

## МОДУЛЬ АВТОРИЗАЦІЇ ТА АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ СИСТЕМИ АВТОМАТИЗОВАНОЇ МІКРОСКОПІЇ

Лящинський П.Б.<sup>1)</sup>, Лящинський П.Б.<sup>2)</sup>, Піцун О.Й.<sup>3)</sup>  
Тернопільський національний економічний університет  
<sup>1-2)</sup> студент; <sup>3)</sup> аспірант

### I. Постановка проблеми

Інформаційні системи (ІС) різного масштабу стали невід'ємною частиною базової інфраструктури держави, бізнесу, громадянського суспільства. З кожним разом, все більше інформації, що захищається, переноситься в ІС [1]. Особливо увагу захисту інформації надається в медицині, зокрема в системах автоматизованої мікроскопії. Оскільки, у таких системах зберігається особиста конфіденційна інформація про користувачів системи та пацієнтів. Механізм розподілу прав доступу, авторизації та автентифікації є складовою успішного та надійного функціонування багатокористувацьких систем. Системи автоматизованої мікроскопії широко застосовуються для аналізу гістологічних та цитологічних зображень [2].

### II. Мета роботи

Метою роботи є розробка алгоритму авторизації та автентифікації користувачів системи автоматизованої системи з подальшим розподілом прав доступу.

### III. Опис та структура модуля

Основою будь-яких систем захисту інформаційних систем є ідентифікація і автентифікація, так як всі механізми захисту інформації розраховані на роботу з поіменованими суб'єктами і об'єктами. В якості суб'єктів можуть виступати як користувачі, так і процеси, а в якості об'єктів - інформація та інші інформаційні ресурси системи. Присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора і порівняння його з заданим переліком називається ідентифікацією. Ідентифікація забезпечує виконання таких функцій: встановлення автентичності та визначення повноважень суб'єкта про його допуск в систему, контролювання встановлених повноважень, реєстрація дій і т.д.

Модуль розроблений за шаблоном проектування MVC (Model-View-Controller). Він побудований таким чином, що модифікація одного компоненту мінімально впливає на зміну будь-якого іншого. Це дозволяє змінювати певний клас без значних змін іншого.

Вікно для вводу даних користувача (логін та пароль) є стартовим для усієї системи. Модуль працює за таким алгоритмом:

1. зчитування введених даних з форм вводу;
2. перевірка даних на коректність за допомогою регулярних виразів;
3. підключення до СУБД MySQL;
4. порівняння перевірених даних з еталоном (автентифікація);
5. надання доступу до системи та розподіл прав (авторизація).

Для шифрування пароля було використано алгоритм md5 з додаванням "солі". Алгоритм MD5 є одним з алгоритмів шифрування на 128-бітній основі [3]. Під шифруванням розуміють перетворення вхідних даних за певним алгоритмом в бітовий рядок певної довжини. При цьому отриманий в ході обчислень результат представлений в шістнадцятковій системі числення, який є хешем, хеш-сумою або хеш-кодом [4]. Для кожного користувача, "сіль" є унікальним набором символів різної довжини. Тому, навіть при однакових паролях, хеш-сума буде різною.

Введені дані перевіряються так:

1. для введеного логіна (якщо такий існує) зчитується унікальний ключ;
2. відбувається конкатинація пароля з ключем;
3. отримана стрічка подається на вхід хеш-функції;
4. відбувається порівняння вихідної стрічки з паролем у базі;
5. в разі успіху відкривається головне вікно програми.

Загальна процедура ідентифікації і автентифікації користувача при його доступі в систему представлена на рисунку 1. Якщо в процесі автентифікації справжність суб'єкта встановлена, то

система захисту інформації повинна визначити його повноваження (сукупність прав). Це необхідно для подальшого контролю і розмежування доступу до ресурсів.

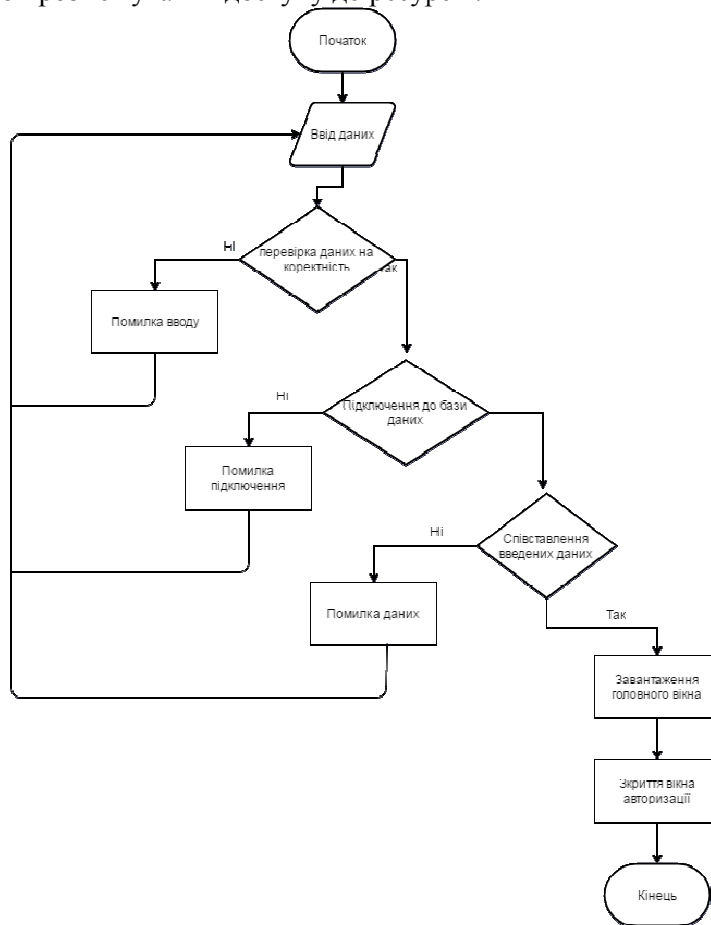


Рисунок 1 - Блок - схема роботи модуля авторизації

З метою аналізу розробленого модуля, наведено основні переваги його використання. Переваги є такі:

1. швидка інтеграція у будь-який Java FX додаток;
2. два ступені авторизації: автентифікація та надання прав доступу;
3. валідація введених даних у два кроки;
4. зручний інтерфейс користувача.

#### Висновок

За допомогою аналітичного підходу досліджено основні етапи авторизації та автентифікації користувачів в інформаційних системах, що дозволило реалізувати модуль для системи автоматизованої мікроскопії.

Розроблений модуль забезпечує конфіденційність користувачів та пацієнтів, що дозволяє підвищити надійність системи. Даний модуль розроблено на мові програмування Java з використанням Java FX Framework.

Даний модуль розроблений в рамках проекту «Гібридна інтелектуальна інформаційна технологія діагностування передракових станів молочної залози на основі аналізу зображень».

#### Список використаних джерел

1. Идентификация и аутентификация пользователя [Електронний ресурс] — Режим доступу: <http://goo.gl/b2LcQQ>
2. Berezsky O. Autometed Processing of Cytological and Histological Images / O. Berezsky, O. Pitsun // Proceedings of XII International Conference Perspective Technologies and methods in mems design - 2016. - pp. 51–53.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер . — М.: Триумф, 2003. - 806 с.
4. Мао В. Современная криптография: Теория и практика / В. Мао. — М.: Вильямс, 2005. — 768 с.