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

АВТОМАТИЗОВАНА МЕДИЧНА ІНФОРМАЦІЙНА СИСТЕМА. ВПРОВАДЖЕННЯ ТА ОПТИМАЛЬНІ ТЕХНІЧНІ РІШЕННЯ

ЧАСТИНА 1

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

Досвід впровадження Автоматизованої медичної інформаційної системи (АМІС) у такому великому спеціалізованому науково-медичному закладі, яким є Національний інститут фтизіатрії і пульмонології ім. Ф.Г. Яновського (НІФП НАМН), що проводилось на протязі 2014-2016 рр. за рахунок бюджетного фінансування, дозволяє нам висловити свої міркування стосовно оптимальних технічних рішень цього складного процесу. Вони лягли в основу технічного проекту впровадження системи.

В 1-й частині статті викладені визначення АМІС, завдання, які вона вирішує, призначення та область її використання та основні застосовані технічні рішення, зокрема, архітектура та склад основних підсистем, логічна та функціональна архітектура системи, рішення щодо захисту інформації.

АМІС представляє собою програмно-апаратний комплекс як сукупність програмно-технічних засобів та баз даних, призначених для інформатизації закладів охорони здоров'я та автоматизації робочих місць і виробничих процесів, що здійснюються на етапах надання медичної допомоги пацієнтам в лікувально-профілактичному закладі (ЛПЗ). Найважливішими функціями АМІС є покращення показників надання медичної допомоги та створення умов для прийняття управлінських рішень.

Функціонально АМІС складається з 2-х взаємопов'язаних компонентів: апаратного та програмного. Апаратний компонент – це локальна комп'ютерна мережа у складі серверів, комутаційних вузлів, кабельних мереж, мережних робочих станцій, терміналів («тонких» клієнтів), друкуючих пристроїв, сканерів, а також програмних продуктів, що безпосередньо забезпечують їх функціонування. Програмний компонент – це спеціалізований програмний продукт (ПЗ АМІС), що працює на базі апаратного компоненту та забезпечує функціонування власне автоматизованої медичної інформаційної системи. Надалі ми будемо використовувати абревіатуру АМІС для позначення всього апаратно-програмного комплексу, а ПЗ АМІС – саме спеціалізованого програмного продукту. АМІС повинна забезпечити потреби медичного та

керуючого персоналу ЛПЗ в систематичній інформації з усіх аспектів діяльності закладу для прийняття рішень, що сприяють досягненню кінцевого результату – підвищенню якості надання медичної допомоги пацієнтам.

1. Завдання АМІС. Основними завданнями впровадження АМІС у ЛПЗ ми вважали наступні:

- вербальна взаємодія між лікарями та іншими учасниками лікувально-діагностичного процесу;
- накопичення, збереження, обробка й оперативна видача інформації про хід лікувально-діагностичного процесу;
- ретроспективний контроль та аналіз лікувально-діагностичного процесу;
- підвищення керованості ЛПЗ за рахунок зменшення рівня невизначеності під час формування та прийняття управлінських рішень;
- підвищення ефективності діяльності структурних підрозділів ЛПЗ при використанні ієрархічної системи збору, збереження, передачі і централізованої обробки інформації, що міститься в амбулаторній карті й історії хвороби, з оперативним доступом до інформації на робочих місцях (АРМ);
- підвищення ефективності праці медичного персоналу, усіх співробітників медичної установи за рахунок автоматизації трудомістких, рутинних операцій (підготовка численних виписок, довідок, звітів, дублювання результатів аналізів, тощо.),
- підвищення достовірності даних і оперативності інформаційного обслуговування;
- організація інформаційної взаємодії різних лікарів-фахівців із можливістю більш повного та оперативного забезпечення в наданні медичної допомоги на всіх етапах обслуговування пацієнта (профілактичного, діагностичного, диспансерного, стаціонарного, реабілітаційного);
- підвищення якості діагностики та лікування за рахунок використання експертної підтримки ухвалення рішення лікарями із впровадженням експертної оцінки їх роботи;
- проведення порівняльної оцінки ефективності різних методів лікування на основі накопиченої бази даних;
- аналіз вартості, контроль повноти та якості діагностичних та лікувальних заходів;
- раціоналізація використання медичних ресурсів (персоналу, обладнання, ліків, розхідних матеріалів тощо);
- надання співробітникам необхідної довідкової інформації з основних видів

медичної допомоги з використанням мережі Інтернет.

- зменшення витрат на медичні послуги за відсутності зниження якості медичної допомоги;
- зменшення тривалості медичного обслуговування пацієнта за рахунок спрощення процедури введення інформації в електронну медичну карту (ЕМК);
- отримання лікарем повної інформації про пацієнта, що міститься в ЕМК, у зручній і наочній формі, а також довідкової інформації;
- підвищення кваліфікації персоналу за рахунок використання в роботі сучасних інформаційних технологій із простим та зручним доступом до єдиних електронних довідників і Баз Даних;
- збереження конфіденційності персональної інформації пацієнтів та захисту її від несанкціонованого доступу.
- постійне й надійне збереження інформації про пацієнтів із можливістю пошуку й перегляду всіх видів медичних карт, результатів аналізів, досліджень, консультацій, а також історій хвороб, що дозволить уникнути додаткових витрат на діагностичні дослідження;
- оперативне отримання інформації про завантаженість ресурсів ЛПЗ, спеціальних служб, персоналу й обладнання для гнучкого й ефективного керування роботою ЛПЗ;
- скорочення термінів створення і спрощення процедури ведення форм державної статистичної звітності, адміністрування страхових медичних випадків, звітів про роботу установи, тощо;
- зменшення термінів і спрощення процедури підготовки звітних матеріалів про роботу ЛПЗ.
- використання єдиних процедур підготовки даних щодо використання робочого часу персоналом ЛПЗ для наступного бухгалтерського обліку;
- автоматизація обліку матеріальних ресурсів ЛПЗ та, зокрема, лікарських засобів та товарів медичного та немедичного призначення.

2. Призначення АМІС. Виходячи з наведених завдань, АМІС призначена для комплексної автоматизації ЛПЗ і має здійснювати підтримку лікувально-діагностичних заходів, забезпечувати інформаційну підтримку роботи медичних працівників ЛПЗ, здійснювати підтримку бізнес-планування та оптимізації всіх виробничих процесів ЛПЗ та здійснювати інформаційну підтримку оцінки їх ефективності. АМІС, без погіршення заданих характеристик, має можливість адаптації до будь-яких змін у лікувально-діагностичному

процесі, методах управління, принципах обліку тощо, зокрема, організаційної структури ЛПЗ, системи кодування ЕМК, форм статистичної та іншої звітності і періодичності їх надання, кількісного та якісного складу діагностичного та іншого обладнання, формату, і структури файлів обміну даними із суміжними системами. Адаптація забезпечується за рахунок процедур адміністрування та конфігурування ПЗ АМІС, модифікації документальних та звітних форм.

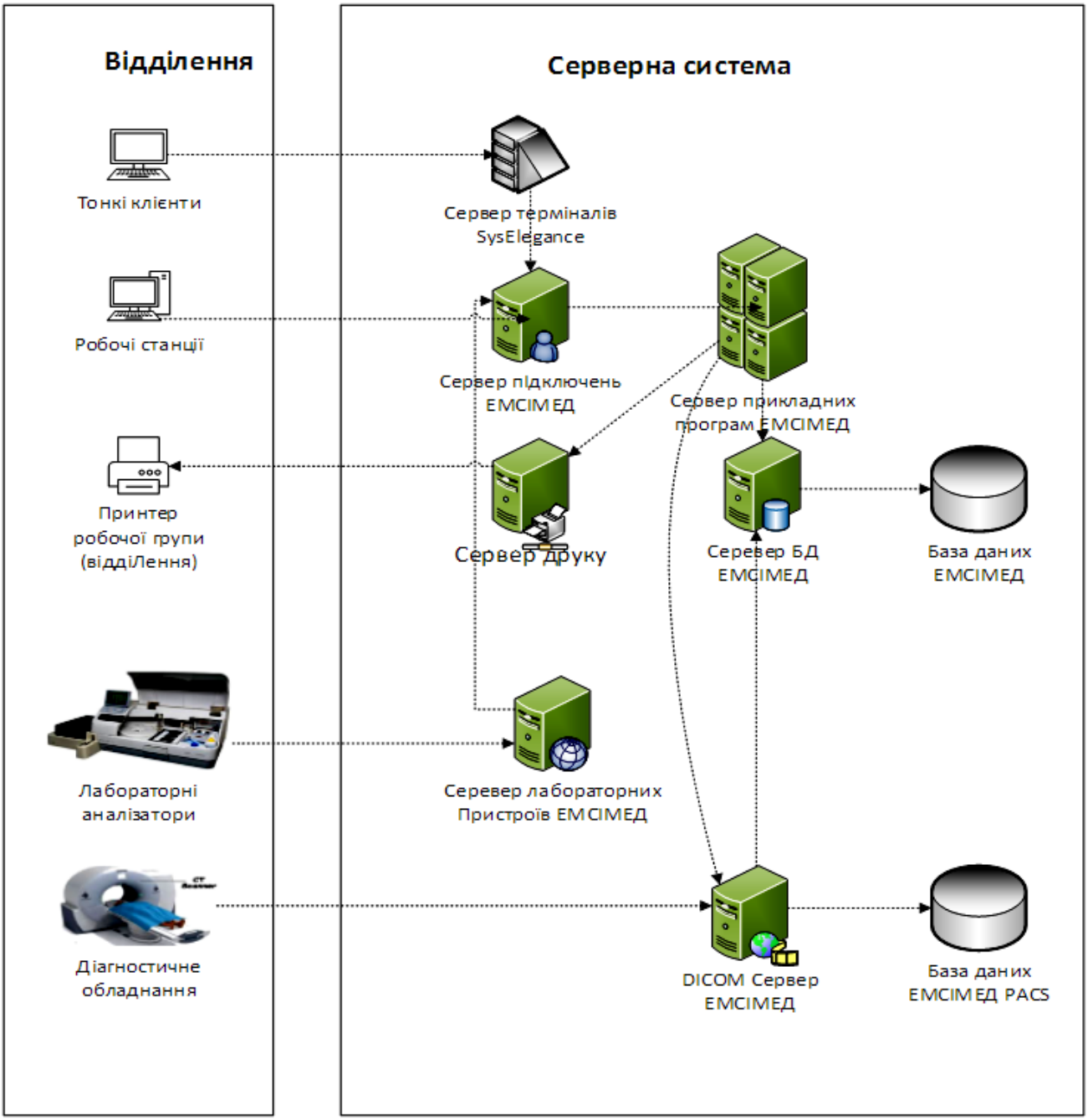
3. Область використання АМІС. АМІС використовується для зберігання всього необхідного набору даних, які можуть з'являтися в ЛПЗ у процесі надання медичної допомоги пацієнтам. Структура побудови масиву даних розробляється у відповідності до світових стандартів, що гарантує подальшу інтеграцію та двосторонню передачу даних до інших медичних Баз даних або реєстрів. АМІС має підтримувати автоматичний режим роботи з діагностичним та лабораторним медичним обладнанням, що відповідає міжнародним стандартам обміну та керування медичними даними DICOM3 та/або ASTM1394.

4. Основні технічні рішення. Далі наводяться основні технічні рішення, які були застосовані нами при впровадженні АМІС у НІФП НАМН, і на практиці довели свою життєздатність та практичну доцільність.

4.1. Архітектура та склад основних підсистем. Компонентна структура АМІС схематично зображена на малюнку 1. Вона побудована на принципі системи керування обробкою трансакцій. Така система характеризуються великою кількістю змін у Базі даних (БД). Зміни вводяться інтенсивно, великою кількістю користувачів. Довільне число користувачів може одночасно звертатися до тих самим даних, але тільки один із них має можливість змінювати їх у даний момент часу. Побудована система гарантує, що тільки один Користувач у кожний конкретний момент часу може змінити будь-які конкретні дані.

Зміни вноситься за допомогою механізму трансакцій. Трансакція являє собою набір змін, розглянутих, як єдине ціле. Якщо одна зі змін не може бути виконана, то й усі інші зміни, виконані в трансакції, будуть скасовані для збереження цілісності даних. Одночасно АМІС має елементи оперативної аналітичної обробки інформації, що накопичується та приймає рішення на основі її аналізу. АМІС працює на основі СУБД SQL і має архітектуру "клієнт-сервер". Єдина БД спільного використання міститься на відмово стійкій підсистемі обробки трансакцій і збереження даних, що включає сервер БД і дисковий масив із розщепленням дисків, що розташована в ЛПЗ, та забезпечує доступ до цієї БД з автоматизованих робочих місць (АРМ) користувачів, підключених до локальної мережі.

Користувачами AMIC є всі медичні працівники із числа уповноважених співробітників ЛПЗ, які працюють на автоматизованих робочих місцях (АРМ), що входять до складу AMIC. На АРМ користувачів установлене клієнтське ліцензійне програмне забезпечення для роботи з AMIC. AMIC підтримує роботу з різним типами АРМ користувачів, зокрема: настільний комп'ютер, ноутбук, «тонкий» клієнт, а також з різними шляхами організації робочих сеансів користувачів, зокрема: робота в звичайному та термінальному режимі, включаючи можливість роботи на без дискових АРМ.



Малюнок 1. Компонентна структура AMIC.

Засобами передачі інформації між клієнтом і сервером БД в АМІС є локально-обчислювальна мережа (ЛОМ) із пропускною спроможністю оптоволоконної магістралі 1 Гбіт/сек, що функціонує на основі стеку транспортних протоколів TCP/IP. Зв'язок із клієнтами забезпечується за допомогою ЛОМ та сервера програмних додатків. Доступ до БД забезпечується за допомогою сервера програмних додатків через спеціалізовані інтерфейси програмування доступу (ADO).

АМІС виключає безпосередній доступ клієнта до БД. Уся передана й отримана клієнтом інформація передається в зашифрованому вигляді. Алгоритм шифрування SSL (від 40 до 128 Біт) використовується у випадку встановлення серверу програмних додатків за допомогою транспортного тунелю через Kerberos. В АМІС можливий вхід тільки авторизованих клієнтів із наданням кожному клієнту відповідних регламентованих прав на перегляд певної інформації й виконання визначених операцій у системі.

Програмне забезпечення клієнта включає клієнтський модуль, що базується на графічному інтерфейсі (GUI). Усе інше програмне забезпечення, що включає правила та логіку обробки даних, зберігається на сервері програмних додатків і сервері БД.

Задачі сервера БД:

- керування інформаційною БД, з якою спільно працюють групи Користувачів;
- керування доступом до БД;
- захист інформації за допомогою засобів архівації/відновлення;
- централізоване завдання для всіх додатків обробки даних глобальної цілісності даних;
- забезпечення високої швидкості обробки запитів.

Задачі клієнтського модуля (клієнтської програми, що запускається користувачем на своєму АРМ):

- представлення інтерфейсу користувача;
- керування логікою додатка;
- виконання логіки додатка;
- перевірка допустимості даних;
- запит і отримання інформації про сервер БД.

4.2. Логічна та функціональна архітектура системи. В основі архітектури АМІС лежить багаторівнева схема прикладних програм баз даних. Сервер баз даних реалізований

на базі програмного забезпечення Microsoft (MS) SQL Server 2012 SE на сервері під управлінням операційної системи (ОС) MS Windows Server 2012 R2. Сама база зберігає дані системи, тригери, збережені процедури та SQL-запити, що забезпечують доступ до цих даних та їх цілісність. Виконання COM+ модулів системи на COM+ сервері під управлінням MS Windows Server забезпечує MS DTC-сервіс. Він також керує SQL-транзакціями. Архітектура системи представлена наступними COM + модулями:

- диспетчер SQL-запитів забезпечує доступ до запитів, які зберігаються в БД, викликає SQL-сервер для їх виконання та передає результати у вигляді ADO Recordset виклику модулю;
- прикладний сервіс виконує аутентифікацію користувача, підтримує сесію користувача nf авторизацію при доступі до ресурсів системи, а також викликає диспетчер SQL-запитів.

Сокет-сервер системи реалізований як Windows-сервіс. Здійснюючи підтримку з'єднання із клієнтом у мережевому середовищі TCP/IP, він забезпечує отримання запитів та передачу даних між прикладним сервісом AMIC та клієнтською частиною. Також сокет-сервер може серіалізувати або десеріалізувати дані у форматі XML або ADTG і зашифрувати/ дешифрувати трафік згідно проколу SSL.

На робочому місці співробітника ЛПЗ працює клієнтський модуль – частина ПЗ, та модуль оновлення версій. Клієнтський модуль AMIC забезпечує користувача можливістю виконання всіх операцій щодо введення даних у систему, їх первісної перевірки на допустимість і несуперечливість, передачі їх на сервер, а також отримання інформації із сервера БД та її представлення в зручному для перегляду та аналізу вигляді.

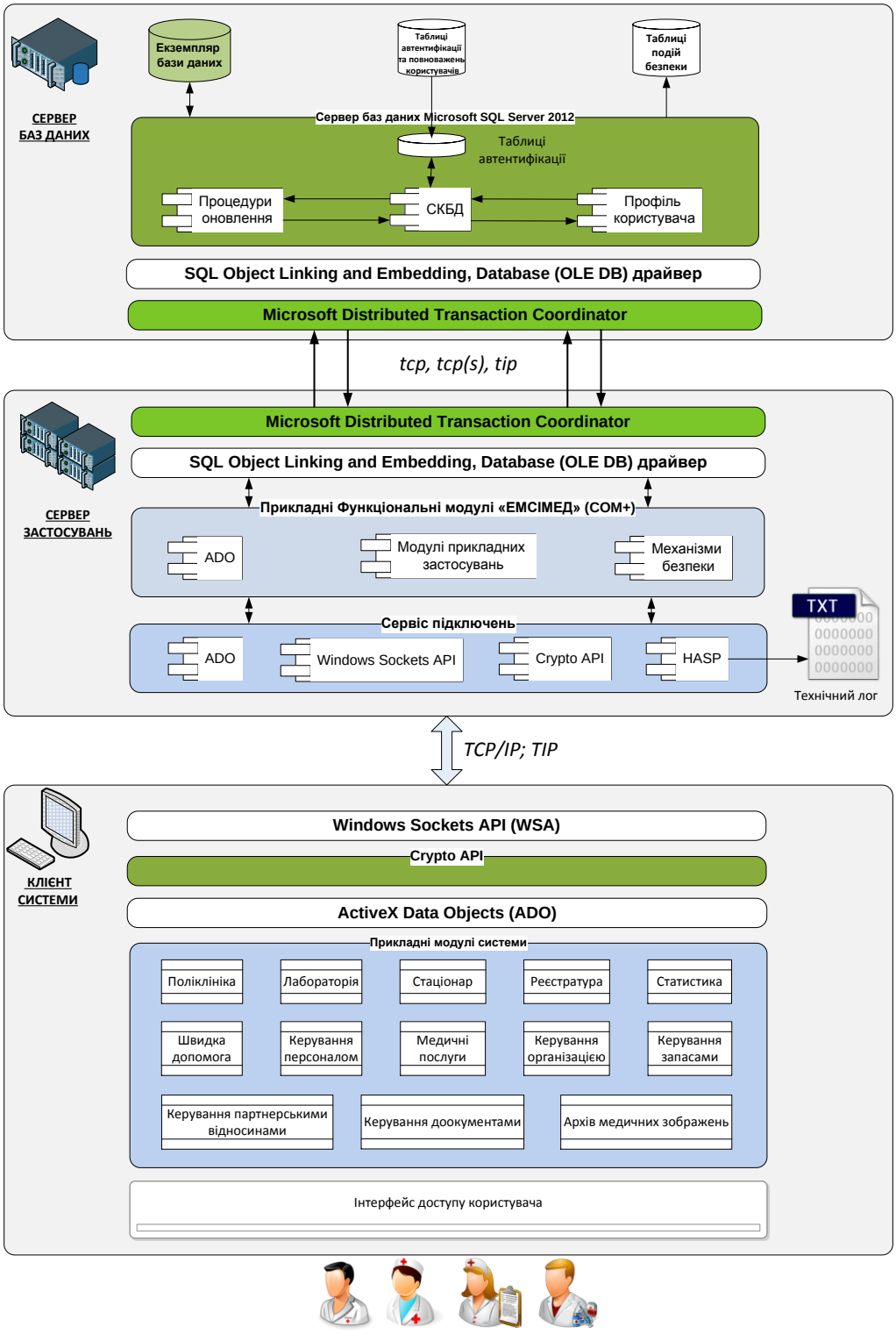
Підсистема з'єднання виконує: підтримку з'єднання (в тому числі віддаленого) із сервером з'єднань AMIC, серіалізацію/десеріалізацію даних, шифрування/дешифрування трафіку, примусове управління клієнтськими SQL-транзакціями.

На сервері даних DICOM (сервері PACS) зберігається база даних DICOM (за винятком зображень) і працює MS SQL сервер. Прикладний сервіс DICOM реалізований як Windows-сервіс, який виконує запити до БД DICOM та здійснює доступ до сховища зображень, розташованого на тому ж комп'ютері або реалізованого як мережевий ресурс. Клієнтський модуль взаємодіє безпосередньо з DICOM-сервером.

Бізнес-логіка системи розподілена на декілька рівнів та оптимізована з погляду мінімізації трафіку між клієнтськими модулями та сервером підключень. Основна її частина

реалізована у вигляді тригерів, збережених процедур і SQL-запитів, які виконуються на SQL-сервері.

Архітектура AMIC розподіляється на 3 рівні (малюнок 2):



Малюнок 2. Архітектура системи.

- клієнтський (рівень презентації). Призначений для відображення бізнес-контенту. На робочому місці користувача системи працює клієнтський модуль і модуль оновлення версій. Клієнтський модуль забезпечує можливість виконання всіх операцій по введенню даних у систему, їх первісній перевірці на допустимість і несуперечність, передачу їх на сервер, а також отримання інформації із сервера даних та її подання в зручному для перегляду та аналізу вигляді;

- рівень застосувань (бізнес-логіки). Складається із сервісу підключень (сокет-серверу) та прикладних функціональних додатків AMIC, розгорнутих на COM+. Сокет-сервер системи реалізований як Windows-сервіс і забезпечує отримання запитів, передачу даних між прикладним сервісом AMIC та клієнтським модулем, моніторинг трафіку клієнтських з'єднань та ведення протоколу запитів. Бізнес-логіка системи представлена наступними COM+ модулями:

- диспетчер SQL-запитів забезпечує доступ до запитів, які зберігаються в БД, викликає SQL-сервер для їх виконання та передає результати у вигляді ADO Recordset викликаному модулю;
- прикладний сервіс AMIC, що виконує автентифікацію користувача, підтримує сесію користувача і авторизацію при доступі до ресурсів системи, а також викликає диспетчер SQL-запитів;

- рівень бази даних. Даний рівень представлений у вигляді багаторівневої схеми прикладних програм баз даних. Сама база зберігає дані системи, тригери, збережені процедури і SQL-запити, що забезпечують доступ до цих даних та їх цілісність. Виконання COM+ модулів системи забезпечується MS DTC-сервісом, до функцій якого входить керування SQL-транзакціями.

ПЗ AMIC інтегрує в собі прикладний сервер Windows Server Application Role, систему керування базами даних Microsoft SQL Server 2012 R2, функціональні модулі ПЗ AMIC, що інсталюються в системі по одинці, та додаткові компоненти. Клієнтський модуль AMIC інсталюється окремо на АРМ користувача системи та термінальні сервери. Прикладний сервер Windows Server Application Role складається з Windows Sockets API, Crypto API та серверних процесів для виконання COM-програм. Доступ серверу до COM-даних у базі даних виконується через OLE DB та MS DTC, які надають єдиний інтерфейс для імпорту програмних пакетів. Система керування базами даних Microsoft SQL Server 2012 складається

з диспетчеру, модуля керування потоками Workflow та інтерфейсу адміністрування СКБД SQL Server Management Studio. Прикладні функціональні модулі ПЗ АМІС складаються з розроблених на базі ADO серверних COM-додатків відповідно до необхідних задач, які виконуються. Клієнтські COM-додатки, які встановлюються на клієнтській стороні під керуванням ОС Windows, реалізують функціональний інтерфейс доступу користувача відповідно до свого призначення;

Додаткові компоненти призначені для здійснення внутрішніх та зовнішніх з'єднань прикладних серверів.

4.3. Рішення щодо захисту інформації. Захист інформації в АМІС є багаторівневим і забезпечується як стандартними засобами серверної операційної системи, так і засобами ПЗ АМІС та антивірусного захисту.

4.3.1. Захист на рівні операційної системи із застосуванням Active Directory. На момент початку впровадження АМІС в інституті вже існувала ЛОМ з доменними принципами керування мережею, що включала:

- єдине сховище об'єктів керування, до яких відносяться користувачі, комп'ютери, сервери, принтери, інформація служби доменених імен, тощо;
- гнучке керування об'єктами, а саме: створення, редагування, видалення, встановлення політик безпеки користувачів і робочих станцій, керування правами доступу, аудит доступу до об'єктів;
- централізоване керування усіма об'єктами з одного робочого місця;
- гнучке визначення політик безпеки, прав та параметрів робочого місця для користувачів, що використовують облікові записи в службі каталогів, у відповідності з правилами групових політик;
- групування об'єктів керування служби каталогів у відповідності з місцем знаходження, організаційною структурою об'єкту тощо, з можливістю часткового делегування прав для адміністрування виділеної групи об'єктів;
- єдина аутентифікація та авторизації користувачів в службі каталогів;
- надання авторизованим користувачам відповідних прав доступу згідно групових політик до прикладних підсистем уніфікованих комунікацій та інфраструктурних систем.

4.3.2. Захист на рівні ПЗ АМІС:

- створення списку користувачів відповідно до штатного розкладу;
- визначення переліку груп користувачів та присвоєння функцій до окремих груп;

- додавання користувачів до груп у відповідності до повноважень;
- визначення переліку профілів лікарів для доступу до форм первинної документації;
- розподіл доступу користувачів до окремих звітів;
- вся інформація між робочим місцем користувача та сервером прикладних програм передається із допомогою захищеного транспортного протоколу із шифруванням за допомогою ключів HASP;
- використання сеансних ключів.

4.3.3. Архітектура засобів захисту від несанкціонованого доступу. Засоби захисту є сукупністю функцій в складі наступних компонентів:

- серверної операційної системи Windows Server 2012 R2;
- клієнтської операційної системи Microsoft Windows 2000/XP/7/8;
- серверу застосувань Windows Server Application Role;
- серверу баз даних Microsoft SQL Server 2012;
- прикладних функціональних модулів АМІС.

Компоненти засобів захисту системи АМІС призначені для реалізації функцій захисту інформації, яка обробляється засобами АМІС від несанкціонованого доступу.

На рівні внутрішніх прикладних застосувань засоби захисту забезпечують:

1) ідентифікацію та автентифікацію користувачів за групами безпеки та функціональними ролями в рамках АМІС;

2) авторизацію повноважень користувачів та процесів в рамках їх транзакцій при спробах доступу до робочих, серверних та технологічних процесів та об’єктів БД;

3) протоколювання та аудит подій в системі;

4) рахист власних компонентів від несанкціонованої модифікації, блокування та відмов;

5) доступність робочих, серверних та технологічних процесів АМІС в рамках транзакцій користувачів;

6) криптографічний захист інформаційного трафіку між сокет-сервером АМІС і клієнтським модулем..

Сервер застосувань – це компонент АМІС, призначений для управління додатками, що розробляються на платформі COM+. Він складається з сервісу підключень AMIC Socket Server та робочих процесів, що виконують COM-програми. Доступ серверу до даних у базі даних здійснюється за OLE DB-схемою та MS DTS. Інструмент ADO надає середовище

розробки для програмування на мові COM.

У той час, як сервер застосувань AMIC забезпечує повний контроль над внутрішніми додатками, його функції служать тільки базисними функціями для використання додатків, керованих клієнтом. Тому в рамках даного документу розглядаються лише функції безпеки, що забезпечуються ядром системи забезпечення фундаментальної політики безпеки і деяких служб безпеки, які будуть використовуватися у внутрішніх додатках AMIC.

Основне призначення засобів захисту:

- захист COM-додатків, до яких реалізується доступ засобам серверу додатків;
- забезпечення аудиту;
- керування користувачами та авторизацією;
- ідентифікація та автентифікація користувачів;
- керування та інтеграція COM-процесів;
- керування захистом.

Сервер баз даних Microsoft SQL Server 2012 – це компонент AMIC, призначений для зберігання інформації з COM-додатків, таблиць автентифікації та повноважень користувача, таблиць подій безпеки. Засоби захисту Microsoft SQL Server 2012 представляють собою набір механізмів безпеки щодо забезпечення конфіденційності, цілісності та доступності інформації, яка зберігається та обробляється у базах даних, а також спостережність (керованість) SQL Server 2012 в цілому.

Є три категорії прав на рівні бази даних. Це право на адміністрування (DBA), право на управління ресурсами (RESOURCE), право на доступ (CONNECT). Деякі користувачі можуть взагалі не мати будь-яких прав, пов’язаних з конкретною базою даних:

1. Користувач, який має право на доступ (CONNECT), має можливість отримувати і модифікувати дані в базі. Він може модифікувати ті об’єкти, якими володіє.

2. Користувач, який має право на управління ресурсами (RESOURCE), на додаток до тих прав, які мають користувачі з правом на доступ, може створювати нові об’єкти.

3. Користувач, який має право на адміністрування бази даних (DBA) на додаток до тих прав, які мають користувачі з правом на управління ресурсами, має наступні можливості: видаляти базу даних та будь-які об’єкти незалежно від того, хто ними володіє; роздавати і змінювати права доступу інших користувачів до бази даних в цілому і до окремих об’єктів.

Захист даних в Microsoft SQL Server 2012 базується на привілеях (дозволених діях), які надаються користувачам (або групам користувачів), які мають ідентифікатори на

конкретні об’єкти бази даних (наприклад, таблиці).

Контроль за доступом до інформації здійснює сервер бази даних. Користувач не має доступу безпосередньо до файлів БД. Він не знає, як і де зберігаються ці файли. При виконанні запиту користувача сервер отримує його від сервера застосувань AMIC, визначає ім’я користувача, і за внутрішньою інформацією визначає, чи може ця особа виконати цей запит. Якщо таке право є, то сервер виконує обробку запиту, якщо ні – користувачу надсилається повідомлення про помилку.

Призначення засобів захисту в структурі Microsoft SQL Server 2012:

- захист таблиць даних, до яких реалізується доступ з боку сервера застосувань AMIC;
- забезпечення аудиту;
- керування захистом;
- зберігання особистих даних пацієнтів в БД в зашифрованому вигляді.

Прикладні функціональні модулі ПЗ AMIC – це компоненти системи, розроблені на COM-платформі серверу застосувань відповідно до необхідних задач (Поліклініка, Лабораторія, Стаціонар, Реєстратура, Статистика, Керування персоналом, Медичні послуги, Керування організацією, Керування запасами, Керування партнерськими відносинами, Керування документами, Архів медичних зображень, Адміністрування, Scientific) які реалізують функціональний інтерфейс доступу користувача відповідно до свого призначення.

Призначення засобів захисту в структурі прикладних функціональних модулів ПЗ AMIC:

- захист прикладних модулів, до яких реалізується доступ з боку сервера застосувань AMIC;
- забезпечення аудиту;
- резервування на архівування даних;
- керування захистом.

4.3.4. Зовнішні інтерфейси засобів захисту. Для кожного із зовні видимих інтерфейсів описані наступні пункти:

- тип інтерфейсу (відношення до функцій захисту);
- протокол/метод використання (наприклад, мережевий протокол, транзакція, запит);
- цільова функція інтерфейсу.

У таблицях 1-4 відображено інтерфейси визначених вище компонентів:

1) зовнішні інтерфейси рівня презентації;
2) зовнішні інтерфейси сервісу підключення;
3) зовнішні інтерфейси COM+ виконань;
4) зовнішні інтерфейси рівня баз даних.

Таблиця 1. Зовнішні інтерфейси засобів захистуAMIC (рівень презентації)

Назва інтерфейсу	**Протокол/Метод використання**	**Цільова функція**
Windows Sockets API	TCP/IP	Підключення обладнання Логіка перевірки вводу
Crypto API	Security Support Provider Interface	Шифрування трафіку
ADO	ActiveX COM+	Презентація даних

Таблиця 2. Зовнішні інтерфейси засобів захистуAMIC (сервіс підключень)

Назва інтерфейсу	**Протокол/Метод використання**	**Цільова функція**
Windows Sockets API	TCP/IP	Підтримка сесій клієнта
Crypto API	Security Support Provider Interf ace	Шифрування трафіку
ADO	ActiveX COM+	Стиснення трафіку
HASP	IPX TCP/IP NetBIOS	Контроль ліцензій MCMed

Таблиця 3. Зовнішні інтерфейси засобів захистуAMIC (COM+ виконання)

Назва інтерфейсу	**Протокол/Метод використання**	**Цільова функція**
ADO	ActiveX COM+	Бізнес логіка
SQL OLE DB	Microsoft Data Access Components	Автентифікація користувача (login) Перевірка прав доступу користувача (авторизація)
MS DTC	Transaction Internet Protocol	Керування транзакціями Протоколювання операцій

Таблиця 4. Зовнішні інтерфейси засобів захистуAMIC (рівень бази даних)

Назва інтерфейсу	Протокол/Метод використання	Цільова функція
MS DTC	Transaction Internet Protocol	Управління розподіленими транзакціями
SQL OLE DB	Microsoft Data Access Components	Уніфікований доступ до сховища даних

4.3.5. Засоби захисту прикладних застосувань:

ActiveX Data Objects

Призначення модулю і опис взаємодії з іншими модулями	Інтерфейс програмування додатків для доступу до даних, розроблений компанією Microsoft (MS Access, MS SQL Server) та оснований на технології компонентів ActiveX. ADO дозволяє представляти дані з різноманітних джерел (реляційних баз даних, текстових файлів, тощо) в об'єктно-орієнтованому вигляді.
Тип	Модуль не реалізовує функції безпеки, а лише надає допомогу в транспортуванні даних до функцій безпеки.

Windows Sockets API

Призначення модулю і опис взаємодії з іншими модулями	WSA представляє собою технічну специфікацію, яка визначає, як мережеве програмне забезпечення Windows буде отримувати доступ до мережевих сервісів, в том числі, TCP/IP. API визначає стандартний інтерфейс між клієнтським додатком та зовнішнім стеком протоколів TCP/IP.
Тип	Модуль не реалізовує функції безпеки, а лише надає допомогу в транспортуванні даних до функцій безпеки.

Crypto API

Призначення модулю і опис взаємодії з іншими модулями	Інтерфейс програмування додатків, який забезпечує Windows-додатки стандартним набором функцій для роботи з криптопровайдером. CryptoAPI підтримує роботу с асиметричними и симетричними ключами, а також працювати з електронними сертифікатами. Набор підтримуваних криптографічних алгоритмів залежить от конкретного криптопровайдера. Інтерфейс Crypto API розділений на 5 функціональних груп: 1. Базові криптографічні функції: • функції шифрування / розшифрування даних; • функції хешування і отримання цифрового підпису даних; • функції ініціалізації криптопровайдера та роботи з

	отриманим контекстом; • функції генерації ключів; • функції обміну ключами. 2. Функції кодування/декодування. 3. Функції роботи з сертифікатами. 4. Багаторівневі функції обробки криптографічних повідомлень. 5. Низькорівневі функції обробки криптографічних повідомлень.
Тип	Реалізація функцій безпеки: • «керування ресурсами (об'єктами захисту)»

HASP

Призначення модулю і опис взаємодії з іншими модулями	Апаратно-програмна система, призначена для захисту програм і даних від нелегального використання, піратського тиражування, несанкціонованого доступу до даних, а також для автентифікації користувачів при доступі до захищених ресурсів. Основою ключів HASP є спеціалізована мікросхема ASIC (Application Specific Integrated Circuit), яка має унікальний для кожного ключа алгоритм роботи. Принцип захисту полягає в том, що в процесі виконання захищена програма запитує підключений до комп'ютера ключ HASP. Якщо HASP повертає правильну відповідь і працює по заданому алгоритму, програма виконується нормально. В зворотному випадку, вона може завершитись, переключитись в демонстративний режим або заблокувати доступ до окремих функцій програми.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «ідентифікація та автентифікація»; • «керування ресурсами (об'єктами захисту)»; • «забезпечення аудиту»

SQL OLE DB

Призначення модулю і опис взаємодії з іншими модулями	Набір програмних COM-інтерфейсів, призначений для доступу до різних джерел даних, таких як реляційні та нереляційні дані, текстові та графічні дані, архіві електронних повідомлень, файлова система та бізнес-об'єкти. Складається з наступних компонентів: споживачі (consumers), провайдери даних (data providers) та сервісні компоненти (service components). Будь-який компонент ПЗ, що застосовує інтерфейси OLE DB, є споживачем. Споживачі можуть звертатись до даних через

	ActiveX Data Objects, який представляє собою високорівневий інтерфейс до OLE DB. Провайдер даних – це компонент ПЗ, що виконує маніпуляції з даними. Провайдер даних виконує наступні функції: 1. отримання от споживача запитів на отримання або модифікацію даних; 2. отримання даних з БД або їх модифікація в БД; 3. повернення даних споживачу. Провайдер сервісів реалізує розширений функціонал, не підтримуваний звичайними провайдерами даних, наприклад сортування та фільтрацію даних, обробку транзакцій і SQL-запитів, тощо. Сервісний компонент може звертатись до сховища даних безпосередньо або за допомогою відповідного провайдера даних.
Тип	Модуль не реалізовує функції безпеки, а лише надає допомогу в транспортуванні даних до функцій безпеки.

MS DTC

Призначення модулю і опис взаємодії з іншими модулями	Координатор розподілених транзакцій – складова частина служб компонентів Windows Component Services. В Component Services також включена технологія COM+. COM+ використовується при необхідності нетранзакційної передачі повідомлень, а MS DTC – при необхідності транзакційної передачі. Служба виконує складні процедури взаємодії та перевірки помилок з метою забезпечення необхідної послідовності виконання операцій.
Тип	Модуль не реалізовує функції безпеки, а лише надає допомогу в транспортуванні даних до функцій безпеки.

COM+

Призначення модулю і опис взаємодії з іншими модулями	Стандарт створення ПЗ на основі взаємодіючих компонентів, кожен з яких може використовуватись в багатьох програмах одночасно. Слугує основою для OLE, ActiveX-об'єктів та елементів управління ActiveX. COM+ надає засоби безпеки, які використовуються для захисту COM-додатків. COM+ дозволяє керувати захистом як за допомогою атрибутів Component Services, так і програмно, викликаючи в коді спеціальні API-функції. Механізми безпеки COM+ включають: • декларативна рольова безпека; • програмна рольова безпека; • служби автентифікації; • делегування прав.

	Рольова безпека є основним засобом безпеки додатків COM+. Використовуючи ролі, можливо автоматично створювати політику авторизації, вказуючи кому які ресурси будуть доступні. Рольову безпеку можна застосовувати програмно, якщо додаток потребує більш детального контролю доступу.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «ідентифікація та автентифікація»; • «керування користувачами та їх авторизацією»

SQL Server Management Studio

Призначення модулю і опис взаємодії з іншими модулями	Компонент СКБД SQL Server 2012, призначений для доступу, налаштування, управління та адміністрування всіма компонентами Microsoft SQL Server 2012. Призначене для розробки та адміністрування об'єктів баз даних та налаштування відповідних об'єктів служб Analysis Services. Дозволяє виконувати налаштування політики ідентифікації для групи користувачів та політики безпеки для всіх компонентів Microsoft SQL Server 2012.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «ідентифікація та автентифікація»

SQL Server Logon

Призначення модулю і опис взаємодії з іншими модулями	Вбудований в СКБД графічний інтерфейс введення облікових даних адміністратора. Для процедури авторизації взаємодіє з SQL Server Authentication Service.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «ідентифікація та автентифікація»

Transact SQL

Призначення модулю і опис взаємодії з іншими модулями	Транзакції до бази даних, призначені для роботи з користувачами та групами. Дозволяє створювати нових користувачів та групи, визначаючи для кожної з них політику безпеки. Для кожного користувача налаштовується доступ до відповідних об'єктів захисту та порядок виконання операцій з ними.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку

	КЗЗ): • «ідентифікація та автентифікація»; • «керування користувачами та авторизацією»

СКБД Logfile

Призначення модулю і опис взаємодії з іншими модулями	Відстеження й протоколювання подій, що відбуваються в SQL Server 2012, здійснюється підсистемою аудиту. SQL Server 2012 дозволяє налаштувати автоматичний аудит подій. Підсистема аудиту надає можливість визначати конкретні події або групи подій, щодо яких потрібно проводити спостереження. Модуль аудиту має можливість визначити формат журналу реєстрації подій (SQL-таблиці, текстовий файл) та місце його зберігання.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «забезпечення аудиту»

Модуль авторизації СКБД

Призначення модулю і опис взаємодії з іншими модулями	Структурний компонент SQL Server Management Studio, який забезпечує застосування відповідних політик доступу до об’єктів захисту після проходження адміністратором процедури авторизації. В рамках підсистеми розмежування доступу взаємодіє з sys.credentials.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «ідентифікація та автентифікація»

sysadmin

Призначення модулю і опис взаємодії з іншими модулями	Роль системного адміністратора, яка автоматично створюється під час інсталяції компонентів СКБД Microsoft SQL Server 2012, та дозволяє здійснювати адміністрування SQL Server 2012 і перегляд журналів реєстрації подій. Системний адміністратор може змінювати права доступу до об’єктів лише під обліковим записом sysadmin.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «ідентифікація та автентифікація»; • «забезпечення аудиту»; • «керування користувачами та авторизацією»

dtexec

Призначення модулю і опис взаємодії з іншими модулями	Структурний компонент Integration Services, що здійснює контроль за роботою всіх модулів СКБД Microsoft SQL Server 2012 та використовується для віддаленого доступу до консолі керування. Для захисту від неавторизованих дій має можливість налаштувати посилену автенетифікацію (з використанням ЕЦП) та встановити пароль та виконання окремих дій (доступ до консолі, журналів реєстрації подій).
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «керування користувачами та авторизацією»

Database Engine (Захищені об'єкти та дозволи)

Призначення модулю і опис взаємодії з іншими модулями	Структурні компоненти служби Database Engine СКБД Microsoft SQL Server 2012, призначені для керування ресурсами бази даних. Дозволяють створювати захищені ресурси та визначати порядок доступу до них. Мають вбудовані механізми налаштування умов, під час яких буде здійснюватись блокування/розблокування ресурсів та контроль за їх виконанням.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «розмежування доступу до ресурсів»

Plug-In

Призначення модулю і опис взаємодії з іншими модулями	Модернізація структурних компонентів СКБД Microsoft SQL Server 2012 виконується шляхом інсталяції окремих плагінів та їх відповідне налаштування. Для цього в складі Microsoft SQL Server 2012 використовується компонент Slipstream, що забезпечує додавання нових плагінів та їх конфігурацію або видалення без зупинки роботи основних компонентів СКБД.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «модернізація компонентів»

Перегляд журналів аудиту

Призначення модулю і опис взаємодії з іншими модулями	Microsoft SQL Server 2012 надає засоби перегляду журналів аудиту. Для перегляду журналів аудиту за допомогою вбудованих в SQL Server 2012 засобів користувач повинен бути членом у визначеній ролі sysadmin рівня серверу.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «забезпечення аудиту»

SQL Server 2012 Data Recovery Tool

Призначення модулю і опис взаємодії з іншими модулями	У процесі функціонування Microsoft SQL Server 2012 можуть виникати наступні типи відмов, які призводять до переривання надання послуг: • неможливість запуску серверу; • сервер не відповідає на запити учасників. У випадку, якщо відмови пов'язані з пошкодженням компонентів SQL Server 2012 внаслідок відмов компонентів середовища функціонування (пошкодження компонентів ОС Windows, пошкодження носіїв даних), потребується повторна інсталяція SQL Server 2012. В інших випадках відмови можуть бути усунені без повторної інсталяції SQL Server 2012. Для цього Microsoft SQL Server 2012 надає користувачу, що є членом ролі sysadmin (SA), наступні інструменти: Використання служби резервного відновлення роботи SQL Server 2012 Data Recovery Tool, що дозволяє завантажити останню вдалу конфігурацію СКБД та відновити об'єкти БД з резервної копії.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «відновлення після збоїв»

SQL Server 2012 Native Client

Призначення модулю і опис взаємодії з іншими модулями	SQL Server 2012 Native Client представляє собою клієнтський додаток до СКБД Microsoft SQL Server 2012 та використовується як додатковий інтерфейс доступу системного адміністратора до консолі керування SQL Server 2012. SQL Server 2012 Native Client встановлюється в якості окремого ПЗ в ОС Windows та використовує механізми безпеки операційної системи. Для ідентифікації в системі взаємодіє з SQL Server Logon, а під час адміністрування може взаємодіями з іншими компонентами SQL Server 2012.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «ідентифікація та автентифікація»; • «керування користувачами та авторизацією»

SQL Server 2012 Server Audit

Призначення модулю і опис взаємодії з іншими	Server Audit представляє собою структурний компонент СКБД Microsoft SQL Server 2012, який відповідає за збір, зберігання та роботу з журналами реєстрації подій. Модуль здійснює накопичення подій, що надійшли від компонентів та служб

модулями	Microsoft SQL Server 2012, їх структурування та надійне збереження. Системний адміністратор має можливість формувати індивідуальні звіти або використовувати стандартні табличні звіти за допомогою служб Reporting Services.
Тип	Реалізація функцій безпеки (реалізує декларативну безпеку КЗЗ): • «забезпечення аудиту

4.3.6. Функціональний профіль захищеності АМІС.

АМІС, що була впроваджена в НІФП НАМН, отримала експертний висновок Державної служби спеціального зв'язку та захисту інформації на відповідність вимогам нормативних документів системи технічного захисту інформації в Україні з рівнем гарантій Г-2, та позитивний висновок Державного закладу "Медичний центр телемедицини МОЗ України".

Продовження статті читайте в наступній **ЧАСТИНІ 2**.