – до 1 Тбайт;
- забезпечення паралельного доступу до даних при одночасній роботі до 500 користувачів (режим роботи багатьох користувачів);
- забезпечення цілісності й вірогідності збережених даних;
- виконання запитів користувачів з часом відповіді не більше ніж 3 хв.;
- керування виконанням операцій, як логічно завершеними блоками команд – транзакціями;
- створення резервних копій БД;
- оптимізація роботи сервера БД;
- управління дисковим простором і файлами БД;
- інтеграцію з іншими джерелами даних (експорт/імпорт даних з(в) суміжних(і) систем(и)).

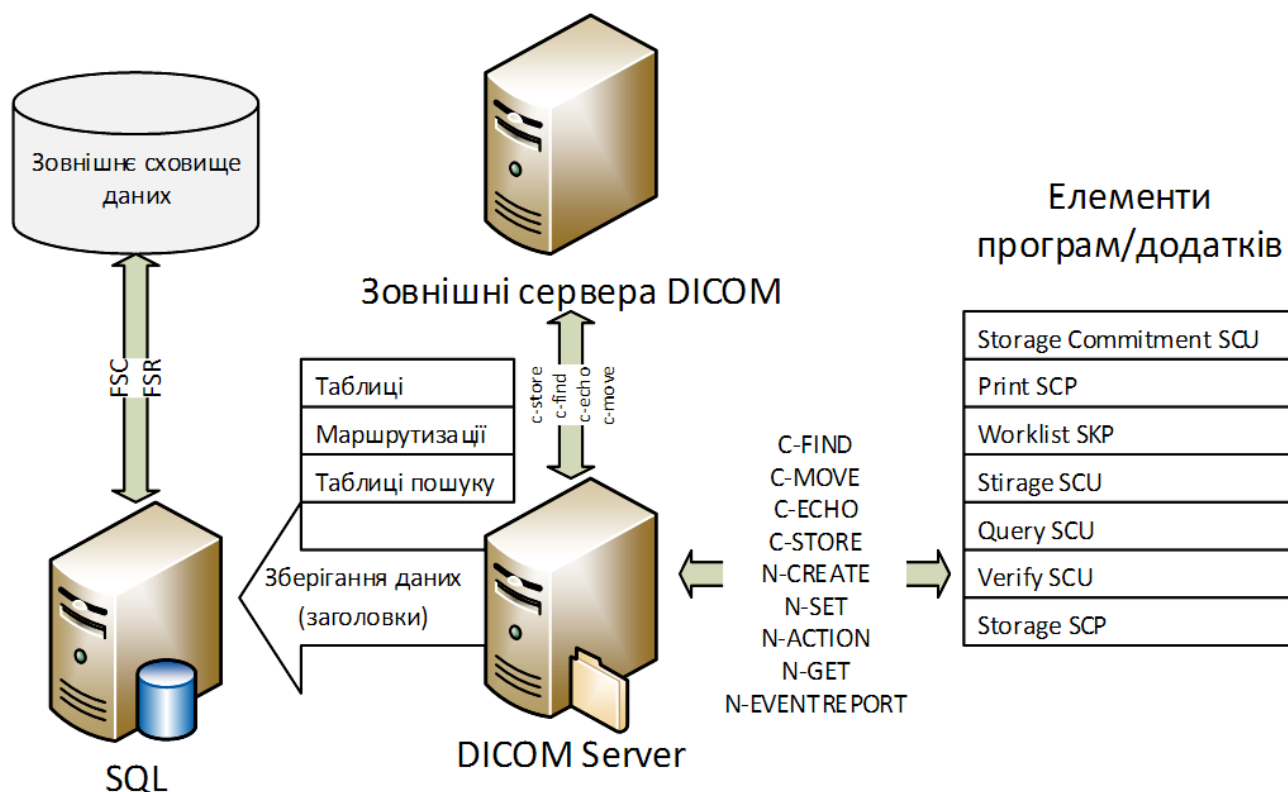
Для реалізації підсистеми зберігання даних використовується промислова СУБД MS SQL Server 2012. СУБД забезпечує реалізацію стандартних службових функцій при роботі з базами даних, а саме: раціональний спосіб зберігання інформації й організацію доступу до неї, забезпечення цілісності й несуперечності інформації, обслуговування спеціалізованих мов запитів до баз даних і ін.

АМІС у частині серверу БД протоколює всі події, пов'язані зі зміною свого інформаційного наповнення, і має можливість у випадку збою в роботі відновлювати свій стан, використовуючи раніше запротокольовані зміни даних.

Сервер керування БД реалізований як окреме сервер-лезо в складі комплексної серверної підсистеми АМІС.

4.4.1.5. Сервер керування обладнанням та PACS.

Основні завдання цього сервера схематично зображені на малюнку 4.



Малюнок 4. Принцип роботи сервера керування обладнанням та PACS.

Сервер керування обладнанням та PACS забезпечує реалізацію наступних завдань:

- організація одно- або двонаправленої керованої взаємодії між ПАК АМІС та діагностичним обладнанням, яке може працювати за протоколом DICOM3;
- організація одно- або двонаправленої керованої взаємодії між ПАК АМІС та лабораторним обладнанням, яке може працювати за протоколом ASTM1394;
- ведення бази даних про медичні цифрові файли, отримані з медичного обладнання, що підключене до ПАК АМІС;
- автоматизація процесу формування архівації, пошуку та доступу до медичних зображень;
- виконання функцій серверу DHCP;
- виконання функцій резервного серверу лабораторних пристроїв;
- організація роботи принт-серверу АМІС для друку документів та штрих-кодів (ця роль реалізована шляхом створення стандартного сервера друку Windows і включає оснащення консолі управління функціями друку, які використовуються для управління роботою всіх принтерів у системі. Сервер друку також допомагає стежити за чергами друку та отримувати повідомлення про припинення обробки ними завдань друку).

Сервер керування обладнанням та PACS реалізований як окреме сервер-лезо в складі комплексної серверної підсистеми ПАК АМІС.

4.4.1.6. Сервери термінального доступу до АМІС.

Сервери термінального доступу виконують наступні функції:

- організація термінальних сесій для АРМ, які побудовані за технологією «тонкий» (нульовий) клієнт із відсутнім жорстким диском та мережевим завантаженням операційної системи;
- організація доступу до АМІС у режимі RDP (remote desktop protocol) для АРМ, які побудовані на звичайних ПК (настільний комп'ютер або ноутбук);
- керування політиками, обмеженнями та профілями Користувачів, що підключаються до АМІС;
- надання доступу до мережевих програмних додатків, якими мають користуватися співробітники в процесі своєї діяльності в рамках АМІС;
- надання дискового простору в рамках виділеної адміністратором АМІС квоти для збереження робочих файлів у рамках її роботи та функціональності.

Для організації термінальних сеансів та доступу до АМІС у режимі remote desktop services нами використане програмне забезпечення для «тонких» клієнтів SysElegance Thinstation версії 4 на платформі Linux, яке забезпечує повну підтримку протоколу RDP, одночасне виконання додатків декількох користувачів на сервері, передачу графічної інформації на клієнтське робоче місце і дій користувача (клавіатура, миша) на сервер. Сервер додатків SysElegance Application Server версії 4 розташовано на кожному термінальному сервері. Сервер ліцензій SysElegance розташовано на сервері керування обладнанням.

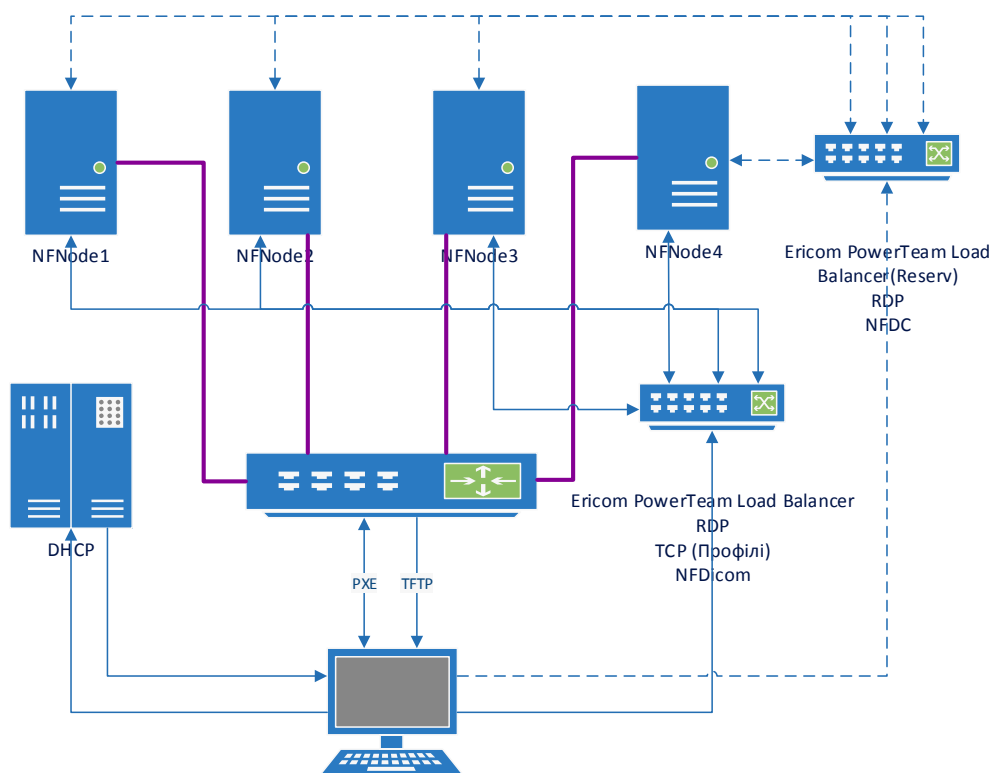
Сервери термінального доступу використовують стандартний протокол RDP та підтримують усі його властивості такі як кольори, перенаправлення буфера обміну, дисків, портів, звуку й смарт-карт та ін. Для сумісності термінального сервера додатків SysElegance з іншими службами та стандартними інструментами Microsoft (такими як, наприклад, Windows Server Administration Tools Pack) SysElegance Application Server встановлює свої служби віддалених робочих столів та допоміжної служби віддалених робочих столів замість аналогічних за функціональністю стандартних служб MS Windows.

Для завантаження «тонкими» клієнтами мережевої операційної системи SysElegance Thinstation на всіх термінальних серверах були встановлені штатні сервіси PXE та TFTP, а на інших серверах ЛОМ установлені основний та резервний сервери DHCP. Для розширення

можливостей автоматизованих робочих місць медичних працівників, обладнаних «тонкими» клієнтами, на термінальних серверах нами був інстальований офісний пакет MS Office 2012.

Для керування розподілом ресурсів при роботі декількох термінальних серверів ми використали дві технології: Network Load Balancing та PowerTeam Load Balancer (малюнок 5).

У процесі завантаження «тонкими» клієнтами мережевої операційної системи балансування мережевого навантаження термінальних серверів здійснюється штатним сервісом MS Windows Server 2012 R2 – Network Load Balancing. При під'єднанні терміналів до термінального серверу за протоколом RDP кожний клієнт з'єднується з найменш завантаженим сервером, за що відповідає ферма PowerTeam Load Balancer, до якої підключені всі термінальні сервери. Завантаження сервера визначається за кількома критеріями – завантаженням центрального процесора, вільною пам'яттю, кількістю активних сеансів. Також підтримується повторне підключення до відключеної сесії, раніше створеної користувачем на одному із термінальних серверів.



Малюнок 5. Схема балансування навантаження між термінальними серверами

Сервери термінального доступу реалізовані як окремі сервер-леза в складі

комплексної серверної підсистеми АМІС. Виходячи з кількості створених в інституті автоматизованих робочих місць медичного персоналу (350) нами було встановлено 4 термінальні сервери.

4.4.1.7. Підсистема збереження даних (ПСЗД).

ПСЗД виконує наступні функції:

- керування безперервним процесом доступу, читанню та модифікації до всіх даних, що використовуються в процесі роботи АМІС;
- збереження робочих та тимчасових файлів операційних систем, серверних програмних додатків та мережевих додатків, які використовуються в процесі роботи АМІС;
- збереження файлів БД, що використовується для роботи ПЗ АМІС;
- збереження файлів БД про місце зберігання медичних цифрових файлів, що використовується сервером PACS;
- збереження медичних цифрових файлів, які отримані в результаті діагностичних процедур із медичного діагностичного обладнання, що підключене до АМІС;
- збереженням профілів термінальних користувачів, файлів для організації термінальних сесій, та персональних файлів Користувачів АМІС у рамках установлених квот та функціональних обов'язків.

Інформація БД АМІС зберігається при виникненні аварійних ситуацій, пов'язаних зі збоями електроживлення в основній або резервній системах збереження даних.

Підсистема збереження даних розташована в серверній шафі та включає в себе дискові масиви DELL PowerVault MD3620f DC та DELL PowerVault MD1200. ПСЗД має власне джерело безперебійного електроживлення, що забезпечує її нормальне функціонування протягом 30 хвилин у випадку відсутності зовнішнього енергопостачання, і 5 хвилин додатково для коректного завершення всіх процесів (за умови повністю зарядженої батареї джерела безперебійного живлення, дотримання правил технічної експлуатації та мінімізації навантаження на систему). Забезпечено контроль за станом блоків безперебійного живлення з єдиного мережного центру управління та оперативного отримання через ЛОМ повідомлень про їх нештатні стани адміністраторами АМІС у режимі реального часу.

Резервне копіювання даних здійснюється на регулярній основі, в обсягах, достатніх для відновлення інформації в підсистемі зберігання даних (із можливістю зміни сценаріїв).

Нами використані наступні способи захисту даних при аваріях і заходи, що застосовуються при експлуатації АМІС:

- дублювання й резервування джерел і мереж електроживлення;
- дублювання й резервування даних, включаючи гаряче резервування;
- використання механізмів відкату транзакцій;
- використання схем контролю й відновлення цілісності даних;
- дублювання й резервування носіїв, накопичувачів даних, пристроїв зберігання даних та інтерфейсів до них;
- уніфікація методів і засобів зберігання даних;
- використання енергонезалежної пам'яті для зберігання даних;
- резервне копіювання даних із віддаленим зберіганням резервних копій і застосуванням схем ротації резервних копій і носіїв;
- впровадження й налагодження документованого процесу резервного копіювання й відновлення даних, включаючи процедуру ухвалення рішення на відновлення резервних копій;
- захист цілісності, доступності й конфіденційності резервних копій даних;
- забезпечення необхідної діагностики збоїв і відмов устаткування програмно-технічними засобами;
- забезпечення протоколювання подій при функціонуванні операційних систем та ПЗ АМІС.

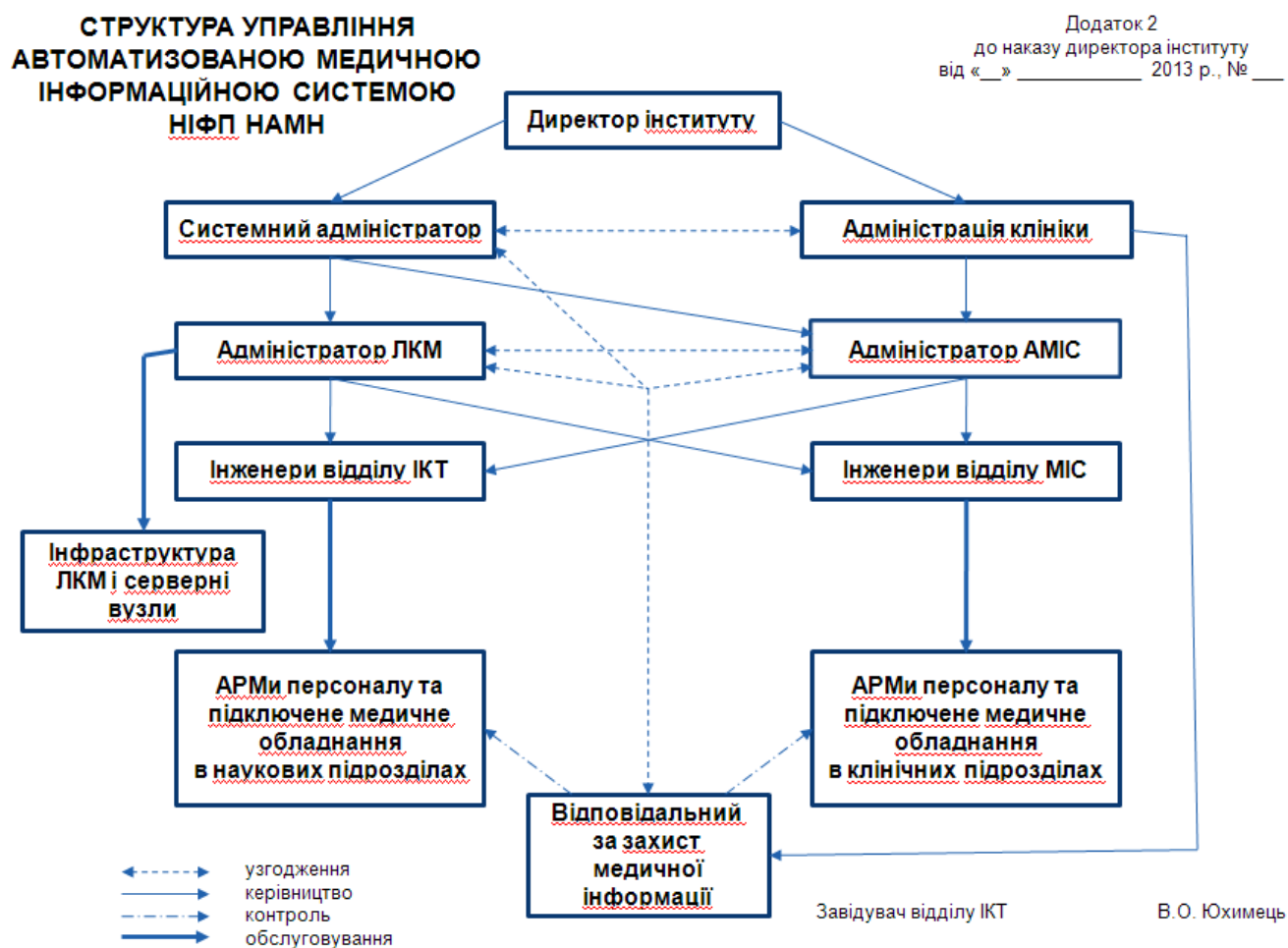
4.4.1.8. Підсистема архівування й відновлення БД.

Підсистема архівації й відновлення БД реалізована нами у вигляді окремого серверу, розташованого в іншому приміщенні, ніж ПСЗД, для виконання штатними сервісами MS Windows Server 2012 R2 та MS SQL Server 2012 таких функцій:

- керування безперервним процесом резервування БД;
- повне відновлення операційних системи серверів, додатків і БД при аварії на момент часу, що безпосередньо передував виникненню аварійної ситуації.

5. Структура управління АМІС наведена на малюнку 6. Загальне керівництво експлуатацією АМІС в інституті здійснює системний адміністратор, який має найвищі права адміністратора схеми Windows. Технічне забезпечення безперебійного функціонування інфраструктури АМІС забезпечують інженери відділу інформаційно-комп'ютерних технологій (ІКТ) під керівництвом адміністратора ЛОМ. Супроводження функціонування ПЗ АМІС та консультативну допомогу медичному персоналу, який її експлуатує, здійснює

адміністратор АМІС. Технічне забезпечення безперебійного функціонування АРМ медичного персоналу здійснюють інженери відділу медичних інформаційних систем (МІС). Системний адміністратор та адміністратор АМІС мають найвищі права адміністратора в ПЗ АМІС. Адміністратор ЛОМ має права адміністратора домену Windows та адміністратора сервера SQL.



Малюнок 6. Структура управління АМІС

Продовження статті читайте в наступній [ЧАСТИНІ 3](#).