Інформаційні технології в медицині та біології

УДК681.518:004.93.1

О.Й. Березький, Л.О. Дубчак, О.Й. Піцун

Тернопільський національний економічний університет, Тернопіль

РОЗПОДІЛ ДОСТУПУ В ІНТЕЛЕКТУАЛЬНІЙ СИСТЕМІ АВТОМАТИЗОВАНОЇ МІКРОСКОПІЇ

В даній статті розглянуто сучасний стан систем автоматизованої мікроскопії та їх застосування в телемедицині. Аналіз показує, що розробка політики безпеки таких САМ є актуальною задачею. Крім того, виділено основні користувачі системи автоматизованої мікроскопії та здійснено розподіл їх прав доступу до інформації. На основі проведених досліджень спроектовано і програмно реалізовано інтелектуальну систему автоматизованої мікроскопії з адаптивним графічним інтерфейсом різних типів користувачів для опрацювання біомедичних зображень.

Ключові слова: *система автоматизованої мікроскопії, адаптивний графічний інтерфейс, біомедичні зображення, політика безпеки, телемедицина.*

Вступ

Телемедицина – це галузь медицини, яка використовує телекомунікаційні та електронні інформаційні (комп'ютерні) технології для надання медичної допомоги і послуг в сфері охорони здоров'я в точці необхідності [1]. Засобом зв'язку між клієнтом та комп'ютерною системою медичного закладу є Інтернет. Звідси випливають усі проблеми захисту інформації, що використовується в телемедицині, з точки зору інформаційної системи та мережі.

Останнім часом у онкологічній клінічній практиці широко застосовуються системи автоматизованої мікроскопії (САМ) для діагностування різного роду захворювань. САМ реалізують інформаційну технологію аналізу біомедичних (гістологічних та цитологічних) зображень [2]. Найпопулярнішими САМ є такі: Amira, AxioVision, BioImageXD, OncoDoc, ImageJ [10], ImageTool, ИМАДЖЕР-ЦГ та ScreenMeter [2–4; 11]. Недоліками більшості з них є висока вартість та складність окремих підпрограм, а також наявність недружелюбних інтерфейсів користувачів.

САМ складаються в основному з мікроскопа, комп'ютера та спеціалізованого програмного забезпечення. Багатофункціональний мікроскоп (лабораторного або дослідницького класу) забезпечує проведення різних методик дослідження [5]. Спеціалізоване програмне забезпечення містить реалізовані методи та алгоритми для покращення якості зображень, фільтрації, проведення морфологічних операцій, сегментації, контурного аналізу, класифікацій мікрооб'єктів [6]. Важливим критерієм, за яким можна класифікувати САМ, є ступінь автоматизації окремих операцій, адже для роботи зі складною системою з великою кількістю ручних операцій потрібно додатково проводити навчання персоналу.

Метою даної статті є розробка структури системи автоматизованої мікроскопії, що забезпечує захист інформації в телемедичній системі та спрощує сам процес взаємодії її складових.

Політика безпеки телемедицини

Телемедицина поділяється на локальну та глобальну. В глобальній медичній консультативно-діагностичній системі в ролі клієнта виступають підсистеми консультативно-діагностичних пунктів чи центрів, а сервер виконує роль накопичувача та координаційно-технічного центру [2].

Будь-яка інформаційна система включає [2]: прикладне програмне забезпечення (ППЗ), яке відповідає за зв'язок системи з клієнтом; системи управління базами даних (СУБД); операційну систему для обслуговування ППЗ та СУБД; мережу, яка забезпечує взаємодію всіх вузлів інформаційної системи.

Найнебезпечнішими для таких інформаційних систем є:

- несанкціонований доступ до паролів чи конфіденційної інформації;
- порушення правдоступу;
- атаки типу «відмова в обслуговуванні»;
- «пряма» атака;

– віруси;

– сучасні атаки по побічних каналах витоку інформації.

Несанкціонований доступ полягає у підборі чи викраденні пароля або підміні IP-адреси законного користувача системи. До цього виду атак вразливі усі компоненти інформаційної системи.

Існує чотири стандартні підходи, за допомогою яких можна обмежити доступ до інформації, а саме контроль доступу, розширення парольного захисту, шифрування даних та використання брандмауерів [3].

Атака типу «відмова в обслуговуванні» полягає у створенні неправильного пакету даних чи передачі великої кількості пакетів даних по мережі з метою блокування роботи контролера домена, що зупиняє роботу комп'ютерної системи. Для захисту компонентів інформаційної системи застосовуються спеціальні програми виявлення такого типу атак чи міжмережеві екрани [4].

Комп'ютерний вірус – комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси або комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Для захисту від вірусів на даний час існує багато антивірусних програм, що захищає інформаційну систему від пошкодження.

Побічними каналами витоку інформації під час передачі пакетів даних по мережі є електромагнітне випромінювання, час виконання алгоритмів шифрування та реакція системи на спеціально внесені помилки. Для протидії таким атакам використовуються, як правило, архітектурна та операційна надлишковість, тобто додаткові апаратні та програмні засоби [3; 5].

Загалом можна визначити наступні методи захисту інформаційної системи від втрати чи викриття конфіденційної інформації [2].

Установка перешкоди – метод фізичного перешкоджання шляху зловмиснику до інформації, що захищається, у тому числі спроб з використанням технічних засобів знімання інформації і дії на неї.

Маскування – метод захисту інформації з використанням інженерних, технічних засобів, а також шляхом криптографічного закриття інформації.

Управління доступом – метод захисту інформації за рахунок регулювання використовування всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту:

1) ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);

2) аутентифікацію (встановлення автентичності) об'єкта або суб'єкта після пред'явлення ними ідентифікатора;

3) перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);

4) дозвіл і створення умов роботи в межах встановленого регламенту;

5) реєстрацію (протоколювання) звернень до ресурсів, що захищаються;

6) реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Проте, застосування всіх відомих методів захисту даних інформаційної системи не гарантує збереження цілісності даних, тому розробка нових підходів залишається актуальною задачею.

З метою побудови стійкої телемедичної системи, яка відповідає усім вимогам, запропоновано наступні складові політики безпеки.

1. Загальні вимоги до ОС та ПК:

– версія Windows 7/10 з метою шифрування диску, де знаходиться база даних чи система в цілому;

– наявність антивірусної та антишпигунських програм;

– розміщення бази даних на сервері, який є недоступним користувачам системи, крім адміністратора;

– опломбування системного блоку сервера запобігання підключення додаткових апаратних засобів зчитування і передачі інформації.

2. Вимоги до адміністрування:

а) рівні доступу:

– адміністратор – доступ до системи, програмних засобів (ПЗ), бази даних (БД) – має право надавати права і рівні доступу користувачам на певний час чи на постійно, вносити зміни в ПЗ чи базу даних, проводити аутентифікацію користувачів, а також перевірку і зміну політики безпеки;

– лікуючий лікар – доступ до системи через власний інтерфейс, доступ до БД, доступ до інформації про пацієнта, доступ до засобів відео- та аудіозв'язку, передача даних по мережі (за допомогою електронного цифрового підпису (ЕЦП) чи записом в журналі телемедицини, згідно наказу МОЗ №681) – має право обирати лікаря-консультанта, здійснювати аудіо- та відеозв'язок, вносити зміни в базу даних, передавати зашифровані дані про пацієнта, підтверджуючи їх за допомогою ЕЦП чи записом в журналі телемедицини, згідно наказу МОЗ №681;

– лікар-консультант – доступ до системи через свій інтерфейс, доступ до засобів відео- та аудіозв'язку, передача даних по мережі – має право доступу до даних, що передає лікуючий лікар, здійснювати запит на додаткову інформацію про пацієнта (крім прізвища та ім'я пацієнта), ставити діагноз та передавати його лікуючому лікареві, підтверджуючи його своїм ЕЦП записом в журналі телемедицини, згідно наказу МОЗ №681;

– пацієнт – доступ до системи через свій інтерфейс, подача особистих даних, зв'язок з лікуючим лікарем – має право здійснювати відео- та аудіозв'язок з лікуючим лікарем, подавати свою особисту інформацію, необхідну для постановки діагнозу, вимагати захисту своїх особистих даних від лікуючого лікаря та адміністратора, вимагати підтвердження особи лікуючого лікаря під час передачі даних (через ідентифікацію чи ЕЦП);

– лаборант – доступ до системи через власний інтерфейс, внесення даних в базу даних з підтвердженням своєї особи (через ідентифікацію чи ЕЦП), передача та отримання повідомлень від лікуючого лікаря.

b) Проведення аутентифікації лікарів-консультантів:

– для підтвердження особи лікаря-консультанта адміністратор може вимагати документи, які підтверджують кваліфікацію лікаря, а також час від часу здійснювати, крім ідентифікації, аутентифікацію;

– при здійсненні доступу користувачів до системи повинна здійснюватись їх ідентифікація.

3. Захист БД:

– гістологічні та цитологічні зображення зберігаються під зашифрованими номерами, відповідно до особи пацієнта, в незміненому стані;

– вся інформація про пацієнта зберігається в зашифрованому вигляді;

– доступ до БД здійснюється через ідентифікацію, відповідно до прав доступу.

4. Передача даних по мережі:

– ідентифікація лікуючого лікаря та лікаря-консультанта перед здійсненням консультації та передачі даних;

– гістологічні та цитологічні зображення передаються по мережі або записуються на віртуальний диск в незміненому вигляді без вказання прізвища та імені пацієнта;

– необхідна додаткова інформація передається в зашифрованому вигляді за допомогою симетричного чи асиметричного криптоалгоритму;

– лікар-консультант пересилає свій діагноз та рекомендації щодо лікування через електронну пошту з підтвердженням за допомогою ЕЦП.

На основі цих вимог розроблено інтелектуальну систему автоматизованої мікроскопії, яка є стійкою до атак.

Структура системи автоматизованої мікроскопії

Ключовою відмінністю пропонованої систем автоматизованої мікроскопії від існуючих аналогів є наявність адаптивного графічного інтерфейсу для різних типів користувачів та відповідно розподіл прав доступу до системи.

Основними групами користувачів телемедицини є лікуючий лікар, лікар-діагност, експерт, лаборант та адміністратор. Комунікація між ними відбувається за допомогою віддаленої бази даних та віддаленого FTP–сервера.

В УБД зберігається інформація про користувачів системи, досліди пацієнтів, кількісні та якісні характеристики зображень, заключення експерта та ін. В процесі роботи із пацієнтами важливим елементом системи є легування дій користувачів. Уся інформація про дії лікарів, яка доступна для перегляду адміністратору системи, знаходиться у базі даних. На FTP сервері розташовані зображення, отримані під час проведення досліджень. Для збереження конфіденційності даних пацієнтів уся інформація шифрується, тому зловмисник не зможе ідентифікувати приналежність зображення з певним діагнозом до конкретного пацієнта.

Лікарю – діагносту чи експерту не потрібно вручну вибирати директорію із зображеннями для подальшого перегляду. Система автоматично при виборі пацієнта та досліду створює локальну копію файлів на стороні клієнта (лікаря – діагноста, експерта). Видалення локальної копії зображень умисно чи з необережності не приведе до втрати усіх файлів конкретного дослідження.

Файли, відібрані для досліду, лікуючим лікарем також автоматично завантажуються на FTP сервер, а відповідна директорія з ними шифрується. Даний підхід значно спрощує інтерфейс користувача та дозволяє зосередитись лікарям лише на опрацюванні зображень.

База знань (БЗ) використовується для зберігання правил діагностування.

Узагальнену структуру розробленої САМ представлено на рис. 1.

Розподіл доступу та інтерфейси користувачів САМ

У процесі опрацювання гістологічних та цитологічних зображень та постановки діагнозу бере участь різна кількість лікарів та експертів [1]. Тому, налагодження комунікації та взаємодії між ними є складним та важливим завданням. Більшість з існуючих САМ не володіють спеціалізованим графічним інтерфейсом користувача для лікуючого лікаря, лікаря діагноста, лаборанта чи експерта. До того ж, процес обміну інформацією між користувачами

(лікарями) є непрактичним, а у деяких САМ взагалі відсутній.

Лікуючий лікар відіграє ключову роль в САМ. До його обов'язків входить:

1) перегляд та аналіз отриманих в результаті досліджень зображень;

2) попередня обробка зображень: покращення якості, фільтрація, виділення області інтересу (ROI), застосування морфологічних операцій, налаштування параметрів сегментації, контурний аналіз, обчислення кількісних характеристик ядер клітини;

3) постановка попереднього діагнозу;

4) збереження записів про дослід в БД;

5) обмін повідомленнями з іншими користувачами. Наприклад, лікуючий лікар може проконсультуватись з експертом щодо кожного окремого діагнозу.

Діаграму послідовності дій для лікуючого лікаря при роботі з розробленою САМ наведено на рис. 2.

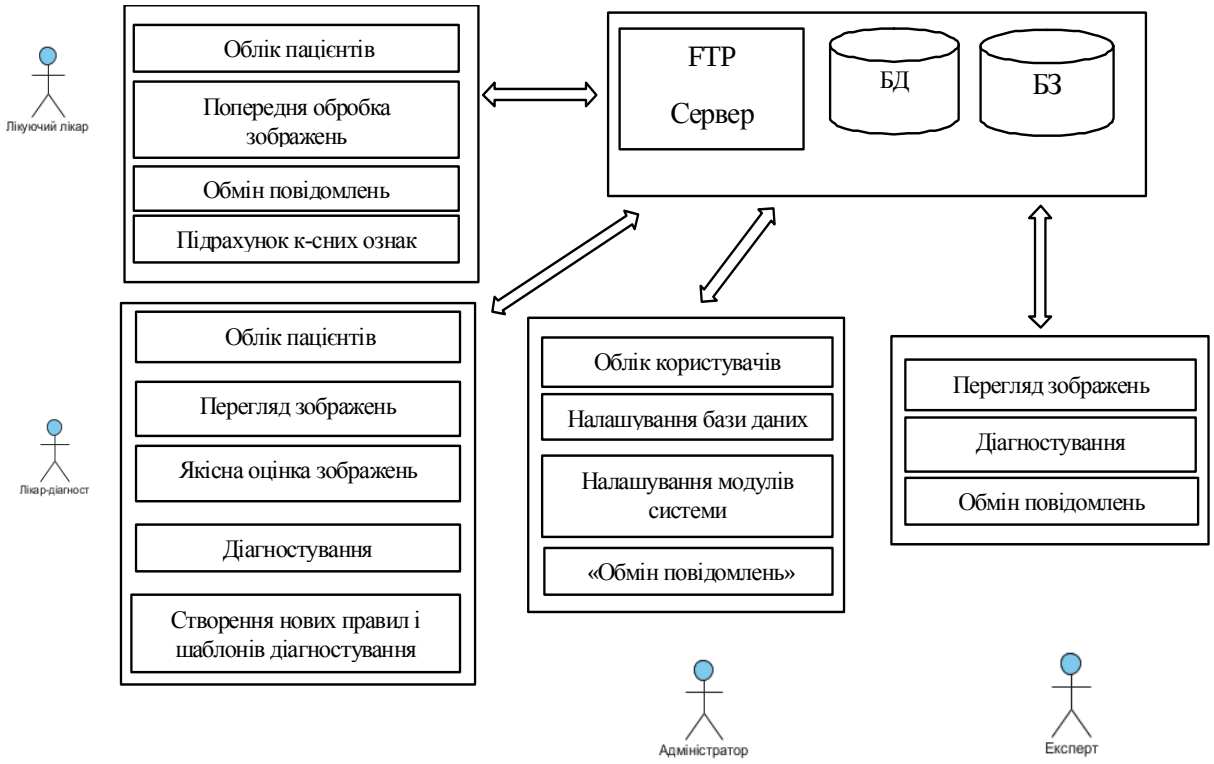


Рис. 1. Узагальнена структура розробленої САМ

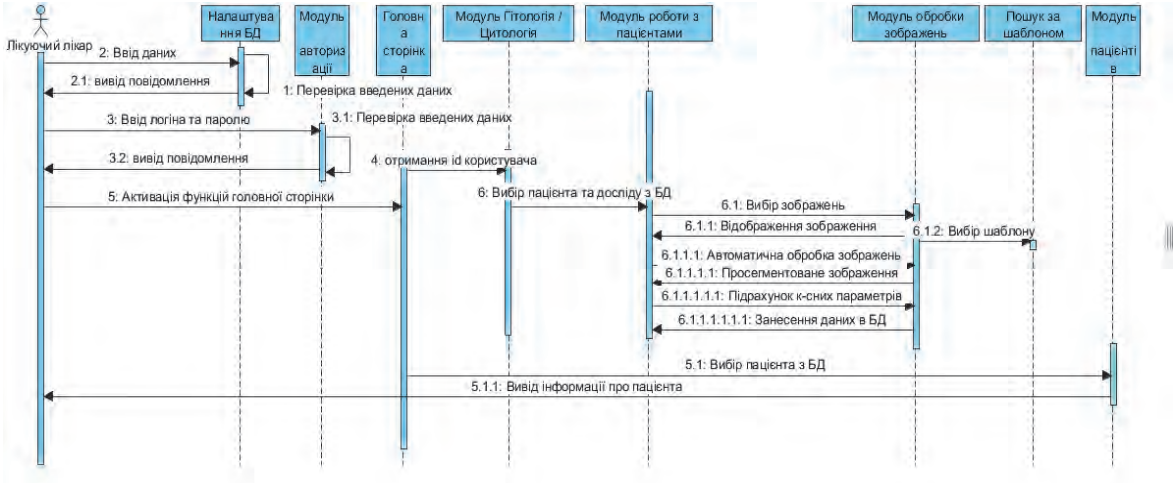


Рис. 2. Діаграма послідовності «Лікуючий лікар»

Першим кроком лікуючого лікаря для входу в систему є підключення до сервера бази даних. Користувач вказує сервер БД та логін і пароль для доступу до неї. Після успішного під'єднання до сервера користувач авторизується в системі, використовуючи власний обліковий запис. Якщо корис-

тувача ідентифіковано, САМ активує доступні для даного користувача модулі. Більшу частину роботи лікуючий лікар проводить з модулями «Пацієнт» та «Гістологія» або «Цитологія» для обробки зображень.

Основним завданням лікаря-діагноста є постановка кінцевого діагнозу, враховуючи напрацювання лікуючого лікаря та власний досвід. В процесі роботи лікар-діагност має доступ до наступних модулів:

1) перегляд результатів досліджень;
2) кількісна та якісна оцінка мікрооб'єктів на зображенні;
3) класифікація мікрооб'єктів;
4) спілкування з іншими учасниками, зокрема, з експертом;
5) створення нових шаблонів оцінки зображень;
6) постановка кінцевого діагнозу.

Діаграму послідовності дій для лікаря – діагноста наведено на рис. 3.

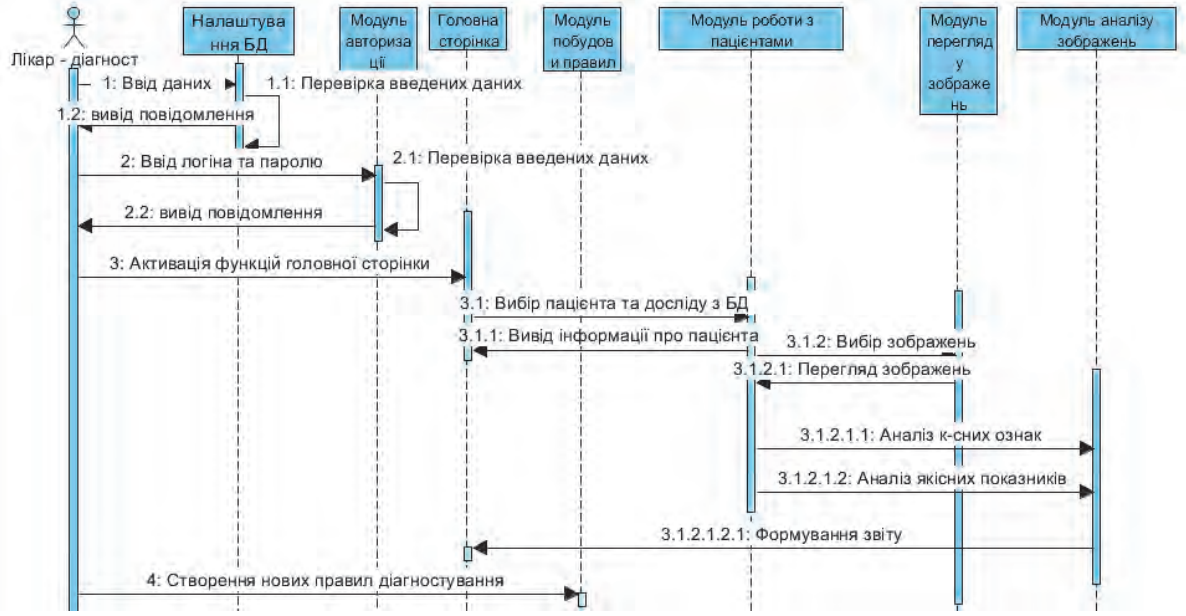


Рис. 3. Діаграма послідовності «Лікар-діагност»

Після процедури авторизації для даного типу користувача активізуються доступні модулі. У модулі «Пацієнти» лікар має можливість перегляду даних про досліди пацієнта та після аналізу встановлювати кінцевий діагноз. Інколи у медичній практиці виникають спірні питання, що потребують консультації експерта. За допомогою спеціального модуля діагност надсилає вибрані зображення експерту по мережі Інтернет за допомогою зручного інтерфейсу.

Завданням експерта у системі автоматизованої мікроскопії є надання консультацій для лікарів – діагностів. Діаграму послідовності для експерта наведено на рис. 4.

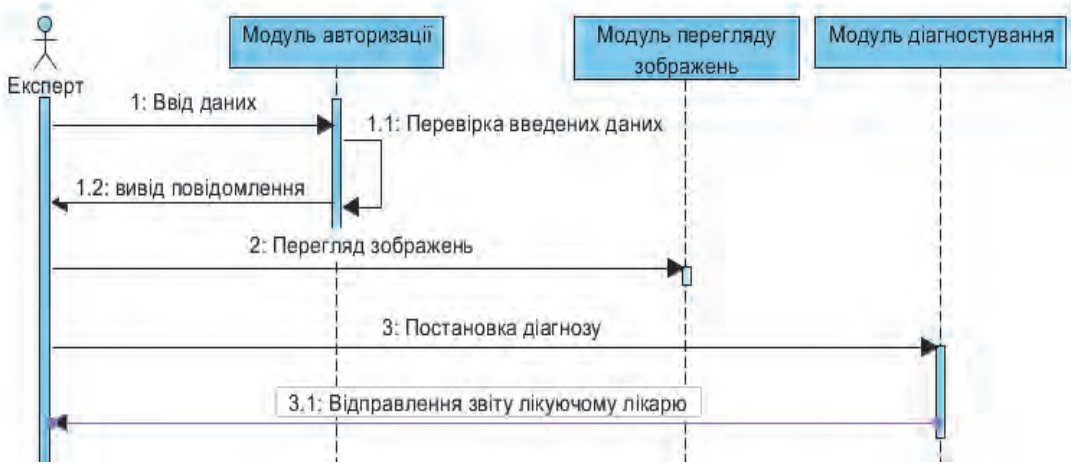


Рис. 4. Діаграма послідовності «Експерт»

Доступ до системи, на відміну від інших користувачів, надається через веб-інтерфейс. Передбачається, що експерт не обов'язково повинен знаходитись у лабораторії. Основною вимогою для роботи експерта є наявність облікового запису в системі та доступ до мережі Інтернет.

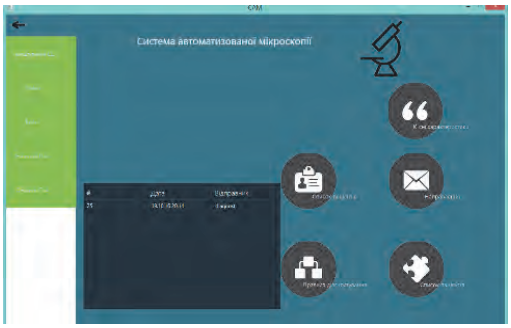
Порівняльний аналіз САМ

Призначенням САМ у медичних закладах є зменшення складності опрацювання зображень, підвищення продуктивності роботи лікарів та налагодження комунікації між окремими користувачами. Перші САМ складались лише із набору методів та алгоритмів обробки зображень [7–9]. У таких систем була відсутня база даних для зберігання інформації про досліди та пацієнтів.

Розроблена САМ характеризується наявністю адаптивних методів опрацювання зображень на усіх рівнях комп'ютерного зору. Наприклад, адаптивний модуль попередньої обробки зображень складається з модуля автоматичного налаштування параметрів фільтрації, коригування яскравості, контрастності, морфологічних операцій та модуля автоматичного налаштування алгоритмів сегментації. У системі також передбачено можливість ручної обробки зображень.

Приклад головної сторінки графічних інтерфейсів користувача для лікуючого лікаря та лікаря – діагноста наведено на рис. 5.

а – лікуючий лікар



б – лікар-діагност

Рис. 5. Графічний інтерфейс користувачів

Порівняльну характеристику існуючих та розробленої САМ наведено у табл. 1.

В результаті порівняльного аналізу систем автоматизованої мікроскопії можна зробити висновок, що розроблена САМ задовольняє усі вимоги до ПЗ обробки зображень та може успішно використовуватись у сучасних телемедичних системах.

Таблиця 1

Аналіз існуючих та розробленої САМ

Критерій	ImageJ	ImageProPlus	ДиаМорф	AxioVision	Розроблена САМ
Наявність рівнів доступу користувачів	-	-	-	-	+
Наявність БД	-	-	+	+	+
Автоматичні модулі обробки зображень	-	-	+/-	+/-	+
Наявність БЗ	-	-	-	-	+
Зберігання та архівування файлів	-	-	+	+	+
Адаптивний графічний інтерфейс	-	-	-	-	+
Захист від SQL ін'єкцій	-	-	-	-	+

Висновки

В даній статті авторами проведено аналіз політики безпеки сучасної телемедичної системи, виділено основні методи захисту інформації та вимоги до інтерфейсів користувачів.

Основною компонентою онкологічної телемедицини є система автоматизованої мікроскопії, тому розроблено САМ з окремими адаптивними інтерфейсами для чотирьох типів користувачів, що дозволило спростити роботу та комунікацію між лікарями з необхідним рівнем захисту інформації.

Застосування методів обробки та аналізу зображень дозволило підвищити ступінь автоматизації САМ та збільшити продуктивність роботи лікарів.

Дана робота розроблена в рамках держбюджетного проекту «Гібридна інтелектуальна інформаційна технологія діагностування передракових станів молочної залози на основі зображень». Реєстраційний номер 1016U002500.

Список літератури

1. *Владзимирский А.В. Телемедицина [монография] / А.В. Владзимирский. - Донецк: ООО «Цифровая типография», 2011. – 437 с.*

2. *Дубчак Л.О. Телемедицина: сучасний стан та перспективи розвитку / Л.О. Дубчак // Системи обробки інформації. – Х.: ХНУПС, 2017. – №1. – С.144-146.*

3. Васильцов І.В. Атаки спеціального виду на криптопристрої та методи боротьби з ними / І.В. Васильцов; за ред. В.П. Широчина. – Кременець: Видавничий центр КОГПІ, 2009. – 264 с.

4. Дубчак Л.О. Атаки на сучасні інформаційні системи та методи захисту проти них / Л.О. Дубчак // Materiály IX mezinárodnívědecko – praktická konference «Vědecký pokroknapřelomutysyachalety – 2013». – PrahaPublishingHouse «EducationandScience» s.r.o, 2013. - С. 3-5.

5. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; Под ред. В.Ф.Шаньгина. – М.: Радио и связь, 1999. – 328 с.

6. Абламейко С.В. Обработка изображений: технология, методы, применение: учебное пособие / С.В. Абламейко, Д.М. Лагуновский. – Минск: Амалфея, 2000. – 304 с.

7. Kraus B. High content analysis with axiovisionassaybuilder: applications in pharmaceutical biology / B. Kraus, H. Wolff // Biotechniques. – 2008. – №44. – P. 820-3.

8. Малов А.М. Компьютерная обработка биомедицинских многоканальных изображений с использованием визуализации меры сходства с эталоном / А.М. Малов // Известия вузов: приборостроение. – 2009. – №52(8) . – С. 74-79.

9. Березский О.Н. Информационная технология анализа и синтеза гистологических изображений в системах автоматизированной микроскопии / О.Н. Березский, Г.Н. Мельник // Управляющие системы и машины. – 2013. – № 4. – С. 26-32.

10. Vrekoussis T. Image analysis of breast cancer immunohistochemistry-stained sections using imagej: an rgb-based model / T. Vrekoussis, V. Chaniotis, I. Navrozoglou, V. Fousias, K. Pavlakis, E.N. Stathopoulos , O. Xoras // Anticancer research. – 2009. – № 29(12). – P. 4995-4998.

11. Медовый В.С. Информационные автоматизированные системы микроскопии для анализа биоматериалов. Врач и информационные технологии / В.С. Медовый // Медицина и высокие технологии. – 2004. – № 6. – С. 32-37.

Надійшла до редколегії 18.05.2017

Рецензент: д-р техн. наук ст. науков. співробітник С.В. Герасимов, Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків.

РАСПРЕДЕЛЕНИЕ ДОСТУПА В ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ АВТОМАТИЗИРОВАННОЙ МИКРОСКОПИИ

О.Н. Березкий, Л.О. Дубчак, О.И. Пицун

В данной статье рассмотрено современное состояние систем автоматизированной микроскопии и их применения в телемедицине. Анализ показывает, что разработка политики безопасности таких САМ является актуальной проблемой. Кроме того, выделены основные пользователи системы автоматизированной микроскопии и осуществлено распределение их прав доступа к информации. На основе проведенных исследований спроектирована и программно реализована интеллектуальная система автоматизированной микроскопии с адаптивным графическим интерфейсом различных типов пользователей для обработки биомедицинских изображений.

Ключевые слова: *система автоматизированной микроскопии, адаптивный графический интерфейс, биомедицинские изображения, политика безопасности, телемедицина.*

ALLOCATION OF INTELLECTUAL ACCESS SYSTEM AUTOMATED MICROSCOPY

O. Berezkij, L. Dubchak, O. Pitsun

In this article the current state of automated microscopy system and their applications in telemedicine. The analysis shows that the development of security policy itself is an actual problem. In addition, the main users of automated microscopy and carried out distribution of access rights to information had pointed. On the basis of the research the software had designed and automated intelligent microscopy responsive GUI for various types of users for processing of biomedical images had implemented.

Keywords: *automated microscopy, adaptive GUI, biomedical images, security policy, telemedicine.*