

АВТОМАТИЗОВАНА МЕДИЧНА ІНФОРМАЦІЙНА СИСТЕМА: ТЕХНІЧНІ ВИМОГИ ТА ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ В КЛІНІЦІ

В.О. Юхимець, В.В. Куц, О.Л. Мельник, О.С. Лісневич

ДУ «Національний інститут фтизіатрії і пульмонології ім. Ф.Г. Яновського НАМН України», Київ, Україна

РЕЗЮМЕ, ABSTRACT

В статті сформульовані мета, завдання та технічні вимоги до автоматизованої медичної інформаційної системи та деякі особливості її впровадження в лікувальному закладі з урахуванням вимог чинної нормативно-правової бази України

Ключові слова: автоматизована медична інформаційна система, технічні вимоги, автоматизація роботи лікувального закладу, впровадження

В статье сформулированы цель, задачи и технические требования к автоматизированной медицинской информационной системы и некоторые особенности ее внедрения в лечебном учреждении с учетом требований существующей нормативно-правовой базы Украины

Ключевые слова: автоматизированная медицинская информационная система, технические требования, автоматизация работы лечебного учреждения, внедрение

The article defines the purpose, objectives and technical requirements for automated medical information system and some features of its implementation in the hospital with the requirements of the existing legal framework of Ukraine

Key words: automated medical information system, technical requirements, automation of the hospital, implementation

На протязі 2012-2013 років відділом інформаційно-комп'ютерних технологій НІФП НАМН була проведена підготовча робота щодо впровадження в клініці інституту автоматизованої медичної інформаційної системи (далі – АМІС або система), що мала впроваджуватись на базі існуючої в нашому закладі локальної комп'ютерної мережі. АМІС ми розглядали як цілісний програмно-апаратний комплекс у складі серверних та комутаційних вузлів, мережного обладнання, терміналів медичного персоналу, периферійних пристроїв та спеціалізованих програмних компонентів. На основі вивчення досвіду російських колег, запозиченого з відкритих джерел, та чинної нормативно-правової бази України [1-19] нами були сформульовані технічні вимоги до цієї системи. Об'єктом впровадження мала бути інститутська клініка фтизіопульмонологічного профілю на 530 ліжок для надання пацієнтам спеціалізованої медичної допомоги 3-го рівня в складі консультативної поліклініки, 13-ти лікувальних та 4-х діагностичних відділень, у т.ч. рентгенологічного та ендоскопічного, 6-ти лабораторій та 2-х лікувальних кабінетів. Усього планувалось, на додаток до існуючих 85-ти, створити близько 230 нових автоматизованих робочих місць для медичного персоналу (АРМів) та під'єднати до системи понад 90 одиниць автоматизованого діагностичного обладнання.

Ми сподіваємось, що наша розробка може стати в пригоді іншим медичним закладам країни.

Мета впровадження АМІС – створення повністю цифрового робочого середовища медичного персоналу, забезпечення високої якості обслуговування пацієнтів, скорочення

кількості медичних помилок, підвищення ефективності та продуктивності роботи клініки та забезпечення лікарського персоналу потрібною інформацією для прийняття правильних рішень.

Завдання впровадження АМІС. Для досягнення поставленої мети при впровадженні АМІС ми планували вирішити наступні завдання:

- підвищити ефективність управління клінікою інституту;
- підвищити якість та оперативність прийняття рішень у процесі діагностики та лікування пацієнтів;
- підвищити якість та зменшити тривалість обслуговування пацієнтів;
- підвищити ефективність праці медичного персоналу;
- організувати оперативну інформаційну взаємодію лікарів-фахівців різних спеціальностей;
- підвищити ефективність наукової діяльності інституту;
- оптимізувати використання наявних кадрових та матеріальних ресурсів;
- сприяти підвищенню кваліфікації медичного персоналу;
- забезпечити збереження конфіденційності персональної інформації про пацієнтів та її захист від несанкціонованого доступу;
- зменшити терміни й спростити процедури підготовки звітних матеріалів за результатами роботи клініки.

Призначення АМІС. АМІС є засобом комплексної автоматизації лікувально-діагностичної та наукової діяльності інституту. Зокрема, впровадження АМІС ми планували спрямувати на автоматизацію наступних бізнес-процесів:

- управління організаційною структурою та персоналом, що передбачає набір адміністративних функцій для формування організаційної структури, штатного розкладу, руху працівників, складанню графіків роботи співробітників та здійснення контролю за його дотриманням;

- ведення електронної медичної карти (ЕМК) пацієнта, що включає амбулаторну карту пацієнта та медичну карту стаціонарного хворого з метою швидкого доступу до записів лікарів, результатів інструментальних та лабораторних досліджень, листів призначень тощо;

- організацію амбулаторного прийому пацієнтів, що передбачає ведення журналів прийому лікарями-консультантами, функції реєстрації, робочих місць лікарів консультативної поліклініки тощо;

- госпіталізацію, виписку та рух пацієнтів. Включає функції роботи приймального відділення з реєстрації пацієнтів, ведення журналів госпіталізації, оперативний облік ліжкового фонду відділень, управління чергою на госпіталізацією пацієнтів, заповнення медичних карт стаціонарного хворого, реєстрацію руху між відділеннями та всіх видів виписки пацієнтів;

- організацію діагностики та лікування пацієнтів у стаціонарі. Передбачає функції запису на консультації, лабораторні та діагностичні дослідження, формування листка призначень та температурного листка, відміток про виконані призначень, ведення журналів операційних втручань, графіку операцій, запису передопераційного, етапного та виписного епікризу та інших документів, що можуть включатись до медичної картки стаціонарного хворого;

- проведення діагностичних досліджень. Складання графіків завантаження діагностичного обладнання, ведення журналів, формування висновків, підключення

діагностичного обладнання до системи архівування медичних зображень, завантаження робочих листів до діагностичного обладнання тощо.

- проведення лабораторних досліджень. Формування направлень на лабораторні дослідження, проведення відбору та реєстрації біоматеріалу, проведення пробопідготовки, визначення робочих місць, підключення одно/двонаправлених аналізаторів, ведення архіву біоматеріалів, контроль якості, валідація результатів досліджень;

- облік лікарських засобів. Визначення місць зберігання лікарських засобів, ведення номенклатури лікарських засобів, витратних та перев'язувальних матеріалів, контроль терміну придатності, облік надходжень, переміщення між складами та відділеннями, списання, автоматичний облік витрачання, проведення інвентаризацій, замовлення лікарських засобів та експорт даних до інших систем обліку;

- формування облікових форм статистичної звітності. Функції аналізу та формування статистичної звітності за затвердженими формами МОЗ, державної статистичної служби та інші звіти для управління інститутом, показники КРІ тощо;

- ведення нормативної бази знань. Функції ведення шаблонів медичної документації, схем лікування, норм для інструментальних та лабораторних досліджень, еталонних протоколів лікування, довідників лікарських засобів тощо;

- інформаційне забезпечення наукової діяльності. Функції введення показників для проведення наукових досліджень. Функції відбору груп пацієнтів для досліджень. Експорт даних до інших систем аналізу первинних даних;

- інформаційна взаємодія в перспективі із загальнодержавним електронним реєстром пацієнтів, створюваного у відповідності з постановою Кабінету Міністрів України від 6 червня 2012 р. № 546. Реєстр, як відомо, є інформаційним ресурсом МОЗ, що ведеться з використанням інформаційних технологій, електронного документообігу та електронного цифрового підпису, у який заклади охорони здоров'я всіх форм власності зобов'язані вносити певні відомості про пацієнтів.

Автоматизація зазначених вище функцій і задач повинна була здійснюватись засобами типового функціоналу АМІС.

На першому етапі автоматизації ми не планували автоматизацію певних бізнес-процесів клініки, зокрема, облік робочого часу для нарахування заробітної плати, регламентований бухгалтерський облік, планування закупівель, управлінський облік непрямих витрат, розрахунків планової та фактичної собівартості продукції, однак передбачали можливість їх реалізації в майбутньому шляхом розширення функціональності системи.

Загальні вимоги до системи.

1. Вимоги до структури АМІС. АМІС повинна мати архітектуру «клієнт-сервер» та базуватися на наступних основних принципах:

- відкритість – система повинна використовувати загальнодоступні й специфіковані рішення, протоколи й інтерфейси, що має забезпечувати інтеграцію створюваних рішень як між собою, так й із зовнішніми інформаційними системами;

- модульність – система повинна бути побудована з використанням модульної архітектури, що передбачає реалізацію основних функцій як окремих модулів, що забезпечують можливість їх незалежної модифікації. Збій у роботі одного з модулів не повинен приводити до повного припинення функціонування системи в цілому;

- масштабованість – архітектура системи повинна дозволяти збільшувати продуктивність систем, обсяги збереженої й оброблюваної інформації без тривалої зупинки роботи й значної модифікації програмного коду;

- керованість і конфігурування – має бути забезпечене керування системою на всіх рівнях її архітектури: на рівні інфраструктури, на функціональному рівні, на рівні представлення даних;

- системність – усі взаємозалежні підсистеми створеної системи мають використовувати єдину методологію, і відповідати єдиним принципам взаємодії, надійності й керування;

- персоналізація – надання інформації користувачам повинне здійснюватися з урахуванням персональних налаштувань користувачів;

- єдність графічного представлення – при проектуванні й розробці користувацьких інтерфейсів повинні використовуватися загальні принципи графічного представлення інформації й організації доступу користувачів до функціональних можливостей і сервісів системи;

- захищеність інформації – має бути передбачені механізми й заходи із забезпечення захисту службової інформації обмеженого доступу.

Враховуючи поставлені завдання ми передбачали наявність у програмному компоненті АМІС наступних основних функціональних підсистем:

ПІДСИСТЕМА 1. Настроювання політики безпеки: формування списку користувачів і визначення їх ролей по використанню функціональності системи.

ПІДСИСТЕМА 2. Формування графіку роботи лікарів.

ПІДСИСТЕМА 3. Введення інформації про пацієнта та оперування нею, включаючи ведення електронної медичної карти пацієнта (ЕМК), в т.ч., електронної амбулаторної карти пацієнта та медичної картки стаціонарного хворого, забезпечення пошуку й організація доступу вповноваженого персоналу до інформації про пацієнта, постановка діагнозів з обліком міжнародною класифікацією хвороб (МКБ 10), прикріплення до ЕМК зображень із поповнюваної бібліотеки й можливість прикріплювати до них анотації, формування твердої копії медичної карти пацієнта та окремих документів медичної карти пацієнта, автоматизоване формування медичних висновків, епікризів і виписок з медичної карти, реєстрацію видачі лікарняних листків, настроювання робочого місця лікаря будь-якої спеціальності, редагування структури бази даних, екранних форм, макетів документів, звітів і інших об'єктів, перегляд електронної медичної карти пацієнта в компактному, узагальненому виді, різні способи відображення медичної інформації: графіки, схеми, таблиці і т.д., інструменти заповнення ЕМК: контекстні довідники, конструктор фраз, шаблони протоколів огляду, контроль введення даних, автоматичне формування й друк епікризів, протоколів досліджень, медичних довідок, результатів аналізів і т.п., інтеграцію з офісними додатками, зовнішніми базами даних і спеціалізованими медичними інформаційними системами, контроль строків відвідування лікаря, і таке інше);

ПІДСИСТЕМА 4. Організація лабораторних досліджень (в т.ч. імпорт і друк протоколів досліджень, потокове створення талонів на лабораторні дослідження, наочне, у вигляді схем і графіків відображення різної динамічно змінюваної інформації про пацієнта, у тому числі результатів лабораторних досліджень) та автоматичне формування аркушів призначень для забезпечення обліку виконання призначених лікувально-діагностичних заходів. Підсистема має забезпечувати автоматизацію діяльності всіх діагностичних лабораторій, відділень і кабінетів;

ПІДСИСТЕМА 5. Рух медикаментів (створення довільної кількості складів для аптеки, відділень, кабінетів і окремих лікарів; облік товарів по партіях і по найменуваннях; повний цикл руху медикаментів і видаткових матеріалів: заявки від відділень, замовлення

постачальникам, приходи, переміщення, списання, інвентаризація; персоніфікований облік лікарських засобів, робота зі сканером штрих-коду й принтером етикеток, формування необхідних документів для бухгалтерського обліку й статистичної звітності);

ПІДСИСТЕМА 6. Опис ліжкового фонду в розрізі відділень, палат різних категорій і розташування ліжок;

ПІДСИСТЕМА 7. Отримання зображення з автоматизованого діагностичного обладнання за протоколом DICOM;

ПІДСИСТЕМА 8. Прикріплення до ЕМК зображень, одержуваних із діагностичного обладнання;

ПІДСИСТЕМА 9. Підключення автоматизованого лабораторного обладнання за стандартними протоколами LIS2, LIS3, ASTM із можливістю ручного введення результатів лабораторних досліджень у тих випадках, коли автоматизований обмін даними з лабораторним обладнанням є неможливим, адресацією вповноваженим співробітником лабораторії результатів проведених аналізів відповідному фахівцю після формування пакета результатів із забезпеченням створення твердої копії результату кожного окремого дослідження та ведення архіву результатів лабораторних досліджень, забезпечення інтеграції з PACS-системами сторонніх виробників за протоколом HL7 та одержанням доступу до зображень з будь-якого робочого місця;

ПІДСИСТЕМА 10. Захист від загроз безпеці персональних даних, оброблюваних в інституті, та ліквідація можливих каналів витоку персональних даних з АМІС;

ПІДСИСТЕМА 11. Оформлення регламентованих запитів, тобто інформування зацікавленого користувача АМІС шляхом надання даних, склад і форма відображення яких визначені заздалегідь, і обумовлені постійними інформаційними потребами. Реалізація нерегламентованих запитів, тобто надання можливості пошуку й перегляду даних, а також складання аналітичних документів, склад яких заздалегідь не визначений і вказується в момент формування запиту;

ПІДСИСТЕМА 12. Забезпечення ведення всіх нормативних документів, довідників і класифікаторів, необхідних для роботи, а також параметрів настроювання, необхідних для адаптації АМІС до умов роботи в установі й підтримки роботи в умовах функціонування інституту, що змінюються. До параметрів настроювання відносяться, зокрема, настроювання АРМів користувачів АМІС;

ПІДСИСТЕМА 13. Підготовка звітності для органів системи охорони здоров'я бібліотекою готових звітів по медичній статистиці за формами, затвердженими МОЗ та державною службою статистики), з можливостями створення нестандартних звітів довільної форми й змісту, необхідних медичній установі, шляхом експорту статистичних даних в один із загальноновизнаних форматів;

ПІДСИСТЕМА 14. Ведення даних огляду пацієнтів «вузькими» спеціалістами різного профілю з можливістю обліку використовуваних для лікування видаткових матеріалів;

ПІДСИСТЕМА 15. Забезпечення підтримки лікувально-діагностичної діяльності медичного персоналу на підставі чинних стандартів лікування.

Функціонально програмне забезпечення (ПЗ) повинне мати можливість без зайвих технологічних і виробничих витрат активізувати зазначені підсистеми й опції за бажанням Замовника. Для ефективної взаємодії між собою всі підсистеми повинні функціонувати в єдиному інформаційному просторі й мати єдину базу даних. В якості протоколу взаємодії між компонентами системи на транспортно-мережному рівні ми планували використовувати стек протоколів TCP/IP.

2. Вимоги до функціонування АМІС. Система повинна підтримувати основний режим, у якому всі підсистеми АМІС виконують усі свої основні функції у форматі 24x7, та профілактичний режим, у якому одна або всі підсистеми АМІС не виконують своїх функцій. Для забезпечення високої надійності функціонування АМІС як системи в цілому, так і її окремих компонентів у комплекті поставки програмного компоненту повинні бути наявні штатні засоби для моніторингу й діагностики стану системи з обов'язковим веденням журналів інцидентів в електронній формі, а також графіків і журналів проведення профілактичних робіт. Для всіх апаратних компонентів необхідно забезпечити регулярний і постійний контроль стану й можливість технічного обслуговування.

3. Вимоги до чисельності та кваліфікації персоналу, який використовує та обслуговує АМІС. Чисельність персоналу клініки, що обслуговує АМІС, повинна відповідати нормам, обумовленим технічними вимогами до використовуваного програмно-апаратного комплексу АМІС. Увесь медичний персонал, допущений до роботи з АМІС, повинен пройти курс навчання роботі із системою.

4. Вимоги до пристосовності АМІС до змін. Забезпечення пристосовності системи повинне виконуватися за рахунок можливості: своєчасного адміністрування, модернізації процесів збору, обробки й завантаження даних відповідно до нових вимог, модифікації процедур доступу й вистави даних кінцевим користувачам, наявності файлів настройки чи конфігураційних файлів у програмному забезпеченні підсистем.

5. Вимоги до надійності АМІС.

5.1. Склад показників надійності для системи в цілому. Рівень надійності повинен досягатися погодженим застосуванням організаційних, технічних і програмно-апаратних засобів, зокрема, за рахунок: застосування технічних засобів, системного й базового програмного забезпечення, відповідних класу розв'язуваних завдань, своєчасного виконання процесів адміністрування АМІС, дотримання правил експлуатації й технічного обслуговування програмно-апаратних засобів, попереднього навчання користувачів і обслуговуючого технічного персоналу.

Час відновлення працездатності АМІС при будь-яких збоях і відмовах не повинен перевищувати 3-х годин, у який входить розгортання й настроювання спеціального програмного забезпечення на сервері (-ах), відновлення даних із використанням останньої резервної копії й «накат» по журналах до стану, що передував аварії. У зазначений час не входить вирішення проблем з апаратної складової АМІС та переінсталяція операційних систем.

5.2. Перелік аварійних ситуацій, з яких регламентуються вимоги щодо надійності. Під аварійною ситуацією розуміється аварійне завершення процесу, виконуваного тією або іншою підсистемою АМІС, а також «зависання» цього процесу. При роботі системи можливі наступні аварійні ситуації, які впливають на надійність роботи системи: збій в електропостачанні сервера, збій в електропостачанні АРМів користувачів системи, збій в електропостачанні комутаційних вузлів ЛКМ, помилки АМІС, не виявлені при налагодженні й випробуванні системи, збої операційної системи та іншого програмного забезпечення сервера.

5.3. Вимоги до надійності технічних засобів і програмного забезпечення. До надійності устаткування пред'являються наступні вимоги:

- у якості апаратних платформ повинні використовуватися засоби з підвищеною надійністю, при цьому перевага надається серверним рішенням на базі модульних серверів з, як мінімум, подвійним запасом надійності основних компонентів – блоків живлення, мережних інтерфейсів, обчислювальних модулів, дискових масивів тощо;

- застосування технічних засобів відповідних до класу розв'язуваних завдань;
- апаратно-програмний комплекс АМІС повинен мати можливість відновлення у випадках збоїв.

До надійності електропостачання компонентів АМІС пред'являються наступні вимоги:

- з метою підвищення відмовостійкості системи в цілому необхідна обов'язкова комплектація серверів джерелами безперебійного живлення з можливістю автономної роботи системи не менш 30 хвилин;
- система повинна бути укомплектована підсистемою оповіщення адміністраторів АМІС про перехід на автономний режим роботи;
- система повинна бути укомплектована агентами автоматичної зупинки операційної системи у випадку, якщо перебіг електроживлення перевищує 30 хвилин;
- безперебійне живлення активного мережного устаткування має забезпечувати можливість автономної роботи системи не менш 30 хвилин.

Надійність апаратних і програмних засобів повинна забезпечуватися за рахунок організаційних заходів, у т.ч. своєчасного виконання процедур резервного копіювання даних.

Надійність програмного забезпечення підсистем повинна забезпечуватися за рахунок:

- надійності загальносистемного та спеціалізованого програмного забезпечення;
- проведенням комплексу заходів налагодження, пошуку й виключення помилок;
- веденням журналів системних повідомлень і помилок по підсистемах для наступного аналізу.

6. Вимоги до ергономіки й технічної естетики. Підсистема формування й візуалізації звітності даних повинна забезпечувати зручний для кінцевого користувача інтерфейс, що відповідає наступним вимогам.

У частині зовнішнього оформлення:

- реалізацію в графічному віконному режимі за стандартами, прийнятими для програмних продуктів, що функціонують під керуванням графічної багатозадачної операційної системи;
- єдиному стилю оформлення інтерфейсу користувача для всіх підсистем;
- повинне бути забезпечена наявність україномовного (російськомовного) інтерфейсу користувача;
- розмір, колір та конфігурація екранних шрифтів повинні забезпечувати комфортну роботу користувачів;
- налаштовуваність графічних елементів інтерфейсу, у тому числі колірною оформлення, у межах можливостей операційної системи.

У частині діалогу з користувачем:

- діалог із користувачем повинен бути оптимізований для виконання типових і часто використовуваних прикладних операцій;
- при виникненні помилок у роботі підсистеми на екран монітора повинне виводитися повідомлення з найменуванням помилки й із рекомендаціями з її усунення;
- на екрані повинне здійснюватися відображення тільки тих можливостей, які доступні конкретному користувачеві й тільки необхідної для рішення поточної прикладного завдання інформації;
- повинна бути передбачена максимальна уніфікація процедур реалізації аналогічних функцій у різних підсистемах;
- повинна бути передбачена орієнтація на використання клавіатури з мінімізацією кількості натискань для стандартних дій;

- повинне бути передбачене використання функціональних і "гарячих" клавіш, при цьому на екрані повинна перебувати підказка про призначення таких клавіш;
- повинне бути передбачене використання маніпулятора "миша" на до дто к до клавіатури й мінімізація кількості натискань кнопок для стандартних дій;
- повинна бути забезпечена можливість зміни складу меню користувача за допомогою налаштування параметрів підсистем;
- повинне виконуватися відображення на екрані ходу тривалих процесів обробки;
- повинна бути передбачена розвинена система контекстної допомоги.

У частині процедур вводу-виводу даних:

- користувач повинен мати можливість гнучко контролювати введення даних – мати можливість переглядати введені дані на моніторі, робити їх коректування, або відмовитися від введення;
- при введенні повинні використовуватися для контролю випадуючі списки даних, що вводяться, і їх допустимих значень, має бути забезпечена можливість введення значень за замовчуванням;
- повинно бути виключене повторне введення даних;
- повинен здійснюватися логічний контроль інформації, що вводиться.

7. Вимоги до експлуатації, технічного обслуговування, ремонту й зберігання компонентів АМІС.

Умови експлуатації, а також види й періодичність обслуговування технічних засобів системи повинні відповідати вимогам з експлуатації, технічного обслуговування, ремонту й зберігання, викладеним у документації виробника. Технічні засоби системи й персонал повинні розміщуватися в приміщеннях, які за кліматичними умовами мають відповідати ГОСТ 15150-69 «Машини, прилади й інші технічні вироби. Виконання для різних кліматичних районів. Категорії, умови експлуатації, зберігання й транспортування в частині впливу кліматичних факторів зовнішнього середовища» (температура навколишнього повітря від 5 до 40 °С, відносна вологість від 40 до 80 % при T=25 °С, атмосферний тиск від 630 до 800 мм рт. ст.). Розміщення технічних засобів і організація автоматизованих робочих місць повинні бути виконані відповідно до вимог ГОСТ 21958-76 «Система "Людина-Машина". Зал і кабіни операторів. Взаємне розташування робочих місць. Загальні ергономічні вимоги». Живлення всіх технічних засобів повинне здійснюватись однофазною напругою 220 В частотою 50 Гц через мережні розетки із заземлюючим контактом відповідно до вимог ДСТУ 13109-97 «Електрична енергія. Сумісність технічних засобів. Норми якості електричної енергії в системах електропостачання загального призначення».

8. Вимоги до захисту інформації від несанкціонованого доступу.

8.1. Вимоги до інформаційної безпеки.

АМІС повинна відповідати вимогам до збереження інформації, викладеним у Законах України «Про захист персональних даних» (01.06.2010 № 2297-VI), «Про інформацію» (02.10.1992 № 2657-XII), "Про захист інформації в автоматизованих інформаційних системах" (05.07.1994 № 81/94-ВР), "Про захист інформації в інформаційно-комунікаційних мережах" (05.07.1994 № 80/94-ВР), іншими нормативно-правовими актами, виданими у відповідності з цими законами, а також «Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави», затвердженою постановою Кабінету Міністрів України від 27.11.1998 р., № 1893 (зі змінами від 07.09.2011 р.).

Забезпечення інформаційної безпеки АМІС повинне задовольняти наступним вимогам:

- захист системи має забезпечуватися комплексом програмно-технічних засобів і підтримуючих їх організаційних заходів;
- захист системи повинен забезпечуватися на всіх технологічних етапах обробки інформації й у всіх режимах функціонування, у тому числі при проведенні ремонтних і регламентних робіт;
- програмно-технічні засоби захисту не повинні суттєво погіршувати основні функціональні характеристики системи (надійність, швидкодію, можливість зміни конфігурації);
- розмежування прав доступу користувачів і адміністраторів системи повинне будуватися за принципом "що не дозволене, те заборонене".

У частині захисту інформації АМІС повинна забезпечувати:

- відповідність вимогам нормативних документів НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 1.1-004-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-008-2002 «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2», НД ТЗІ 3.7003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі";
- підтримку пристроїв введення ідентифікаційних ознак;
- контроль буфера обміну операційної системи MS Windows;
- контроль друку конфіденційного документа;
- розмежування доступу до пристроїв і контроль апаратної конфігурації: послідовні й паралельні порти; змінні, логічні й оптичні диски; USB-пристрої, пристрої PCMCIA, IEEE1394, Secure Digital;
- керування підключеннями Irda, Wifi, Firewire, Ethernet, Bluetooth;
- створення замкненого програмного середовища;
- контроль цілісності файлів, каталогів, елементів системного реєстру, секторів дисків;
- автоматичне знищення вмісту файлів при їхньому видаленні;
- гарантоване знищення інформації, що захищається, на локальних і змінних дисках;
- контроль апаратної конфігурації комп'ютера з реєстрацією подій і можливістю блокування комп'ютера;
- контроль друку захищеної інформації;
- реєстрацію подій безпеки;
- можливість збереження записів подій у log-файли;
- можливість перегляду архівів записів подій;
- можливість створення звітів щодо переліку встановленого програмного забезпечення, відомостям про ресурси, об'єкти й параметри комп'ютера, що захищається;
- функціональний самоконтроль підсистем;
- імпорт і експорт параметрів.

У процесі впровадження програмний компонент АМІС повинен бути сертифікований ДССЗІ на відповідність комплексу засобів захисту інформаційної системи від несанкціонованого доступу вимогам нормативних документів із технічного захисту інформації.

8.2. Вимоги до антивірусного захисту. Засоби антивірусного захисту повинні бути встановлені на всіх серверах, АРМах користувачів і адміністраторів АМІС. Засоби антивірусного захисту АРМів користувачів і адміністраторів повинні забезпечувати:

- централізоване мережне керування скануванням, видаленням вірусів і протоколюванням вірусної активності на АРМах користувачів;
- централізовану автоматичну інсталяцію клієнтського антивірусного програмного забезпечення на АРМах користувачів і адміністраторів;
- централізоване автоматичне відновлення вірусних сигнатур на робочих місцях користувачів і адміністраторів;
- ведення журналів вірусної активності;
- адміністрування всіх антивірусних продуктів.

8.3. Розмежування відповідальності ролей при доступі до об'єктів обмеження.

Вимоги щодо розмежування доступу мають бути наведені у вигляді матриці розмежування прав: код (тип) відповідальності, найменування об'єкту системи, на який накладаються обмеження, роль співробітника/одиниця організаційної структури, для яких накладаються обмеження. Адміністратор АМІС повинен мати права на створення та зміни форм і довідників.

9. Загальні вимоги щодо збереження інформації при аваріях. АМІС повинна забезпечувати резервне копіювання всіх даних. Вихід із ладу певної кількості жорстких дисків дискового масиву не повинен позначатися на працездатності підсистеми зберігання даних. Пріоритетним слід вважати застосування відмовостійких дискових масивів RAID рівнів 10 або 6 із використанням жорстких дисків SAS та наявністю достатньої кількості резервних дисків для «гарячої» заміни.

Після збою програмних модулів ядра АМІС або АРМів у процесі виконання завдань користувачами повинна бути забезпечена можливість відновлення даних до стану, що існував на момент закінчення останньої нормально завершеної перед збоєм транзакції.

10. Вимоги до захисту від дії зовнішніх впливів. До програмно-апаратного оточення системи пред'являються наступні вимоги до захисту від впливу зовнішніх впливів.

10.1. Вимоги до радіоелектронного захисту: електромагнітне випромінювання радіодіапазону, що виникає при роботі електропобутових приладів, електричних машин і установок, приймаючо-передаючих пристроїв, експлуатованих на місці розміщення системи, не повинні приводити до порушень працездатності підсистем.

10.2. Вимоги до стійкості, стабільності й витривалості до зовнішніх впливів:

- система повинна мати можливість функціонування при коливаннях напруги електроживлення в межах від 160 до 286 В;
- система повинна мати можливість функціонування в діапазоні припустимих температур навколишнього середовища, установлених виробником апаратних компонентів;
- система повинна мати можливість функціонування в діапазоні припустимих значень вологості навколишнього середовища, установлених виробником апаратних компонентів;
- система повинна мати можливість функціонування в діапазоні припустимих значень вібрацій, установлених виробником апаратних компонентів.

11. Вимоги щодо стандартизації й уніфікації. Для розробки інтерфейсів користувачів та засобів генерації звітів (будь-яких твердих копій) повинні використовуватися вбудовані можливості програмного компоненту АМІС.

12. Додаткові вимоги. АРМи користувачів АМІС мають бути побудовані на платформі x86 та на базі "тонких клієнтів" (бездискових термінальних станцій) у залежності від виду АРМу. Передбачається створення 3-х видів АРМів: для керівного складу клініки, включаючи завідувачів структурних підрозділів, для лікарів та наукових співробітників та середнього медичного персоналу. Система повинна забезпечувати стійке функціонування в мережі з одночасною роботою з інформаційною системою до 350 користувачів. Отримання твердих

копій документів повинне забезпечуватися на рівні кожного структурного підрозділу з використанням мережних технологій друку.

13. Вимоги безпеки. При впровадженні, експлуатації й обслуговуванні технічних засобів системи повинні виконуватися заходи електробезпеки відповідно до «Правил технічної експлуатації електроустановок споживачів».

Апаратне забезпечення системи повинне відповідати вимогам пожежної безпеки у виробничих приміщеннях за ДСТУ 12.1.004-91. «ССБП. Пожежна безпека. Загальні вимоги». Повинне бути забезпечене дотримання загальних вимог безпеки відповідно до ГОСТ 12.2.003-91. «ССБП. Устаткування виробниче. Загальні вимоги безпеки» при обслуговуванні системи в процесі експлуатації.

Значення еквівалентного рівня акустичного шуму, створюваного апаратурою системи, повинне відповідати ГОСТ 21552-84 «Засоби обчислювальної техніки. Загальні технічні вимоги, приймання, методи випробувань, маркування, упакування, транспортування й зберігання».

Вимоги до функцій, виконуваних АМІС. Система повинна забезпечувати такі показники швидкості виконання операцій (таблиці 1-3).

Таблиця 1. Вимоги до часу відгуку

№	Характеристика	Максимальний час
1.	Пошук пацієнта	5 сек.
2.	Відкриття медичної карти пацієнта	5 сек.
3.	Бронювання номерка до лікаря	3 сек.
4.	Бронювання ліжка	3 сек.

Таблиця 2. Вимоги до швидкості обробки даних

№	Характеристика	Максимальний час
5.	Друк комплекту регулярної (щоденної) звітності	30 хв.
6.	Друк титульного аркуша медичної карти	1 хв.
7.	Уведення результатів огляду	10 хв.
8.	Друк результатів огляду	2 хв.

Таблиця 3. Вимоги до швидкості формування звітів

№	Характеристика	Максимальний час
9.	Швидкість формування комплекту зведених річних звітів	120 хв.
10.	Швидкість формування комплекту зведених кварталних звітів	60 хв.
11.	Швидкість формування комплекту зведених щомісячних звітів	40 хв.
12.	Швидкість формування оперативного звіту	7 хв.
13.	Швидкість формування аналітичних звітів	30 хв.

Вимоги до видів забезпечення.

1. Вимоги до математичного забезпечення.

Не пред'являються.

2. Вимоги до програмного забезпечення.

2.1. Вимоги до складу, структури й способів організації даних у АМІС. Структура зберігання даних в АМІС повинна складатися з наступних основних областей:

- область тимчасового зберігання даних;
- область постійного зберігання даних;
- область вітрин даних.

Області постійного зберігання й вітрин даних повинні будуватися на основі багатомірної моделі даних, що передбачає виділення окремих вимірів і фактів з їх аналізом по обраних вимірах. Багатомірна модель даних фізично повинна бути реалізована в реляційній СУБД за схемою «зірка» і/або «сніжинка».

2.2. Вимоги до інформаційного обміну між компонентами системи. Інформаційний обмін між компонентами системи АМІС повинен бути реалізований у такий спосіб (таблиця 4).

Таблиця 4. Інформаційний обмін між компонентами системи АМІС

	Підсистема збору, обробки й завантаження даних	Підсистема зберігання даних	Підсистема формування й візуалізації звітності
Підсистема збору, обробки й завантаження даних		X	
Підсистема зберігання даних	X		X
Підсистема формування й візуалізації звітності		X	

2.3. Вимоги до інформаційної сумісності із суміжними системами. Система не повинна бути закритою для суміжних систем, і повинна підтримувати можливість експорту даних у суміжні системи через інтерфейсні таблиці, або файли даних в одному із загально визнаних форматів. Система повинна забезпечити можливість імпорту даних, одержаних від суміжної системи.

2.4. Вимоги щодо використання уніфікованих документів і класифікаторів. Значення необхідних класифікаторів і довідників повинні зберігатись і підтримуватись в спеціально розроблених файлах або репозиторії бази даних.

2.5. Вимоги по застосуванню систем керування базами даних. Для реалізації підсистеми зберігання даних повинна використовуватися промислова система управління базою даних (СУБД). СУБД повинна забезпечувати 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 тощо.

СУБД повинна включати:

- речення визначення даних (визначення баз даних, а також визначення й знищення таблиць і індексів);
- запити на вибір даних (речення SELECT);
- речення модифікації даних (додавання, видалення й зміна даних);

- речення керування даними (надання й скасування привілеїв на доступ до даних, керування транзакціями й інші).

Крім того, СУБД має надавати можливість виконувати в цих пропозиціях:

- арифметичні обчислення (включаючи різноманітні функціональні перетворення), обробку текстових рядків і виконання операцій порівняння значень арифметичних виразів і текстів;

- упорядкування рядків і (або) стовпців при виводі вмісту таблиць на печатку або екран дисплея;

- створення подань (віртуальних таблиць), що дозволяють користувачам мати свій погляд на дані без збільшення їх обсягу в базі даних;

- запам'ятовування виведеного по запиту вмісту таблиці, декількох таблиць або вистави в іншій таблиці (реляційна операція присвоєння);

- агрегування даних: групування даних і застосування до цих груп таких операцій, як середнє, сума, максимум, мінімум, число елементів і т.п.

2.6. Вимоги до структури процесу збору, обробки, передачі даних в АМІС та представлення даних. Процес збору, обробки й передачі даних у системі повинен бути передбачений регламентом процесів збору, перетворення й завантаження даних на етапі «Проектування. Розробка ескізного проекту. Розробка технічного проекту».

2.7. Вимоги до захисту даних від руйнувань при аваріях і збоях в електроживленні системи. Інформація в базі даних системи повинна зберігатися при виникненні аварійних ситуацій, зв'язаних зі збоями електроживлення. Система повинна мати безперебійне електроживлення, що забезпечує її нормальне функціонування протягом 30 хвилин у випадку відсутності зовнішнього енергопостачання, та 5 хвилин додатково для коректного завершення всіх процесів. Необхідно забезпечити контроль за станом блоків безперебійного живлення серверів з єдиного центру та отримання повідомлень через ЛКМ про їх нештатні стани адміністраторами АМІС у режимі реального часу. Резервне копіювання даних повинне здійснюватися на регулярній основі, в обсягах, достатніх для відновлення інформації в підсистемі зберігання даних. Перелік масивів даних, баз даних, накопичувачів інформації й інших інформаційних активів, що захищаються тем, або іншим способом визначається в результаті виконання проектних робіт на стадії «Технічний проект». Повинна бути передбачена можливість перегляду в процесі експлуатації складу активів, що захищаються, і методів захисту.

Способи захисту даних при аваріях і заходи, які повинні застосовуватися при експлуатації АМІС:

- дублювання й резервування джерел і мереж електроживлення;
- дублювання й резервування даних, включаючи гаряче резервування;
- використання механізмів відкоту транзакцій;
- використання схем контролю й відновлення цілісності даних;
- дублювання й резервування носіїв, накопичувачів даних, пристроїв зберігання даних і 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 програмного забезпечення.

2.8. Вимоги до контролю, зберігання, оновленню й відновленню даних. До контролю даних пред'являються наступні вимоги: система повинна протоколювати всі події, пов'язані зі зміною свого інформаційного наповнення, і мати можливість у випадку збою в роботі відновлювати свій стан, використовуючи раніше запротокольовані зміни даних. Вимоги до термінів зберігання даних визначаються чинними нормативними документами МОЗ України. Повинні бути розроблені апаратно-програмні рішення та організаційні заходи стосовно резервного копіювання й архівування даних.

3. Вимоги до мовного забезпечення. Для організації діалогу системи з користувачем повинен застосовуватися графічний віконний інтерфейс користувача. Підсистема збору, обробки й завантаження даних, підсистема зберігання даних, підсистема формування й візуалізації звітності повинні підтримувати українську, російську та англійську мови.

4. Вимоги до додаткового програмного забезпечення. Перелік необхідних додаткових програмних продуктів:

- програмне забезпечення серверу DICOM для збереження цифрових медичних зображень;
- серверні операційні системи MS Windows;
- операційні системи для АРМів клієнтів MS Windows;
- клієнтські ліцензії доступу до серверів MS Windows;
- клієнтські ліцензії MS Office (мінімальний набір повинен обов'язково включати програми MS Outlook, MS Word, MS Excel);
- клієнтські ліцензії програми корпоративного антивірусного захисту.

5. Вимоги до технічного забезпечення. Система повинна бути реалізована з використанням виділених серверів, конфігурація й технічні властивості яких визначаються у відповідності до задач, покладених на АМІС та обраних варіантів технічного вирішення. Мінімальний обсяг вільного простору для зберігання даних на дисковому масиві повинен забезпечувати зберігання інформації (окрім медичних зображень) на протязі 25 років. Архівні дані повинні зберігатись протягом 50 років. Об'єм дискового масиву має забезпечувати збереження бази цифрових медичних зображень протягом не менше 5 років.

5.1. Вимоги до активного мережного устаткування. Усе активне мережне устаткування, яке поставляється, повинне бути новим, сучасних моделей, з оптимальними версіями програмного забезпечення для управління й моніторингу мережі та інтегруватись в існуючу ЛКМ. Розміщуватись устаткування повинне в спеціалізованих закритих комутаційних шафах. Виробник мережного устаткування повинен обов'язково мати представництво в Україні та авторизовані сервіс-центри.

Активне мережне устаткування повинно задовольняти наступним вимогам:

- забезпечувати управління й моніторинг мережі за протоколами SNMP версій 1,2,3, RMON1,2, SPAN, RSPAN, підтримку технології sFlow, мати WEB-інтерфейс для дистанційного керування, підтримувати можливість стекування;
- забезпечувати повну підтримку протоколу 802.1x, апаратну підтримку Integrated Firewall subsystem, апаратну підтримку Integrated Intrusion Detection subsystem, функціональність Identity-Based Networking Services (IBNS), мати апаратно реалізовані списки доступу рівнів 2/3 (без зниження продуктивності), функціональність Private VLAN, фільтрацію

за MAC-адресами і протоколами, постійні записи ARP, Port Security і т.п.; для забезпечення безпеки при адмініструванні – підтримка протоколів SSHv1, SSHv2 і SNMPv3, а також централізованої аутентифікації на TACACS+ і RADIUS серверах;

- забезпечувати підтримку апаратної маршрутизації трафіку (протоколи RIP, OSPF, IS-IS, EIRGP, BGP4, MBGP, PIM, DVMRP і т.п.);

- забезпечувати розширену підтримку якості обслуговування (QoS): апаратну реалізацію механізмів якості обслуговування, включаючи класифікацію (L2/3), полісинг, маркіровку трафіку, черговість на вході (L2) і виході (L2/3), можливість обмеження смуги пропускання (у тому числі для окремих користувачів і потоків);

- забезпечувати підтримку новітніх розробок в області забезпечення QoS/CoS;

- мати відповідну документацію (інструкцію з експлуатації, настройки тощо) російською та (або) українською мовою.

Активне мережне устаткування повинне бути сумісне із продукцією інших виробників (сумісність має підтверджуватися документами або публічно доступними посиланнями на них відповідних виробників).

Активне мережне устаткування вузлів комутації магістралі повинне забезпечувати виконання вимог інформаційної безпеки: аутентифікацію й авторизацію користувачів.

Активне мережне устаткування повинно мати довічну гарантію фірми-виробника (під довічною гарантією мається на увазі увесь період випуску даної продукції виробником + 5 років). Гарантійні зобов'язання для активного мережного устаткування повинні забезпечуватись Сервісним центром при представництві фірми-виробника або авторизованим Сервісним центром українського партнера, сертифікованого представництвом фірми-виробника.

5.2. Вимоги до пасивного мережного устаткування. З'єднання активного мережного обладнання (комутаторів) між собою повинне здійснюватись за допомогою багатомодового оптичного кабелю та забезпечувати швидкість передачі даних не менше 1 Гбіт/с; під'єднання серверів здійснюється мідним кабелем «вита пара» (UTP) із забезпеченням швидкості 1 Гбіт/с; під'єднання АРМів користувачів здійснюється мідним кабелем «вита пара» (UTP) із забезпеченням швидкості 100 Мбіт/с.

5.3. Вимоги до робіт із прокладання кабельної мережі та її тестування. Зміст і якість будівельно-монтажних робіт із прокладання кабельної мережі повинні відповідати діючим будівельним нормам і правилам на ці види робіт. Після закінчення всіх будівельно-монтажних робіт та монтажу активного мережного обладнання має бути проведено належне тестування мережі з оформленням протоколів тестування та кабельних журналів.

5.4. Вимоги до серверного устаткування. Конфігурація і технічні можливості серверів повинні відповідати покладеним на них завданням, кількості АРМів користувачів та програмному компоненту системи і забезпечувати:

- відмовостійку роботу;
- безперервний доступ до критичних додатків;
- можливість модернізації програмного забезпечення без зупинки критичних додатків;
- безперервний доступ до даних.

Серверне устаткування повинно мати не менше як 3-річну гарантію фірми-виробника. Гарантійні зобов'язання повинні забезпечуватись Сервісним центром при представництві фірми-виробника або авторизованим Сервісним центром українського партнера, сертифікованого представництвом компанії-виробника.

5.5. Вимоги до сховищ даних. Загальні дані АМІС та цифрові медичні зображення повинні зберігатись в окремих сховищах. Сховища повинні бути відмовостійкими – побудовані на дискових масивах та мати 2-кратний або більше запас надійності по електроживленню (із можливістю «гарячої» заміни як блоків живлення, так і окремих дисків із дискового масиву) та обладнані блоками безперебійного живлення. Архівація загальних даних повинна здійснюватись по мережі в окреме сховище, фізично віддалене від основного сховища.

5.6. Вимоги до обладнання АРМів користувачів. Конфігурація й технічні можливості комп'ютерного обладнання АРМів користувачів повинні відповідати покладеним на них завданням і забезпечувати продуктивну і комфортну роботу з АМІС. Обладнання стаціонарних АРМів блоками безперебійного живлення ~~взаємним~~ ^{взаємним}. Комп'ютерне обладнання АРМів користувачів повинно мати не менше як 3-річну гарантію фірми-виробника. Гарантійні зобов'язання повинні забезпечуватись Сервісним центром при представництві фірми-виробника або авторизованим Сервісним центром українського партнера, сертифікованого представництвом фірми-виробника.

5.7. Вимоги до інтеграції автоматизованого діагностичного та лабораторного обладнання в АМІС. Повинна бути здійснена інтеграція до АМІС через ЛКМ наявного автоматизованого діагностичного обладнання, яке підтримує стандарт DICOM (рентгенапарати, відеоторакоскопичне обладнання та ін.), та лабораторного устаткування, яке підтримує стандарт ASTM 1394. Для роботи з файлами зображень АМІС повинна мати засоби обробки та архівування зображень (PACS). Із системою повинен постачатись сервер DICOM, що може працювати з діагностичним обладнанням, яке підтримує протокол DICOM, забезпечує архівацію зображень та їх отримання за запитом користувача. Вбудований переглядач зображень повинен забезпечувати можливості для перегляду та аналізу зображень, експорту/імпорту з різних графічних форматів, запису на CD/DVD тощо.

Автоматизація технологічного процесу проведення лабораторних досліджень повинна забезпечуватись реалізацією наступних функцій:

- формування та друк направлень на проведення аналізів;
- реєстрацію направлень на лабораторні дослідження;
- диспетчеризацію замовлень;
- реєстрацію забору біоматеріалу;
- ведення архіву біоматеріалів;
- підготовку робочих журналів;
- автоматичне формування журналу реєстрації проведених аналізів та їх результатів;
- реєстрація результатів методик досліджень, проведених вручну;
- контроль результатів аналізів на відповідність нормам;
- оперативний аналіз динаміки результатів досліджень;
- формування бланків результатів досліджень;
- формування відповідної звітної форми за його результатами в залежності від проведеного аналізу;
- підтримку діяльності різних видів лабораторій (експрес лабораторії, клініко-діагностичні лабораторії, бактеріологічні лабораторії та інші): налагодження різних видів досліджень та вимірювальних показників; ведення довідникової інформації (типові звіти, одиниці виміру, покази на дослідження тощо); формування статистичних довідок та звітів у довільній формі;

- автоматизоване сполучення з біохімічними аналізаторами за протоколами стандарту ASTM 1394.

- автоматизацію процесу внутрішньо-лабораторного контролю якісно-кількісних методик досліджень повинна забезпечуватись реалізацією таких функцій:

- автоматизацію методу контролю по атестованим та не атестованим контрольним матеріалам: реєстрацію методик та груп методик (приладів); реєстрація контрольних матеріалів; реєстрацію паспортних характеристик контрольних матеріалів; реєстрацію даних контрольних досліджень; визначення кількісних статистичних характеристик контрольних серій; оцінку якісних критеріїв за даними контрольних серій;

- формування друкованих форм протоколів внутрішньо-лабораторного контролю якості за контрольними матеріалами;

- контроль якості по щоденним середнім;

- контроль відповідності методик нормам вірогідності та відтворюваності результатів;

- контроль за дотриманням правил по забору матеріалу та відповідності правилам зберігання;

- контроль технології проведення лабораторних досліджень;

- використання рекомендованих гранично допустимих значень зміщень та варіацій;

- використання тимчасових норм точності досліджень.

- функції системи по адаптації до умов роботи в конкретній лабораторії:

- налагодження видів досліджень;

- налагодження параметрів досліджень;

- налагодження діапазонів норм;

- налагодження методик досліджень.

6. Вимоги до метрологічного забезпечення АМІС. Не пред'являються.

7. Вимоги до організаційного забезпечення функціонування АМІС. Основними користувачами системи АМІС є співробітники структурних (клінічних та наукових) підрозділів. Забезпечує експлуатацію системи відділ інформаційно-комп'ютерних технологій. Склад співробітників кожного зі структурних підрозділів визначається штатним розкладом, який може змінюватися. До захисту від помилкових дій персоналу пред'являються наступні вимоги:

- повинна бути передбачена система підтвердження легітимності користувача при перегляді даних;

- для всіх користувачів повинна бути заборонена можливість видалення наперед налаштованих об'єктів і звітності;

- для зниження помилкових дій користувачів має бути розроблений повний і доступний посібник користувача АМІС.

8. Вимоги до методичного забезпечення функціонування АМІС. Методичне забезпечення АМІС здійснюється у вигляді навчання співробітників методиці роботи з нею та поставки експлуатаційної документації на робочі місця АМІС.

9. Вимоги до патентної чистоти. Щодо всіх апаратних та програмних засобів, що входять до складу системи, повинні дотримуватись умов ліцензійних угод та забезпечуватись патентна чистота відповідно до норм чинного законодавства України..

Види й обсяг випробувань системи. Система зазнає випробування наступних видів:

1. Попередні випробування.

2. Експериментальна експлуатація.

3. Приймальні випробування.

Вимоги до складу й змісту робіт по підготовці об'єкта автоматизації до введення системи в дію. У цьому розділі наводиться перелік заходів, що має передувати впровадженню АМІС (підготовка приміщень для розміщення програмно-апаратного комплексу АМІС, відповідно до вимог, наведених у сформованому технічному завданні, виконання необхідних будівельно-монтажних робіт щодо створення (розширення) ЛКМ тощо). Обсяг і характер цих заходів цілком залежать від конкретних умов медичного закладу.

Вимоги до термінів та якості гарантійного обслуговування:

- терміни гарантійного обслуговування апаратного компоненту АМІС викладені в пп. 6.5.1, 6.5.4 та 6.5.6;
- термін гарантії на пасивні елементи ЛКМ та виконанні монтажні роботи щодо прокладання кабельних мереж має бути не менше 10 років;
- термін реагування авторизованого Сервісного центру на виникнення несправності повинен бути не більше 2-х годин;
- термін прибуття фахівця авторизованого Сервісного центру для усунення несправності не повинен перевищувати 24-х годин із моменту отримання повідомлення;
- термін гарантійного ремонту устаткування не повинен перевищувати 30 діб;
- заміна несправних гарантійних елементів устаткування виконується безкоштовно шляхом передачі авторизованому Сервісному центру з метою подальшого ремонту або заміни цього устаткування, усі види витрат при цьому несе авторизований Сервісний центр. На час проведення гарантійного ремонту Сервісний центр надає устаткування, аналогічне по продуктивності відданому в ремонт, для забезпечення працездатності системи на термін гарантійного ремонту;
- як справне (відремонтоване) устаткування авторизований Сервісний центр може повернути аналогічне по функціональності й продуктивності устаткування, сертифіковане фірмою-виробником і допущене до продажу на території України з документацією.

Конкретні вимоги до складу та конфігурації серверів бази даних, DICOM, PACS, резервного копіювання та АРМів користувачів доцільно формулювати після визначення програмних компонентів системи та кількості робочих місць, що планується підключити до неї.

Література та вебліографія

1. Проект наказу МОЗ України "Про затвердження Концепції інформатизації сфери охорони здоров'я України" [Електронний ресурс]. – Режим доступу: http://www.moz.gov.ua/ua/portal/dn_20121226_pp.html.
2. Концепция информатизации здравоохранения России [Электронный ресурс]. – Режим доступа: <http://www.med-obr.info/med-organisation/actual-documents/informatisation/2.pdf>.
3. Орлов, Г. М. Типовая медицинская информационная система персонифицированного учета оказания медицинской помощи [Текст] / Г. М. Орлов // Врач и информационные технологии. – 2009. – № 2, – С. 38–43.
4. Дабагов, А. Р. Информатизация здравоохранения и некоторые проблемы построения интегрированных медицинских информационных систем [Электронный ресурс] / А. Р. Дабагов. – Режим доступа: <http://jre.cplire.ru/mac/sep11/2/text.html>.
5. Павлов, В. В. Актуальные вопросы внедрения и использования медицинских информационных систем (МИС). Проблемы и ошибки при внедрении и использовании МИС [Текст] / В. В. Павлов, А. В. Закамсков, З. Б. Рахманова // Информационно-измерительные и управляющие системы. – 2010. – Т. 8, № 12. – С. 82–85.
6. Морозов, Д. В. Информатизация медицины. Новый этап развития [Электронный ресурс] / Д. В. Морозов, К. И. Лысенко, Л. И. Баранов. – Режим доступа: http://zhenilo.narod.ru/main/ips/2009_medicine.pdf.
7. Об опыте разработки и внедрения медицинских информационных систем [Электронный ресурс]. – Режим доступа: <http://www.zdrav.ru/articles/practice/detail.php?ID=77693>.
8. Сравнительная характеристика различных подходов к автоматизации деятельности стационара [Электронный ресурс]. – Режим доступа: <http://ucr.gs.com.ua/support/files/hcr&meds.doc>.
9. Гусев, А. Медицинские информационные системы: анализ рынка [Электронный ресурс] / А. Гусев, Ф. Романов, И. Дуданов. – Режим доступа: http://www.pcweek.ru/idea/article/detail_print.php?ID=75038&print=Y.
10. СТО МОСЗ 91500.16.0002-2004. Стандарт организации «Информационные системы в здравоохранении. Общие требования» [Электронный ресурс]. – Режим доступа: http://www.miacso.ru/UPLOAD/fck/files/Doc_all/Standart.pdf.
11. Методические рекомендации по составу создаваемых в 2011 – 2012 годах в рамках реализации региональных программ модернизации здравоохранения прикладных компонентов регионального уровня единой государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним [Электронный ресурс]. – Режим доступа: <http://www.minzdravsoc.ru/docs/mzsr/informatics/45>.
12. Методические рекомендации по составу и техническим требованиям к сетевому телекоммуникационному оборудованию учреждений системы здравоохранения для регионального уровня единой государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним [Электронный ресурс]. – Режим доступа: <http://www.minzdravsoc.ru/docs/mzsr/informatics/46>.
13. Методические рекомендации по оснащению медицинских учреждений компьютерным оборудованием и программным обеспечением для регионального уровня единой государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним [Электронный ресурс]. – Режим доступа: <http://www.minzdravsoc.ru/docs/mzsr/informatics/47>.

14. Требования к МИС, передаваемым в фонд алгоритмов и программ Министерства здравоохранения и социального развития Российской Федерации, применяемым в Государственной информационной системе персонифицированного учета в здравоохранении Российской Федерации. № SBR1009140314-02-2.20 [Электронный ресурс]. – Режим доступа: http://gosbook.ru/system/files/2010/12/14/Trebovaniya_k_MIS_na_sajt.

15. Федеральная типовая МИС [Электронный ресурс]. – Режим доступа: <http://www.med.korusconsulting.ru/systems/ftmis/>.

16. Технические требования медицинской информационной системы [Электронный ресурс]. – Режим доступа: http://www.kmis.ru/site.nsf/pages/kmis_tech.htm.

17. Техническое задание на выполнение работ по созданию системы защиты персональных данных в сегменте информационной системы «Республиканская медицинская информационная система» МБУЗ г. Улан-Удэ «Городская больница №1» [Электронный ресурс]. – Режим доступа: <http://zakupki.ulau-ude-eg.ru/Competition/Doc/3468-2012102416275260918136.doc>.

18. Техническое задание на выполнение работ по автоматизации деятельности ГОАУЗ «Мурманский областной центр восстановительной медицины и реабилитации» путем внедрения комплексной медицинской информационной системы, интегрированной с региональным информационным ресурсом системы здравоохранения Мурманской области [Электронный ресурс]. – Режим доступа: <http://do2.gendocs.ru/download/docs-441259/441259.doc>.

19. Выполнение научно-исследовательских и опытно-конструкторских работ по созданию общегородского информационного сервиса интегрированной медицинской информации (СИМИ ЕМИАС). Техническое задание [Электронный ресурс]. – Режим доступа: http://www.dit.mos.ru/upload/1622/СИМИ_ТЗ_10.doc.