СПб. – 2001. – 464 с. 9. Параллельная обработка информации: Т.4. Высокопроизводительные системы параллельной обработки информации / Под ред. В.В. Грицыка. – К.: Наук. думка, 1988. – 272 с. 10. Самофалов К.Г. и др. Прикладная теория цифровых автоматов. – К.: Вища школа, 1987. – 375 с. 11. Грушицкий Р.И., Мурсаев А.Х., Угрюмов Е.П. Проектирование систем на микросхемах программируемой логики. – СПб.: БХВ-Петербург, 2002. – 608 с. 12. Каневский Ю.С. Систолические процессоры. – К: Техніка. – 1991. – 173 с. 13. Шалыто А.А. Методы аппаратной и программной реализации алгоритмов. – СПб.: Наука, 2005. – 780 с. 14. Ткаченко Р.О., Цмоць І.Г., Скорохода О.В. Вертикально-паралельні методи та структури для реалізації базових компонентів нейромережевих технологій реального часу // Технічні вісті. – 2010/1(31), 2(32). – С.166–169. 15. Грицик В.В., Ткаченко Р.О., Цмоць І.Г. Технологія нейрокомп'ютингу реального часу // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні науки та інформаційні технології". – 2010. – № 672. – С.359–371.

УДК 004.89

В. Литвин
Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДІАГНОСТУВАННЯ РЕВМАТОЛОГІЧНИХ ЗАХВОРЮВАНЬ НА ОСНОВІ АДАПТИВНИХ ОНТОЛОГІЙ

Розглянуто побудову інтелектуальної системи підтримки прийняття рішень діагностування ревматологічних захворювань. Для функціонування такої системи розроблено математичний апарат на основі адаптивних онтологій.
Ключові слова: онтологія, концепт, відношення, інтерпретація.

In the paper the design of the decision support diagnosing rheumatic diseases. For the operation of the system developed mathematical tools based on adaptive ontologies.
Keywords: ontology, concept, relation, interpretation.

Постановка проблеми у загальному вигляді

Технологія інтелектуальних систем підтримки прийняття рішень (ІСППР) є одним із найрозвинутіших напрямків штучного інтелекту. Дослідження у цій області полягають у розробленні автоматизованих інформаційних систем, які застосовуються у тих областях діяльності людини, які вимагають логічного міркування, певної майстерності та досвіду.

Сучасний рівень розвитку ІСППР відбувається у двох напрямках розроблення інтелектуальних агентів (ІА) [1]:

- ІА, засновані на прецедентах (англійською – Case-Based Reasoning, або CBR);
- ІА планування діяльності (пошук у просторі станів).

Вибір ІА залежить від задачі. Метод виведення за прецедентами ефективний, коли основним джерелом знань про задачу є досвід, а не теорія; рішення не є унікальними для конкретної ситуації, а можуть бути використані в інших випадках; метою розв'язування задачі є отримати не гарантований правильний розв'язок, а кращий з можливих. Виведення, засноване на прецедентах, є

методом побудови ІСППР, які приймають рішення щодо цієї проблеми або ситуації за наслідками пошуку аналогій, що зберігаються в базі прецедентів [2]. Такий прецедент називають релевантним. З математичного погляду серед елементів множини прецедентів $Pr=\{Pr_1, Pr_2,\ldots, Pr_N\}$ релевантним Pr_k є прецедент, для якого відстань до поточної ситуації S є найменшою, тобто

$$Pr_k = \arg\min_i d(Pr_i, S).$$

ІА планування діяльності має досягти цільового стану. Насамперед він повинен побудувати план досягнення цього стану із всіма можливими альтернативами. Процес планування ґрунтується на декомпозиції. Задача планування ZP містить три складові [3]: множину станів *St*, множину дій *A*, множину цільових станів *Goal* (станів мети); тобто

$$ZP = \langle St, A, Goal \rangle.$$

Отже, для планування діяльності ІА повинен вміти оцінювати стани та дії.

Як бачимо, для обох класів ІСППР необхідна метрика. У першому випадку для оцінювання релевантності прецедентів, у другому випадку – для оцінювання релевантності станів. Від способу визначення цієї метрики напряму залежить ефективність роботи ІА. На наш погляд, такий спосіб має ґрунтуватися на чіткому і аргументованому стандарті баз знань. У галузі інженерії знань таким стандартом стали онтології [4]. Тому нами запропоновано для побудови метрики використовувати онтології.

Під моделлю онтології *O* розуміють трійку вигляду:

$$O = \langle C, R, F \rangle,$$

де *C* – поняття, *R* – відношення між поняттями, *F* – інтерпретація понять та відношень (аксіоми). Аксіоми встановлюють семантичні обмеження для системи понять та відношень.

Аналіз останніх досліджень та публікацій

Сьогодні розрізняють три типи онтологій: предметно-орієнтовані (Domain-oriented), орієнтовані на прикладну задачу (Task-oriented) та загальні онтології (Top-level). У нашій роботі, використовуючи термін “онтологія”, ми вважатимемо, що вона містить всі три типи.

Рис. 1. Класи задач для розв’язування яких використовують ІСППР

Проаналізувавши клас задач, для яких розробляють ІСППР, можна зробити висновок, що всі задачі можна поділити на два підкласи. Існує клас задач, для яких істотне значення понять (властивостей). Це задачі діагностики захворювань, розпізнавання образів, класифікація явищ на основі збирання даних тощо. Такі задачі назвемо ознаковими. Для іншого класу задач не є істотним

значення понять, а скоріше – їх семантика або частотність знаходження термінів у тексті і т.д. Це кластеризація інформаційних ресурсів, класифікація текстів згідно з УДК, інтелектуальні пошукові системи, реферування та анотування текстових документів. Такий клас задач назвемо семантичними задачами. У результаті отримаємо поділ ІСППР за двома вимірами, як це зображено на рис. 1. У кожній чверті перераховано окремі задачі, які потрапляють у відповідний клас.

Для ефективного функціонування ІА необхідно побудувати метрику, на основі якої визначати релевантність станів чи прецедентів. На наш погляд, побудова такої метрики напряму залежить від класу задач: семантичні вони чи ознакові.

Отже загалом, на нашу думку, виділяють чотири різні класи задач, які розв'язують ІСППР. Зріз за напрямами потребує двох різних функціональних моделей (пошук релевантних прецедентів та планування діяльності), зріз за типом задачі – використання двох різних метрик для розв'язування цих задач та оцінювання якості отриманих розв'язків. Побудову ІСППР на основі онтологій для розв'язування семантичних задач нами детально розглянуто у роботах [5–7]. Тому у цій роботі детально розглянемо ІСППР для ознакових задач, яка ґрунтується на прецедентух, а саме для діагностування ревматологічних захворювань.

Формування цілей

Побудувати метрику для оцінювання релевантності прецедентів для ознакових задач. Апробувати цю метрику під час функціонування прикладної ІСППР діагностування ревматологічних захворювань.

Основний матеріал

1. Поняття адаптивної онтології

Ефективність адаптації онтології бази знань до особливостей предметної області визначають закладені в її структуру елементи та механізми її адаптації шляхом самонавчання під час експлуатації. Одним з підходів до реалізації таких механізмів є автоматичне зважування понять бази знань та семантичних зв'язків між ними під час самонавчання. Цю роль беруть на себе коефіцієнти важливості понять та зв'язків [5]. Коефіцієнт важливості поняття (зв'язку) – це чисельна міра, котра характеризує значущість певного поняття (зв'язку) у конкретній предметній області і динамічно змінюється за певними правилами у процесі експлуатації системи. Отже, ми розширимо поняття онтології, ввівши в її формальний опис коефіцієнти важливості понять та відношень. Тому таку онтологію ми будемо визначати як п'ятірку:

$$O = \langle C, R, F, W, L \rangle,$$

де W – важливість понять C, L – важливість відношень R.

Визначену таким чином онтологію називатимемо адаптивною, тобто такою, що адаптується до ПО за рахунок модифікації понять та коефіцієнтів важливості цих понять і зв'язків між ними. Така онтологія однозначно представляється у вигляді зваженого концептуального графу (КГ) [8]. Отже, до складу адаптивної онтології входять скалярні величини, які використаємо для побудови метрики.

2. Побудова метрики для прецедентів у просторі ознак

Очевидно, що залежно від прецеденту ваги понять різні. Тобто насправді W – вектор вимірності кількості прецедентів $W=(W_1,W_2,\ldots,W_N)$. Надалі будемо розглядати лише один прецедент, тобто нижній індекс у вазі понять опускаємо.

Побудуємо метрику для ознакових задач, які використовують прецеденти.

Нехай множина прецедентів $\mathrm{Pr}=\{\mathrm{Pr}_1,\mathrm{Pr}_2,\ldots,\mathrm{Pr}_N\}$ описується характеристиками (властивостями) $X=\{x_1,x_2,\ldots,x_M\}$. D_i – домен властивості x_i, w_{i_i} – коефіцієнт важливості властивості x_{i_i} прецеденту Pr_i. Значення властивості x_i позначатимемо $z_i = z(x_i)$. Отже

$$\mathrm{Pr}_i \leftrightarrow X_i = \left\{ x_{i_1} = z_{i_1}, x_{i_2} = z_{i_2}, \ldots, x_{i_k} = z_{i_k} \right\}, \text{ де } z_{i_j} \in D_{i_j}.$$

Позначимо I_i як множину індексів властивостей прецеденту Pr_i Тоді відстань між прецедентом Pr_i та поточною ситуацією S визначається як:

$$d_i = \sum_{i_l \in \overline{I}_i} j\left(z_{i_l}, z_{i_l}^S\right), \tag{1}$$

де z_{i_l} значення властивості x_{i_l} прецеденту Pr_i, $z_{i_j}^S$ – значення властивості x_{i_l} поточної ситуації S, $\overline{I}_i$ – множина індексів важливих властивостей прецеденту Pr_i, $\overline{I}_i = \overline{I}_{i1} \cup \overline{I}_{i2} \cup ... \cup \overline{I}_{iN_i}$, N_i – кількість властивостей, які необхідно розглянути, щоб прийняти рішення стосовно прецеденту Pr_i. Тобто

$$\overline{I}_{i1} = \left\{ i_{s1} \middle| i_{s1} = \arg\max_{i_l \in I_i} w_{i_l} \right\}, \quad \overline{I}_{i2} = \left\{ i_{s2} \middle| i_{s2} = \arg\max_{i_l \in I_i / i_{s1}} w_{i_l} \right\}, \quad \overline{I}_{i3} = \left\{ i_{s3} \middle| i_{s3} = \arg\max_{i_l \in I_i / i_{s1} / i_{s2}} w_{i_l} \right\}, \ldots$$

Розглянемо функцію $j(x,h)$. Очевидно, що x може бути діапазоном, тобто нечіткою підмножиною $x \subseteq D$, де D – універсальна множина; числовим значенням або нечисловим значенням. Залежно від цього $j(x,h)$ визначається по-своєму, а саме:

$$j(x,h) = \begin{cases} 1 - m_x(h), & x - \text{нечітка множина}, \\ l \cdot |x - h|, & x,h - \text{числові значення}, \\ 1 - m(x,h), & x,h - \text{нечислові значення}, \end{cases} \tag{2}$$

де $m_x(h)$ – коефіцієнт впевненості в тому, що h належить нечіткій підмножині x; l – числова величина, яка залежить від ПО, щоб добуток $l \cdot |x - h| \in [0,1]$ (розмірність величини l обернено-пропорційна до розмірності величин x та h, тобто, якщо x та h є маса і вимірюється в кг, то l вимірюється в кг$^{-1}$); $m(x,h) \in [0,1]$ – нечітка величина подібності значень x та h. Наприклад, $m(x,h) = 1$, якщо $x = h$, $m(x,h) = 0{,}9$, якщо $x \approx h$, $m(x,h) = 0$, якщо $x \neq h$.

Розглянемо визначення ваг понять для ознакових задач на основі інтелектуального аналізу даних, а саме на основі побудови дерева рішень (ДР). Як відомо, ознакові задачі дають змогу для пошуку релевантних прецедентів будувати ДР [9]. Однак ДР не є панацеєю, оскільки згадувані ознаки, що лежать на відповідній гілці, що задає прецедент, не гарантують врахування повної множини ознак, які необхідно врахувати для знаходження релевантного прецеденту. Нами пропонується використовувати ДР для визначення ваг базових термінів, які задають деякий прецедент, а потім на основі онтології ПО розвинути отримані ваги на всю онтологію для відповідного прецеденту. Тоді для пошуку релевантного прецеденту використовувати значення тих n понять, які для відповідного прецеденту мають найбільші ваги.

Розглянемо гілку дерева рішень. Вершини (ознаки) цієї гілки знаходяться на k рівнях. Очевидно, що чим вищий рівень, тим значуща ознака, яка на цьому рівні знаходиться. Ця евристична думка має бути відображена в значеннях ваг цих ознак. Крім того, пропонується ці ваги нормувати, тобто щоб їх сума для кожного прецеденту (гілки) дорівнювала 1.

Розглянемо два способи визначення ваг базових ознак, які задовольняють вищеописані два припущення.

1 спосіб. Арифметичний. Визначаються як відношення різниці (k+1) рівня дерева та рівня, на якому знаходиться ознака до суми всіх рівнів гілки, тобто ґрунтуються на сумі арифметичної прогресії:

$$w_i = \frac{k+1-i}{\sum_{j=1}^{k} j} = \frac{k+1-i}{\frac{(1+k)k}{2}}$$

2 спосіб. Геометричний. Ґрунтуються на сумі геометричної прогресії:

$$w_i = \frac{2^{k-i}}{2^k - 1}.$$

Отримані на основі ДР ваги назвемо вагами базових ознак прецеденту і позначимо таку множину ваг W_B. Тепер необхідно їх розвинути на всю онтологію ПО, використовуючи таксономію понять онтології, відношення між поняттями та їх інтерпретацію. Математично (формально) цей процес запишемо у вигляді:

$$W_B \xrightarrow{O} W. \quad (3)$$

Для ознакових задач нами пропонується такий метод розповсюдження ваг. Спочатку ваги всіх ознак дорівнюють 0. Вважаємо, що вага вертикальних зв'язків (ієрархія, агрегація) дорівнює 1,2 (чим конкретніше, тим краще). Для ознак, які беруть участь у дереві рішень для відповідного прецеденту до нуля додаємо вагу, отриману на основі дерева рішень. Потім розглядаємо функціональні та семіотичні зв'язки, якщо вони визначені в онтології.

Для ознакових задач квантатативні відношення не розглядаються, оскільки синонімія та корелювання ніяк не впливають на значення ознак. Відразу вважається, що це одна і та сама ознака. Кваліативні функціональні відношення поділяють на симетричні R_S (деяка підмножина горизонтальних зв'язків) та несиметричні R_N (вертикальні зв'язки, інша підмножина горизонтальних зв'язків). Те, що елементи містять між собою симетричний зв'язок, позначатимемо подвійною стрілкою $C_i \leftrightarrow C_j$, несиметричний – одинарною від області визначення в множину значень $C_i \rightarrow C_j$.

Очевидно, що елементи, які беруть участь у симетричних зв'язках, є рівносильними. Тому ваги L симетричних відношень дорівнюють одиниці. Таким симетричним зв'язком є „Об'єкт дії↔дія↔суб'єкт дії", який належить до групи функціональних зв'язків. Всі інші функціональні зв'язки є близькими до симетричних, тому їх ваги дорівнюють 0,9. Отже, якщо відома вага W_i терміна C_i і цей термін має симетричний зв'язок із терміном C_j, вага якого невідома, то $W_j = L \cdot W_i$. Для несиметричних зв'язків $C_i \rightarrow C_j$ отримаємо аналогічне співвідношення

$$W_j = L \cdot W_i, \quad (4)$$

якщо відома вага C_i і

$$W_i = \frac{W_j}{L}, \quad (5)$$

якщо відома вага C_j. Семіотичні відношення мають вагу 0,2. У табл. 1 наведено значення ваг важливості різних груп відношень для різних задач. Стовпчик значення ваг для семантичних задач нами визначено у роботі [10].

Таблиця 1

Ваги важливості відношень

Група відношень	**Відношення**	**Значення ваг важливості *L***	
		Для семантичних задач	**Для ознакових задач**
1	2	3	4
Ієрархія	Рід↔вид	*0,9*	*1,2*
	Ознака↔значення ознаки	*0,9*	*1,2*
	Інваріант↔варіант	*0,9*	*1,2*
Агрегація	Ціле↔частина	*0,9*	*1,2*
	Об'єкт↔простір реалізації (локалізації) об'єкта	*0,4*	*1,2*
	Об'єкт↔властивість/ознака	*0,4*	*1,2*
	рівень↔одиниця рівня	*0,4*	*1,2*

Продовження табл. 1

1	2	3	4
Функціональні	Об'єкт дії↔дія↔суб'єкт дії	*0,3*	*1*
	причина↔наслідок	*0,3*	*0,9*
	умова↔дія	*0,3*	*0,9*
	явище↔дія	*0,3*	*0,9*
	стан↔дія	*0,3*	*0,9*
	явище↔стан	*0,3*	*0,9*
	інструмент↔дія	*0,3*	*0,9*
	дані↔дія	*0,3*	*0,9*
	дані↔величини	*0,3*	*0,9*
Семіотичні	Термін↔спосіб вираження	*0,2*	*0,2*
	Термін↔спосіб подання	*0,2*	*0,2*
	Термін↔метазнак терміна	*0,2*	*0,2*
Тотожності	Термін↔синонім терміна	1	-
Кореляції	Термін↔корелят терміна	1	-

Отже, загалом процес функціонування ІСППР на основі онтологій складається із кроків, наведених на рис. 2. Для їх зображення використано діаграму діяльності (UML Activity) [11].

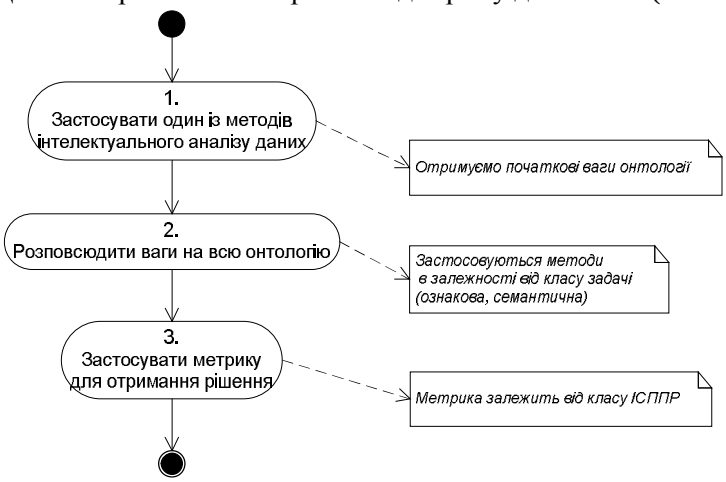


Рис. 2. Діаграма діяльності ІСППР на основі адаптивних онтологій

ІСППР діагностування ревматологічних захворювань

Розглянемо приклад функціонування ІСППР у галузі медицини, а саме – ревматології. Як прецеденти ми розглянули сім захворювань: Pr={'Ревматоїдний артрит (РА)', 'Деформуючий остеоартроз (ДО)', 'Системний червоний вовчак (СЧВ)', 'Анкілозуючий спондиліт (АС)', 'Гостра ревматична лихоманка (ГРЛ)', 'Подагричний артрит (ПА)', 'Системна склеродермія (СС)'}. Нами виділено 27 ознак, які супроводжують ці захворювання. Наведемо деякі з них: *X*={*Симетричний поліартрит дрібних суглобів кистей рук, Звуження суглобової щілини, Остеофіти, Біль у суглобах при фізичному навантаженні, Феномен Рейно, Експресія HLA-D27 антигену, Виявлення LE-клітини у крові*}. Очевидно, що не всі ознаки присутні в окремо взятому захворюванні. Тому залежно від прецеденту важливість цих ознак різна. Саме таку вагу важливості нам необхідно визначити, щоб для діагнозу використати формулу (1). Детальніше домени ознак розглянемо, коли визначатимемо вагу їх важливості.

Використовуючи різні ревматологічні довідники, ми побудували онтологію ревматології. В онтології відображено взаємозв'язок між ознаками, їх вплив на захворювання залежно від значення

ознаки. Використовуючи цю онтологію, визначимо вагу важливості цих ознак залежно від захворювання. Насамперед обчислимо початкові вагові коефіцієнти. Для цього побудуємо дерево рішень (ДР) на основі архіву даних про захворювання колишніх пацієнтів. Отримане ДР наведено на рис. 3. Щоб спростити виклад, присвоїмо кожній ознаці індекс, який відповідає її коду в базі даних. На рис. 4 наведено структуру БД, деякі дані беруться із онтології та дерева рішень. Для задання ваг базових ознак прецедентів скористаємось арифметичним способом їх визначення. Для РА отримаємо такі значення: $W_{12}^0 = \frac{1}{2}$, $W_1^0 = \frac{1}{3}$, $W_7^0 = \frac{1}{6}$. Верхній індекс (0) вказує, що ваги є початковими. До уваги беремо лише ознаки, які характерні для цього захворювання. Тому, наприклад, для АС глибина ДР дорівнює двом, і ми отримуємо початкові ваги лише для ознак „*Біль у суглобах в спокої*" (код в БД 14) та „*Сакроілеїт*" (код – 5). Їх ваги для АС будуть $W_{14}^0 = \frac{2}{3}$ та $W_5^0 = \frac{1}{3}$. Для ПА та СС взагалі лише одна базова ознака. Так, для ПА це „*Тонуси*" (код – 27), а для СС „*Феномен Рейно*" (код – 17). Початкові ваги цих ознак для відповідних прецедентів дорівнюють одиниці.

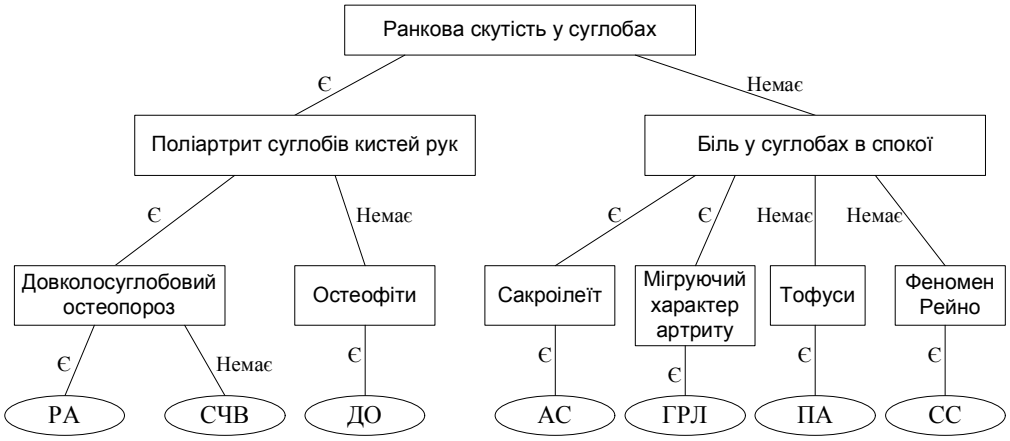


Рис. 3. Дерево рішень, отримане на основі аналізу даних ревматологічних захворювань

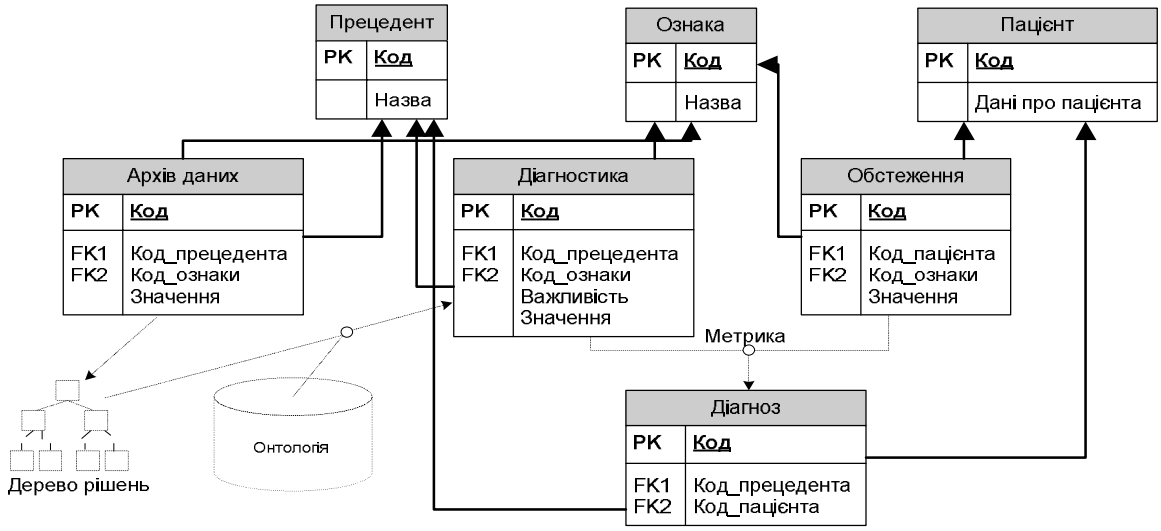
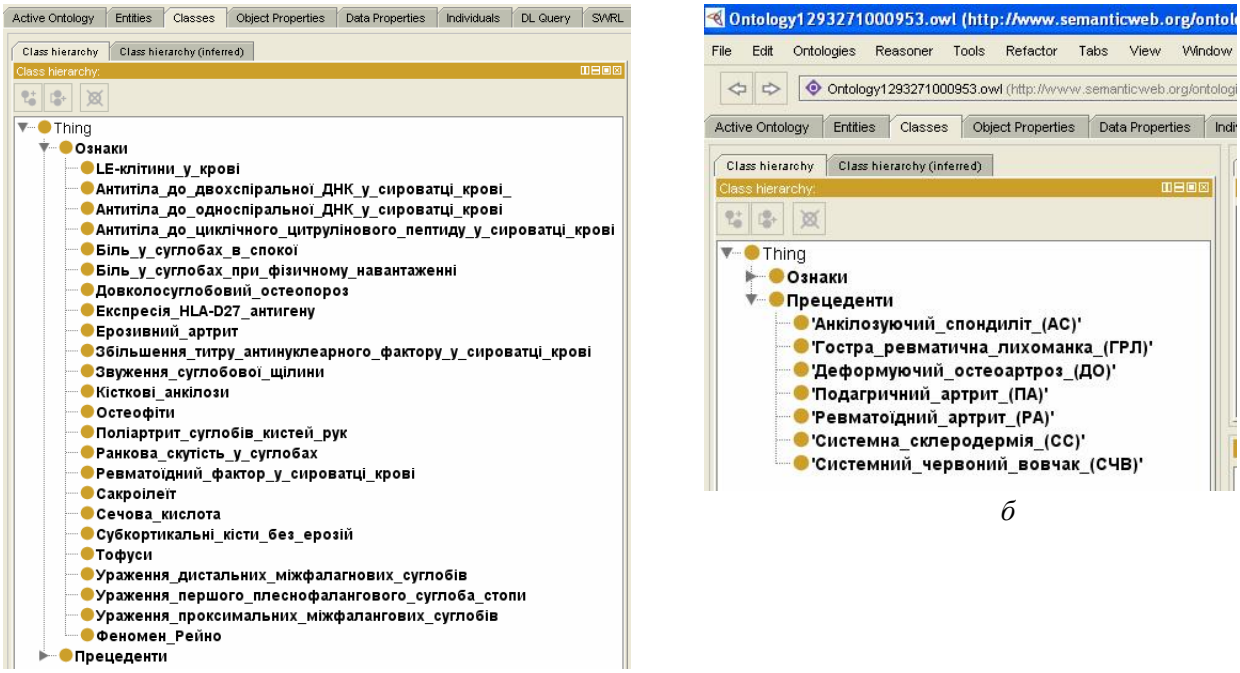


Рис. 4. Структура бази даних ІСППР діагностування ревматологічних захворювань

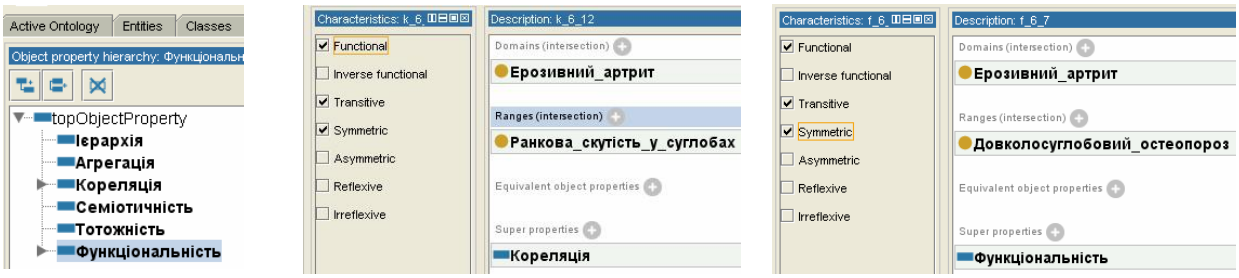


а *б*

Рис. 5. Ієрархія понять онтології ревматології

Розглянемо процес розвинення ваг базових ознак на всю онтологію ревматології, використовуючи (4) та (5). Для цього проаналізуємо нашу онтологію. Онтологія реалізована в редакторі Protégé-OWL_4.1. На верхньому рівні ієрархії онтології знаходяться ознаки та прецеденти (див. рис. 5а-б). Ієрархію відношень представимо у вигляді, розглянутому в 3-му розділі. Отже, в онтології ревматології існує 6 типів відношень (див. рис. 5, а). Перші два типи (ієрархія, агрегація), як правило, задаються у вигляді ієрархії понять, однак можливі випадки, що існуватиме множинне наслідування, або деяке поняття буде складовим кількох інших понять. Тоді ці відношення необхідно визначити в закладці Object Properties.

Однак основними для перерахунку ваг важливості понять онтології є функціональні та кореляційні відношення. Окремі з них наведено на рис. 6, б,в). В обидвох відношеннях доменом є ознака „Ерозивний артрит" (ключ 6 в БД). Множиною значень у першому випадку є „Ранкова скутість у суглобах" (ключ 12 в БД) та „Довколосуглобовий остеопороз" (ключ 7 в БД). Обидва відношення є функціональні, транзитивні та симетричні.



а *б* *в*

Рис. 6. Види відношень онтології ревматології

Перерахувавши ваги важливості понять за формулами (4), (5) отримаємо такі ознаки для різних захворювань, які необхідно використати під час обчислення відстаней за формулою (1) (див. табл. 2). Ми взяли не більше як три ознаки для кожного прецеденту. У випадку, якщо вага 2-го або 3-го поняття була меншою за 0.5, то відповідно до розгляду бралась одна або дві ознаки (так, як у випадку ПА та СС). Окрім того, використання такої властивості, як Disjoint (тобто заперечення) в

онтології ревматології привело до того, що віднутність ознаки також має значну вагу (такий результат ми отримали у випадку ГРЛ, коли відсутній „Ерозивний артрит").

Таблиця 2

Залежність захворювань від ознак

Прецедент	Ознака 1	Ознака 2	Ознака 3
Ревматоїдний артрит (РА)	Поліартрит суглобів кистей рук	Ерозивний артрит	Довколосуглобовий остеопороз
Деформуючий остеоартроз (ДО)	Остеофіти	Субкортикальні кісти без ерозій	Біль у суглобах при фізичному навантаженні
Системний червоний вовчак (СЧВ)	Біль у суглобах у спокої	Антитіла до двоспіральної ДНК у сироватці крові	Поліартрит суглобів кистей рук
Анкілозуючий спондиліт (АС)	Сакроілеїт	Біль у суглобах у спокої	Експресія HLA-D27 антигену
Гостра ревматична лихоманка (ГРЛ)	Моноолігоартрит великих суглобів	Мігруючий характер артриту	Ерозивний артрит (*відсутність*)
Подагричний артрит (ПА)	Тофуси	Сечова кислота	
Системна склеродермія (СС)	Феномен Рейно		

Аналіз табл. 2 порівняно з ДР, яке наведене на рис. 3, показує, що для ПА та СС ознаки практично не змінились, для інших захворювань змінилися в одній або двох позиціях. Перевірка реальних захворювань показала, що використання ДР правильно класифікує захворювання в 64% випадках, а за класифікацією, отриманою згідно онтологією ревматології, у 79 % випадках.

Висновки

Розроблено математичну модель функціонування інтелектуальних систем підтримки прийняття рішень на основі адаптивних онтологій для ознакових задач. Ця модель ґрунтується на метриці для знаходження релевантних прецедентів або визначення релевантності станів. Для побудови такої метрики використано онтологію. З цією метою у загальноприйнятий трьохелементний кортеж, який задає онтологію (множина понять, відношень та їх інтерпретація), нами додано дві скалярні величини (важливість понять та відношень), які використовуються для обчислення необхідних відстаней. Розглянуто способи задання початкових коефіцієнтів важливості понять та зв'язків, зокрема на основі інтелектуального аналізу даних. Розглянуто приклад функціонування такої системи для діагностики ревматологічних захворювань. Отримані результати показують ефективність розробленої моделі порівняно з деревами рішень.

1. Каменнова М.С. Корпоративные информационные системы: технологии и решения / М.С.Каменнова // Системы управления базами данных. – 1995. – № 3. – С. 88–99. 2. Funk P. Advances in Case-Based Reasoning / P.Funk, P.A.González-Calero // 7th European Conference, ECCBR 2004. – Madrid, Spain. – P. 375–380. 3. Рассел С. Искусственный интеллект / С. Рассел, П. Норвиг. – М., СПб., К.: Вильямс, 2006. – 1408 с. 4. Gruber T. R. A translation approach to portable ontologies / T.R.Gruber // Knowledge Acquisition. – 1993. – N 5 (2). – P. 199-220. 5. Інтелектуальні системи, базовані на онтологіях // Д.Г. Досин, В.В. Литвин, Ю.В. Нікольський, В.В. Пасічник. – Львів: „Цивілізація", 2009. – 414с. 6. Литвин В.В. Мультиагентні системи підтримки прийняття рішень, що базуються на прецедентух та використовують адаптивні онтології / В.В. Литвин // Радіоелектроніка, інформатика, управління. – Запоріжжя, 2009. – №2(21). – С. 120–126. 7. Даревич Р.Р. Оцінка подібності текстових документів на основі визначення інформаційної ваги

елементів бази знань / Р.Р. Даревич, Д.Г. Досин, В.В. Литвин, З.Т. Назарчук // Искусственный интеллект. – Донецк. – № 3. – 2006. – С. 500–509. 8. Sowa J. Conceptual graphs for a database interface / J.Sowa // IBM Journal of Research and Development. – Vol. 20. – 1976. – № 4. – P. 336–357. 9. Цветков А.М. Разработка алгоритмов индуктивного вывода с использованием деревьев решений / А.М. Цветков // Кибернетика и системный анализ. – 1993. – № 1. – С. 174–178. 10. Даревич Р.Р. Метод автоматичного визначення інформаційної ваги понять в онтології бази знань / Р.Р. Даревич, Д.Г. Досин, В.В. Литвин // Відбір та обробка інформації. – 2005. – Вип. 22(98). – С.105–111. 11. Фаулер М. UML в кратком изложени / М. Фаулер, К. Скотт. – М.: Мир, 1999. – 340 с.

УДК 681.142.2; 622.02.658.284; 621. 325

Ю.Ю Рашкевич, А.М. Ковальчук, Д. Д. Пелешко, М.Л. Навитка
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ПОТОКОВА МОДИФІКАЦІЯ АЛГОРИТМУ RSA З ВИКОРИСТАННЯМ ПРОЕКТИВНИХ ТА АФІННИХ ПЕРЕТВОРЕНЬ ДЛЯ ДЕЯКИХ КЛАСІВ ЗОБРАЖЕНЬ

На основі алгоритму RSA як найбільш вживаного промислового стандарту шифрування даних запропоновано модифікації з використанням проективних відображень та афінних перетворень для шифрування зображень, що дають змогу строго виділяти контури.

Ключові слова: алгоритм RSA, шифрування даних, проективні відображення, контур

Based on the algorithm of RSA, as the most common industry standard data encryption, proposed modifications using projective mappings and affine transformation for image encryption, allowing strictly allocate paths.

Keywords: algorithm RSA, data encryption, projective mapping, contour.

Вступ

У сучасному світі бурхливого розвитку інформаційних технологій все гострішим стає питання захисту інформації. Однією з найпоширеніших форм представлення інформації в цифровому вигляді є цифрові зображення.

Одним з найбільш вживаних і захищених алгоритмів шифрування даних є алгоритм RSA [1]. Він належить до групи асиметричних алгоритмів з відкритим ключем. Безпека алгоритму RSA ґрунтується на ресурсно витратній факторизації великих чисел. При цьому відкритий і закрити ключі є функціями двох простих чисел з розрядністю 100–200 десяткових знаків і більше.

Алгоритм RSA є універсальним алгоритмом, тобто може застосовуватись до будь-яких сигналів. Однак недоліком такої універсальності є те, що деякі класи зашифрованих сигналів можуть бути частково відтворені іншими засобами обробки. До таких класів сигналів належать цифрові зображення. В такому випадку виникає потреба в реалізації спеціальних алгоритмів або модифікації існуючих. Детально проблему використання алгоритму RSA стосовно зображень описано в [4].