- неможливість уніфікації методик щодо кіберзахисту АСУ ТП, оскільки кожна конкретна система має свої особливості функціонування і свої вимоги до забезпечення кібербезпеки, які висуваються окремими компонентами або системою в цілому.

Зазначені особливості необхідно враховувати при розробці та впровадженні заходів забезпечення кібербезпеки автоматизованих систем управління технологічними процесами, які працюють на об'єктах критичної інфраструктури.

1. *Постанова* Кабінету Міністрів України від 23.08.16р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави». [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/ 563-2016-%D0%BF.
2. *Industrial* communication networks – Network and system security: IEC 62443. – Part 1-1: terminology, concepts and models.
3. *Кибератаки:* вирус – диверсант Stuxnet в ядерной энергетической программе Ирана. [Електронний ресурс]. Режим доступу: http://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html.
4. *Guide* to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.
5. *Домарев В.В.* "Безопасность информационных технологий. Методология создания систем защиты" – К.: ООО "ТИД "ДС", 2002. – 688 с.
6. *Гончар С.Ф.* Визначення актуальних загроз безпеці інформації в автоматизованих системах управління технологічними процесами / Гончар С.Ф. // Захист інформації. – 2015. – Том 17, № 3. – С.225-230.

Поступила 18.09.2017р.

УДК 004.932.2:616-006.6

Г.М. Мельник, Ю.М. Батько, Тернопіль

ОБ'ЄКТНА МОДЕЛЬ ГІБРИДНИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ АНАЛІЗУ БІОМЕДИЧНИХ ЗОБРАЖЕНЬ

Abstract. Oncology diagnostic systems are complex systems that combine computer vision and artificial intelligence methods. A large number of use cases are the cause of the complexity of developing a system. To develop the object model of the system, we used the Model-View-Presenter methodology. The object model of the software is evaluated.

1. Актуальність

При діагностуванні злоякісних новоутворень використовуються системи онкологічної діагностики. Системи онкологічної діагностики є складними системами, що поєднують методи комп'ютерного зору та методи штучного

інтелекту [1–3] і призначені для аналізу цифрових цитологічних і гістологічних зображень.

В останні роки найбільше поширення та розвиток під час проектування програмних систем та комплексів отримали об'єктно-орієнтований, компонентний та сервісно-орієнтовані підходи. Для роботи з ними були інструментальні засоби: Rational Rose, Rational Software, RUP, Demral, OOram тощо. Дані підходи формують основну групу методів проектування програмних систем, що застосовуються на практиці різними розробниками в залежності від поставлених задач. Окрім основної групи методів також використовуються математичні, алгебраїчні та логіко алгоритмічні підходи, методи формальної побудови систем тощо.

Більшість праць в області інженерії програмного забезпечення присвячено здебільшого принципам проектування архітектури веб орієнтованих додатків або додатків аналізу фінансової інформації. Складність розроблення концептуальної та об’єктної моделей автоматизованої системи онкологічної діагностики на основі зображень випливає з наступних факторів:

– наявність декількох ролей користувачів (акторів);
– наявність великої кількості прецедентів;
– комбінування методів комп’ютерного зору, методів штучного інтелекту, зокрема методів нечіткого виводу висновку;
– різнорідність даних в системі (зображення, ознаки класів мікрооб’єктів правила виводу, функції належності та ін.);
– наявність складного графічного інтерфейсу.

Одними із самих широковживаних сьогодні паттернів розробки архітектури є Model-View-Controller, Model-View-Presenter, Model-View-View-Model (MVVM), View-Interactor-Presenter-Entity-Routing (VIPER). Всі ці архітектури вимагають чіткого розділення програмної системи на шари: представлення, предметної області, даних. Шар представлення описує модель запиту до об’єктів шару предметної області і модель відповіді. Об’єкти цього шару повинні представляти вхідну на вихідну інформацію в спосіб не залежний від обраних бібліотек і фреймворків графічного інтерфейсу. Найкращим випадком є використання бібліотеки графічного інтерфейсу користувача як плагіна до розроблюваного ядра системи [4].

Ядро системи включає правила предметної області і сутності даних. Ці сутності розробляється окремо від модулів графічного інтерфейсу, модулів мережевої взаємодії чи модулів взаємодії з базою даних. Ядро системи можна представити об’єктами Інтерактор та Сутність (рис. 1). Об’єкт Інтерактор може відображати окремий прецедент.

На етапі аналізу потрібно сформулювати вимоги до програмного забезпечення, обмежити кількість акторів, розробити прецеденти, обрати паттерн розробки архітектури, розробити концептуальну модель автоматизованої системи. На етапі проектування потрібно розробити об’єктну модель програмного забезпечення.

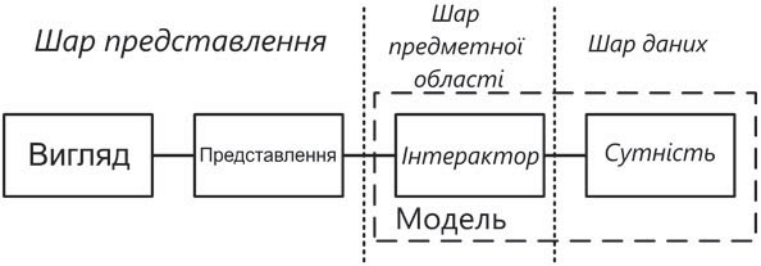

Рис. 1. Узагальнена архітектура програмного забезпечення автоматизованої системи

Постановка задачі полягає в розробленні прецедентів та узагальненої об'єктної моделі гібридної інформаційної системи аналізу біомедичних зображень.

2. Прецеденти для системи автоматизованої мікроскопії

Об'єктно-орієнтовані системи розглядаються як сукупність автономних і незалежних об'єктів, що взаємодіють між собою на різних рівнях. Зміна реалізації будь-якого об'єкта або додавання/корекції нових функцій не впливає на інші об'єкти системи. Чітка відповідність між реальними об'єктами (сутностями) та керуючими об'єктами програмної системи полегшує розуміння та реалізацію проекту [5, 6].

При використанні об’єктна-орієнтованого підходу під час проектування програмних систем використовують два основних типи моделей системної архітектури:

– статичні моделі, що описують статичну структуру системи в термінах класів об'єктів і взаємин між ними. Основними взаємовідносинами, що розглядаються на даному етапі, є відносини узагальнення, відносини виду ”використовують-використовуються” та структурні відносини;

– динамічні моделі. Дані моделі описують динамічну структуру системи та показують взаємодії між об'єктами системи (але не класами об'єктів).

Етап проектування є одним з головних під час розробки програмних систем та має замету забезпечити виконання таких задач:

– виділення основних сутностей, що описують предметну область;

– визначення основних полів, методів класів;

– теоретична перевірка правильності функціонування програмної системи та її модулів;

– усунення надлишкових зв’язків між окремими модулями системи;

– оцінка технічних вимог та функціональних характеристик майбутньої програмної системи.

Про проектуванні системи був використаний об’єктно-орієнтований

підхід. В основі даного підходу лежить об’єктна декомпозиція, що дозволяє провести попередню оцінку обраної структури. При аналізі предметної області було виділено 4 основних користувачі та 3 додаткових користувачі (рис. 2). Приведемо опис функції користувачів.

Адміністратор: встановлення, налаштування, модифікація наявних модулів, додавання, редагування, видалення користувачів системи, модифікації форм звітності, технічна підтримка ІС та бази даних, аналіз записів роботи системи та прогнозування можливих помилок, доступ до всіх функціональних модулів системи, наявність унікального ідентифікатора та ідентифікація в системі.

Лікар-діагност: отримання зображень, пошук інформації в БД, створення нових правил діагностування, створення нових шаблонних описів медичних об'єктів, редагування облікових карток пацієнта, постановка діагнозу, обмін повідомленнями, наявність унікального ідентифікатора та ідентифікація в системі.

Лікуючий лікар: отримання зображень, первинна обробка зображень, пошук інформації в БД, редагування облікових карток пацієнта, постановка діагнозу, обмін повідомленнями, наявність унікального ідентифікатора та ідентифікація в системі.

Лаборант: отримання зображень, пошук інформації, первинна обробка зображень, внесення інформації в БД зображень, ідентифікація в системі тільки при необхідності, доступ до модулів обробки зображень, обмін поштовими повідомленнями.

Даний набір Акторів та прецедентів дозволяє оцінити основні складові майбутньої системи, визначити майбутню структуру та множину класів для подальшої її реалізації.

3. Концептуальна модель системи

Відповідно до об’єктної моделі стандарту DICOM інтерфейс зокрема повинен забезпечити відображення та редагування даних про пацієнта, дослідження, серію біомедичних зображень, екземпляри біомедичних зображень). Додатково для кожного зображення потрібно представити (описати), атрибути зображення, клас мікрооб’єктів вибраного досліду та самі мікрооб’єкти вибраного класу, яким і будуть задаватися певні атрибути.

Моделювання знань на основі візуальної інтерпретації зображень і створення бази знань діагностичних ознак складний багатокроковий процес [7]. Він має такі кроки: опис мікрооб’єктів та їх якісних ознак, визначення числових ознак мікрооб’єктів, визначення нечітких змінних та побудова функцій належності, формалізація правил діагностування злоякісних новоутворень, побудова бази нечітких правил.

Основними мікрооб’єктами на цитологічному зображенні є клітина певної тканини органу, її складові частини а також групи клітин.

Для задоволення вимог персистентності системи і збереження інформації про пацієнта, зображень, отриманих із відповідного препарату,

кількісних ознак мікрооб'єктів розроблено базу даних [6]. Головна таблиця зберігає дані про пацієнта. Вона має зв'язки із таблицями для зберігання даних про дослідження та таблицею, що пов'язує серію зображень, розміщених в певному каталозі файлової системи із ідентифікатором дослідження. Окрема таблиця пов'язує зображення та набір виділених на ньому областей і їх числових ознак.

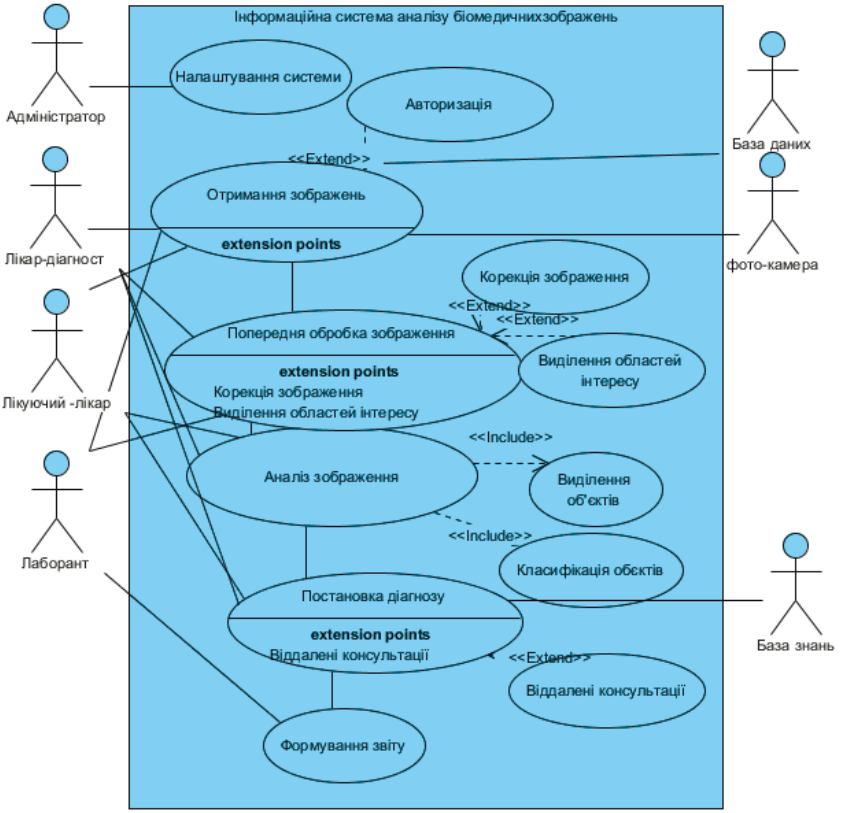

Рис. 2. Діаграма прецедентів інформаційної системи аналізу біомедичних зображень

Для опису мікрооб'єктів та їх якісних ознак потрібно формалізувати знання (досвід) експерта морфолога: логічні дерева рішень, мову опису клітин та діагнозу. Описові знання можна представити у вигляді спеціальної онтології опису клітин, яка містить всю інформацію про морфологію ракових клітин. Структурована та ієрархічна онтологія складається з усіх значних морфологічних характеристик, які розглядаються окремо. Для кожної характеристики (наприклад, розмір ядра) необхідно зафіксувати якісні

значення категорій, які можна присвоїти цій ознаці (наприклад, дуже малий, малий, середній або великий). Узагальнена об'єкта модель автоматизованої системи зображена на рис. 3.

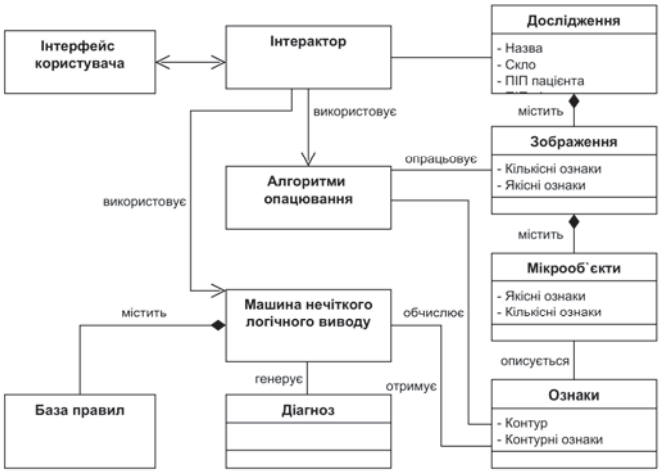

Рис. 3. Об'єктна модель програмного забезпечення системи

Підсистема набуття знань призначена для перегляду уже зроблених досліджень, яка дозволяє переглянути зображення цих дослідів та усі виділені мікрооб'єкти на зображенні. Людина-експерт може охарактеризувати зображення та виділені мікрооб'єкти у вигляді атрибутів або якісних категорій.

Інтерфейс системи повинен відображати інформацію про: пацієнта, дослід вибраного пацієнта, зображення і клас мікрооб'єктів вибраного досліду та самі мікрооб'єкти вибраного класу, яким і будуть задаватися певні атрибути. Вибраному зображенню теж можуть задаватися атрибути або якісні категорії.

Узагальнена об'єктна модель машини нечіткого логічного складається із об'єкта обчислення числових ознак, об'єкта – агрегатора числових ознак, об'єкта фазифікації, об'єкта – агрегатора правил діагностування, об'єкту функцій належності, об'єкта нечіткого логічного виводу, об'єкта дефазифікації та об'єкта постановки діагнозу. Нечіткий логічний вивід працює в двох режимах:

1) отримання знань;

2) постановки попереднього діагнозу (класифікації).

В режимі отримання знань агрегатор правил діагностування заносить правила діагностування в нечіткій формі, які отримані від експертів (цитолога та гістолога). Крім цього об'єкт функцій належності заповнюється конкретними параметрами функцій належності.

У режимі постановки діагнозу об’єкт обчислення числових ознак зчитує цитологічні та гістологічні зображення, в якому обчислюються відповідно цитологічні та гістологічні ознаки, що утворюють множину вхідних ознак, яка записується в агрегаторі числових ознак. На основі числових ознак ідентифікуються функції належності. Використовуючи множину числових ознак і їх функції належності, об’єкт фазифікації утворює нечітку множину вхідних ознак. Об’єкт нечіткого логічного виводу на основі множини правил та множини ознак, виводить (inference) нечітку множину діагнозів. Об’єкт дефазифікації переводить нечітку множину діагнозів у множину діагностичних ознак із відповідними ваговими коефіцієнтами кожного правила.

Правило діагностування має наступну форму:

IF розмір_клітини = дрібний AND форма_клітини=кубічна TO діагноз=нормальна

Ознака «розмір клітини» задано терм-множиною: дрібний (small), збільшений (enlarged), гігантський (giant). На етапі набуття знань для кожного терму обчислено мінімальне і максимальне значення а також параметри нормального розподілу.

4. Оцінка моделі програмної системи

При аналізі об’єктно-орієнтованих моделей розглядаються та оцінюють множину класів, їх структуру та взаємозв’язки між ними. Для проведення оцінки програмних засобів часто використовуються характеристики та атрибутів, які оформлені у вигляді стандарту ISO 9126 – «Інформаційна технологія. Оцінка програмного продукту. Характеристики».

Для аналізу структури системи можна використовують метрики Чідамбера та Кемерерома. Метрики застосовують до окремих класів з метою виявлення тих, які можуть містити найбільшу кількість помилок. Нижче перераховано найпоширеніші метрики.

Зважена насиченість класу методами (WMC – Weighted methods per class) – визначає відносну міру його складності; якщо вважати, що всі методи мають однакову складність, то це буде просто число методів в класі:

$$WMC = \sum_{i=1}^{n} c_i ,$$

де c_i – складність i -го методу, що обчислюється за деякою метрикою.

Глибина дерева успадкування (Depth of Inheritance tree) – кількісні характеристики форми та розміру структури класів.

Число нащадків (Number of children) – кількісна міра, що характеризує кількість класів-нащадків для кожного з класів.

Зчеплення об'єктів (Coupling between object classes) – міра їх взаємозалежності.

Передача зв'язуючих повідомлень (Message Passing Coupling) – цей показник вимірює кількість повідомлень, що проходять між об'єктами класу.

Відгук на клас (RFC – Response for a class) – кількість методів, які можуть викликатися екземплярами класу:

$$RFC = |RS|,$$

$$RS = M_i \cup_{all\ \ i} \{R_i\}, i = 1..n,$$

де M – кількість методів класу;

R_i – кількість методів, які можуть бути викликані i -тим класом;

n – кількість класів.

Недолік зв'язності в методах (LCOM – Lack of cohesion in Methods) – характеризує спільне використання даними в середині класу:

$$LCOM = |P| - |Q|,$$

де P – множина пар методів, що не мають спільних змінних;

Q – множина пар методів, що мають спільних змінних.

Для оцінки концептуальної моделі спроектованої автоматизованої системи проведемо аналіз її структури на основі діаграми класів та множини характеристик розглянутих вище. Аналіз окремо кожного класу наведено в таблиці 1.

Таблиця 1

Оцінка головних класів системи

Номер класу	Інтерактор	Об'єкт опрацювання	Дослідження	Зображення	МНЛВ	Середнє значення
Кількість методів	12	17	15	18	19	13
Кількість атрибутів	57	52	35	20	35	30
Кількість нащадків	2	10	2	3	5	4
Кількість звернень	150	102	180	200	30	132

Висновки

Аналіз даних характеристик проілюстрував складність абсолютної автоматизації процесу оцінки складності моделі, тому що в кожному конкретному випадку необхідно враховувати особливості поставлених задач і способи їх реалізації у взаємодії окремих підсистем/класів/підкласів/функцій.

1. *Berezsky O.* Methods and Algorithms of Biomedical Image Transforms in Affine and Topological Spaces // International Journal of Advanced Information Science and Technology (IJAIST) – 2016. – Vol. 10, № 5. – P.1-10.
2. *Berezsky O.* An intelligent system for cytological and histological image analysis / O. Berezsky, G. Melnyk, T. Datsko, S. Verbovy // 13th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2015 – Lviv, 2015. – P.28-31.
3. *Berezsky O.* Fuzzy System of Diagnosing in Oncology Telemedicine / O. Berezsky, S. Verbovyy, L. Dubchak, T. Datsko // Sensors & Transducers – 2017. – № 208. – P.32-38.
4. *Мельник Г.М.* Метод знаходження відповідних точок на контурах мікрооб'єктів біомедичної природи // Вісник Національного університету "Львівська політехніка" "Комп'ютерні науки та інформаційні технології" – 2012. – № 732. – С.343-350.
5. *Мельник Г.М.* Інформаційна технологія аналізу структурних текстур для опрацювання зображень ауто- та ксеногенних тканин //Вісник Хмельницького національного університету – 2014. – № 6 (217). – С.132-141.
6. *Мельник Г.М.* Зменшення простору текстурних ознак гістологічних зображень за допомогою методу головних компонент / Г. М. Мельник // Моделювання та інформаційні технології. Збірник наукових праць. – 2016. – № 77. – С.176-180.
7. *Батько Ю.М.* Аналіз контурних ознак мікрооб'єктів на цифрових кольорових біомедичних зображеннях / Ю.М. Батько // Моделювання та інформаційні технології. – 2016. – Вип. 76. – С.184-190.

Поступила 14.09.2017р.

УДК 511:003.26.09

С.Д. Винничук, В.М. Міський, Київ

ПРИСКОРЕННЯ МЕТОДУ КВАДРАТИЧНОГО РЕШЕТА НА ОСНОВІ ВИЗНАЧЕННЯ ДОСТАТНЬОЇ КІЛЬКОСТІ B-ГЛАДКИХ ЧИСЕЛ

Abstract. The quadratic sieve method is the fastest for integers under 100 decimal digits or so. This paper describes the method which allows to stop sieving with less number of B-smooth than basic Quadratic Sieve method. This fact reduces complexity of sieving part, building and resolving matrix.

Вступ

На сьогоднішній день криптоалгоритм RSA реалізовано у багатьох комерційних системах. Він використовується у web серверах та браузерах для захисту трафіку, у електронній пошті для забезпечення конфіденційності та автентичності, та є ключовою технологією у системах електронних платежів. Найбільш поширена атака на цей криптоалгоритм заснована на факторизації публічного ключа [7,8]. Якщо факторизація успішна, усі повідомлення зашифровані відкритим ключем можуть бути прочитані.

