Таблиця

Довжини ключів [7]

Довжина ключа симетричної криптосистеми, біт	Довжина ключа асиметричної криптосистеми, біт
56	384
64	512
80	768
112	1792
128	2304

Тому швидкодія криптосистем з відкритим ключем звичайно в сотні і більше разів менше швидкодії симетричних криптосистем з секретним ключем.

Ось чому застосовується комбінований (гібрідний) метод шифрування: поєднання високої секретності асиметричних криптосистем з високою швидкістю роботи симетричних криптосистем: криптосистема з відкритим ключем застосовується для шифрування, передачі і подальшого розшифрування тільки секретного ключа симетричної криптосистеми, яка застосовується для шифрування і передачі початкового відкритого тексту. Це схема електронного цифрового конверта.

Список використаних джерел

1. *Диффи У.* Защищенность и имитостойкость: Введение в криптографию / У. Диффи, М. Э. Хэллмэн // ТИИЭР. – 1979. – Т. 67, № 3. – С. 71–109.
2. *Зегжда Д. П.* Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М. : Горячая линия – Телеком, 2000. – 496 с.
3. *Мельников В. В.* Защита информации в компьютерных системах / В. В. Мельников. – М. : Финансы и статистика, 1997. – 368 с.
4. *Программирование* алгоритмов защиты информации / А. В. Домашев, В. О. Попов, Д. И. Правиков, И. В. Прокофьев, А. Ю. Щербаков. – М. : Нолидж, 2000. – 288 с.
5. *Романец Ю. В.* Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М. : Радио и связь, 1999. – 328 с.
6. *Столингс В.* Криптография и защита сетей / В. Столингс. – М. : Вильямс, 2001. – 672 с.
7. *Ященко В. В.* Введение в криптографию / В. В. Ященко. – СПб. : Питер, 2001. – 288 с.

УДК 519.8

Ю.М. Гебура, аспірант
Ужгородський національний університет, м. Ужгород, Україна

ПРИНЦИПИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДЕРЕВОПОДІБНИХ РОЗПІЗНАВАЛЬНИХ СИСТЕМ

Ю.М. Гебура, аспирант
Ужгородский национальный университет, г. Ужгород, Украина

ПРИНЦИПЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ДРЕВОВИДНЫХ РАСПОЗНАВАТЕЛЬНЫХ СИСТЕМ

Yurii Hebura, PhD student
Uzhhorod National University, Uzhhorod, Ukraine

PRINCIPLES OF MATHEMATICAL MODELLING OF TREELIKE RECOGNITION SYSTEMS

Розглянуто принципи математичного моделювання деяких деревоподібних розпізнавальних систем, де система різницевих рівнянь, із вбудованими в них графіками подій, може бути вирішена аналітично для траєкторії системи. Деревоподібні розпізнавальні системи є дискретними подіями ієрархічних систем. Представлені імітаційні моделі є основними принципами математичного моделювання деревоподібних розпізнавальних систем, які мають явні переваги у порівнянні з керованими моделями моделювання.

***Ключові слова**: математичне моделювання, деревоподібні розпізнавальні системи, ієрархічні системи, граф, імітаційна модель.*

Рассмотрены принципы математического моделирования некоторых древовидных распознавательных систем, где система разностных уравнений со встроенными в них графиками событий может быть решена аналитически для траектории системы. Древовидные распознавательные системы являются дискретными событиями иерархических систем. Представленные имитационные модели выступают основными принципами математического моделирования древовидных распознавательных систем, которые имеют явные преимущества по сравнению с управляемыми моделями моделирования.

***Ключевые слова**: математическое моделирование, древовидные распознавательные системы, иерархические системы, граф, имитационная модель.*

In this work are considered some of the principles of mathematical modeling of tree recognition systems, where the system of difference equations, with the built-in schedule of events can be solved analytically for the trajectory of the system. Tree-recognition systems are hierarchical systems of discrete events. Presented simulation models are the basic principles of mathematical modeling of tree recognition systems, which have obvious advantages compared to model-driven simulation.

***Key words**: mathematical modeling, tree recognition systems, hierarchical systems, graph, simulation model.*

Постановка проблеми. Динаміка безперервних розпізнавальних систем часто моделюється набором диференціальних рівнянь, що виражають відносини між часом змін у значеннях стану системи. Враховуючи початковий стан і граничні умови, ці рівняння повністю формують модель динамічної поведінки системи. Знайти шлях системи руху (траєкторії), який описує ця система диференціальних рівнянь, можна аналітично. Тим не менш багато цікавих моделей занадто складні для запропонованого методу рішення і повинні бути змодельовані за допомогою чисельного інтегрування в набір диференціальних рівнянь. Якщо розпізнавальна система моделюється за допомогою випадкових процесів, то моделювання може бути використане для створення траєкторій для статистичного аналізу. Аналогічним чином відносини між змінами у значеннях змінних стану (подій) у дискретній системі подій можуть бути змодельовані за графіком подій. Вершини графа являють собою зміну стану, а ребра графа – це динамічні та логічні відносини між цими змінами. Графік подій, поряд з початковими умовами, повністю визначає динаміку дискретної системи події. Як і у випадку безперервних систем, динаміка більшості моделей дискретної системи подій є складною сферою і повинна бути змодельована. В межах цієї статті розглянемо принципи математичного моделювання деяких деревоподібних розпізнавальних систем, де система різницевих рівнянь із вбудованими в них графіками подій може бути вирішена аналітично для траєкторії системи.

Аналіз останніх досліджень і публікацій. Питання математичного моделювання складних систем на сьогодні доволі повно розкрито у працях таких відомих учених, як: В.Є. Бахрушин [1], Л.Н. Сергєєва [2], Б. Оксендаль [3], Б.Я. Советов, С.А. Яковлев [4], В.М. Томашевський [5; 6] та ін.

Дж. Ту, Р. Гонсалес у своїй праці «Принципы распознавания образов» [7] наводять методи побудови систем, що розпізнають, і систему оброблення великих інформаційних масивів. Автори розглядають основні постановки завдань і найважливіші моделі алгоритмів (комбінаторно-логічні, статистичні та лінгвістичні). Виклад ведеться на досить високому рівні математичної строгості.

Особливість цієї роботи полягає в тому, що проблеми розглядаються у тісному зв'язку із завданнями ефективного оброблення інформації, причому теорія розпізнавання є самостійним напрямом прикладної математики зі своїми завданнями, апаратом і методологією.

Стосовно математичної теорії розпізнавання варто виділити роботи таких науковців, як М.Б. Айдарханов [8], О.О. Большаков, Р.І. Карімов [9].

Принципи графічного моделювання розкривають D. and L. Schruben [10], T. Yeh, J. Lee and T. Darrell [11], O. Boiman, E. Shechtman and M. Irani [12].

Однак, незважаючи на масштабність наукових досліджень відносно математичного моделювання розпізнавальних систем, питання висвітлення та розмежування принципів залишається відкритим і сьогодні.

Виклад основного матеріалу. В умовах сьогодення, враховуючи стрімкий розвиток програмних інформаційних технологій, деревоподібні розпізнавальні системи виходять на перший план у сферах генерації формальних описів класів, формуванні графових моделей динаміки системи, організації структур різних типів даних тощо.

У загальному представленні описувані моделі своєю суттю складають безліч кінцевих зв'язкових орграфів, які задаються співвідношенням:

$$S = \{V, D\}. \quad (1)$$

де V – це множина вершин;

D – множина орієнтованих ребер.

У загальному відношенні орграф сприймається як оргдерево, що походить від кореня. Так, будь-яке дерево класифікується за такими параметрами:

1) кількістю елементів множини вершин;
2) стабільністю розподілення вершин стосовно рівнів;
3) ступенем вихідної величини для кожної окремої вершини;
4) числом вихідних дуг вершини;
5) відношенням підмножини до множини.

Описи об'єктів, лінгвістичні та булеві змінні, предикати використовуються як перетворювачі в різних деревоподібних розпізнавальних структурах. Як наслідок, такі моделі являють собою ті чи інші вирішальні функції.

Слід наголосити, що деревоподібні розпізнавальні системи є дискретними подіями ієрархічних систем. Моделі графіка подій для деяких систем масового обслуговування мають розширені траєкторії й описуються в межах математичної оптимізації. У межах цієї наукової роботи будемо позначати клас графових моделей подій математичного моделювання як *S*. Підмножина, $L \subset S$, містить графіки подій, розширена траєкторія може бути знайдена як рішення задачі лінійного математичного моделювання.

Математична модель для динаміки системи розпізнає обмеження, які повинні бути виконані у відповідній задачі оптимізації планування ресурсів. Замість генерації обмежень планування (одноранговий процес), ці обмеження можуть бути отримані більшменш методично з динамічної моделі системи. Ще одна причина застосування аналітичної моделі для деревоподібних розпізнавальних систем – можливість «запуску» імітаційної моделі у S системі, вирішуючи відповідну задачу оптимізації. Як альтернатива, імітаційна модель може бути виконана звичайним способом, щоб забезпечити оптимальне рішення задачі оптимізації. Тоді це рішення може бути використано як початкове місце для проведення аналізу чутливості продуктивності системи параметричних та структурних змін. Математичне моделювання також застосовується для структуризації підсистеми ієрархічної моделі.

До ресурсів керованого моделювання відноситься граф, подія, клас. Представлені імітаційні моделі виступають основними принципами математичного моделювання деревоподібних розпізнавальних систем, які мають явні переваги у порівнянні з керованими моделями (процес) моделювання.

Поширений спосіб моделювання багатьох розпізнавальних систем – це граф з перехідною схемою [13]. Вершини цього графа – змінні стану системи. В межах його виконання навіть простій M/M/1 черзі потрібна діаграма переходів з нескінченою кількістю вершин.

Більш компактне представлення графа для динаміки розпізнавальної системи представлятимуть тільки зміни у стані системи від вершини. Кожна вершина у цьому графі являє собою одне або більше різницевих рівнянь, які визначають зміни стану, пов'язані з системною подією. Такий графік називається граф подій [14]. Вершини графа подій являють собою зміни стану, які виникають, коли відбувається певна подія. Ці вершини

з'єднані ребрами, що представляють відносини між подіями. Ребро у графі подій показано на рис. 1.

Рис. 1. Елемент з графіка подій

Рис. 1 інтерпретується таким чином: кожного разу, коли відбувається подія I, якщо умова (*j*) виконується, подію II буде призначено після затримки t.

Зміни стану, пов'язані з кожною подією, з'являються як вершинні умови в дужках. Значення параметрів можуть бути передані як аргументи для вершин подій, що дозволяють моделювати дуже великі системи розпізнавання з невеликими графіками. Значення параметрів вершин різні для кожного вузла. Будь-який з об'єктів у графі подій сам може бути графіком подій.

Розглянемо просту модель графіка подій (рис. 2).

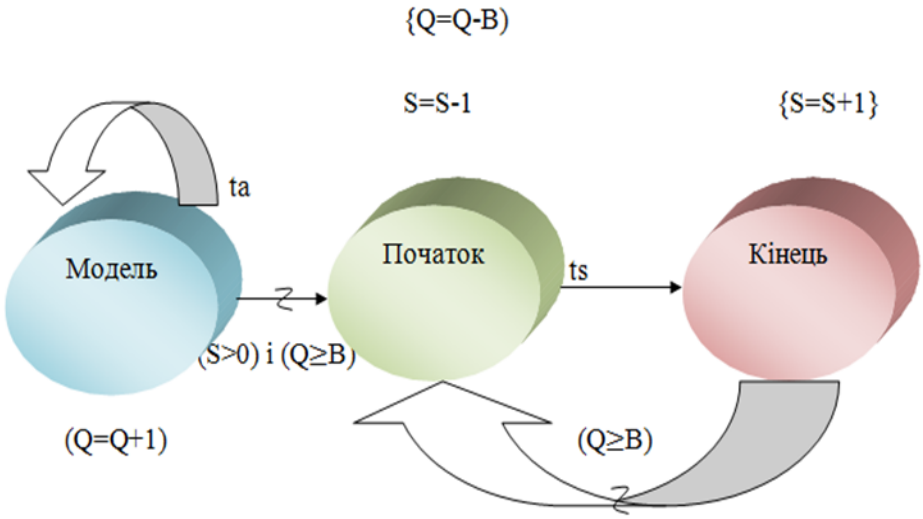

Рис. 2. Пакетне оброблення R паралельних ресурсів; Q – довжина черги; B – розмір партії; S – вільні ресурси; ts – початковий час; ta – час моделі

Джерело: розроблено автором на основі [4; 15].

Спочатку черга передбачається порожньою з усіма ресурсами простою. Таким чином, початкове значення довжини лінії, *Q* встановлюється рівним нулю, а початкове значення для числа вільних ресурсів *S* встановлюється рівним *R*. Єдина подія, яка спочатку планувалася – перша подія «*Модель*», у нульовий момент часу. Звичайно, є кілька еквівалентних графіків подій для цієї системи. Справді, окремі випадки системи можуть бути змодельовані з єдиним «*Кінцем*» вершини подій.

Дискретна ієрархічна система подій використовує чисельний алгоритм моделювання та ступінчастий підхід, які іноді називають «керованою роботою» або «взаємодією процесів» [14].

Перевагою використання моделі графа є те, що детальні опрацювання окремих робочих місць можна легко відстежити. Основним недоліком роботи керованого моделювання є те, що кожен раз, коли моделювання стає дуже перевантаженим, обсяг пам'яті збільшується, а його виконання сповільнюється або зупиняється повністю.

У моделі, розглянутій у цій роботі, індивідуальні тимчасові об'єкти у системі є пасивними, вони «переїхали» або «оброблені» за ресурсами системи. Будемо називати

такі імітаційні моделі «ресурс» керованого моделювання. Стан системи описується наявністю ресурсів та пунктів роботи. Таким чином, усі змінні стану в моделюванні на основі наявних ресурсів невід'ємні цілі числа.

Щоб перевірити істинність умов, застосовується процес підрахунку точкових подій. Тобто кількість разів, що подія *E* відбулася в часі *t,* задається безперервною функцією лічильної події.

$$C_E(t) = \lim_{\varepsilon \to 0} max\{i; E_i \leq t + \varepsilon\}. \quad (2)$$

Використовуємо відносини між подією та її точковим процесом підрахунку:

$$E_i \leq t \leftrightarrow C_E(t) \geq i. \quad (3)$$

Цей зв'язок підсилює прогресії часу: якщо поява *i* подій *E* в часі *t*, то це повинно було статися принаймні *i* раз за часом *t*.

Число робочих місць у черзі в момент часу *t, Q (t)* дорівнює числу прибулих подій мінус число початкових подій, або,

$$Q(t) = C_A(t) - B \cdot C_s(t). \quad (4)$$

У процесі моделювання *Q (t)* повинно бути більше нуля.

Наступним альтернативним рішенням виступають деревоподібні системи прийняття рішень, які спрямовані на створення додаткових систем завдяки зміщенню покоління дерева рішень за поділом загальної структури. А також отримання стандартних статистичних даних для генерації дерева рішень.

$$l(\widetilde{W}|M) = \left(1 - P(\widetilde{W}|O_i M)\right)^{\alpha}. \quad (5)$$

Далі за допомогою перемноження кількості помилок на загальну систему отримуємо рівень розпізнання системи

$$\sum_i \gamma_j(t) O_i \rightarrow \sum_i l_j(t) \gamma_j(t) O_i. \quad (6)$$

Отже, що розпізнавальна система вийде на максимально точний результат. Цей принцип з використанням дерев рішень, спрямований на будівництво тільки однієї додаткової системи. Хоча важливо зазначити, що цей принцип легко розширити до побудови декількох додаткових систем, що використовують ітеративні рамки. По-перше, необхідно враховувати, як змінюється розрахунок функції втрат під час навчання системи, як вихід доповнення ряду попередніх моделей M^l–M^s:

$$l(\widetilde{W}|M^1 \dots M^s) = \left(1 - P_{avg}(\widetilde{W}|O_i M^1 \dots M^s)\right)^{\alpha}. \quad (7)$$

Система M^{s+1} доповнює систему M^l–M^s, хоча вона може бути використана для альтернативної побудови декількох додаткових систем. На рисунку 3 показано цю структуру. Спочатку перша система навчається за рахунок базової лінії. Потім друга система навчається комплементарно як за рахунок базової лінії, так і першої додаткової системи. Це може бути повторено з отриманням ряду систем, які доповнюють один одного. Перевага цього ітеративного підходу в тому, що порядок комбінації тепер подається як порядок систем, які були побудовані.

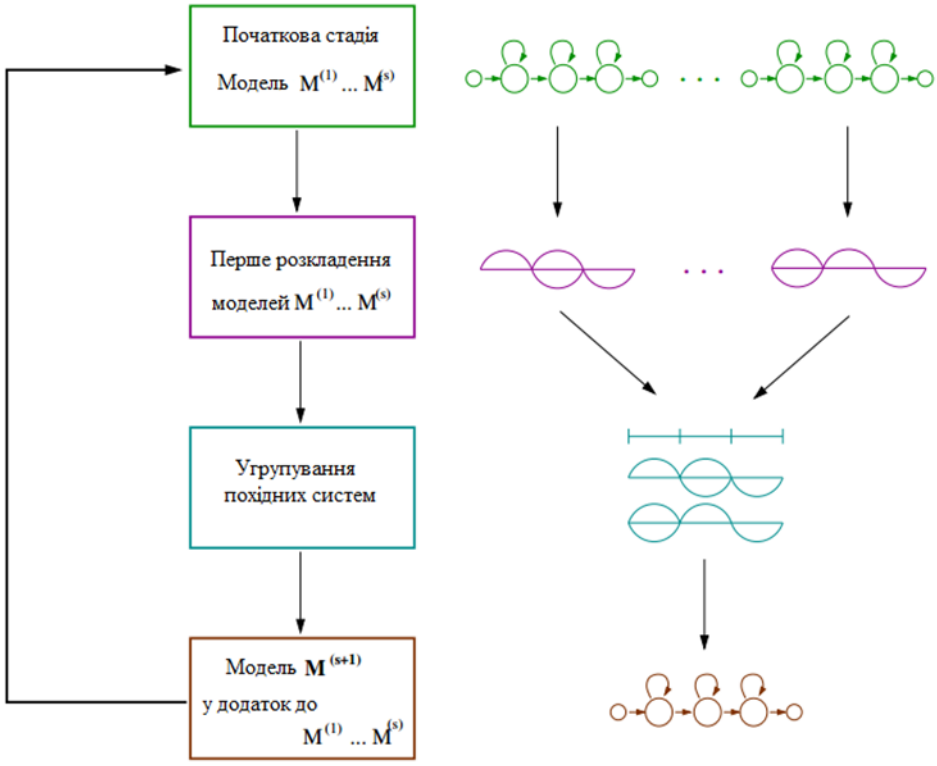

Рис. 3. Алгоритм створення декількох взаємодоповнюючих розпізнавальних систем
Джерело: розроблено автором на основі [3; 16].

Висновки і пропозиції. Математичне моделювання деревоподібних розпізнавальних систем головним чином походить від побудови орграфів, які сприймаються як оргдерева, що походять від кореня. Загальний принцип моделювання випливає з формування вирішальних функцій, які складають загальну систему рівнянь, рішення якої сприймається як модель, що має розширені траєкторії, й описується в межах математичної оптимізації. Також важливим аспектом є те, що система різницевих рівнянь з вбудованими в них графіками подій може бути вирішена аналітично для траєкторії системи.

Список використаних джерел

1. *Бахрушин В. Є.* Математичне моделювання : навчальний посібник / В. Є. Бахрушин. – Запоріжжя : ГУ «ЗІДМУ», 2004. – 140 с.
2. *Сергеева Л. Н.* Моделирование поведения экономических систем методами нелинейной динамики (теории хаоса) / Л. Н. Сергеева. – Запорожье : ЗГУ, 2002. – 154 с.
3. *Оксендаль Б.* Стохастические дифференциальные уравнения. Введение в теорию и приложения / Б. Оксендаль. – М. : Мир, 2003. – 186 с.
4. *Советов Б. Я.* Моделирование систем. Практикум : учеб. пособие для вузов / Б. Я. Советов, С. А. Яковлев. – М. : Высш. шк., 2006. – 295 с.
5. *Томашевський В. М.* Імітаційне моделювання систем і процесів / В. М. Томашевський. – К. : ІСДО, 1994. – 124 с.
6. *Томашевський В. М.* Моделювання систем / В. М. Томашевський. – К. : BHV, 2005. – 352 с.
7. *Ту Дж.* Принципы распознавания образов / Дж. Ту, Р. Гонсалес. – М. : Мир, 1978. – 267 с.
8. *Айдарханов М. Б.* Метрический и структурный подходы к построению групповых классификаций / М. Б. Айдарханов. – Алматы : Гылым, 1994. – 56 с.
9. *Большаков А. А.* Методы обработки многомерных данных и временных рядов : учебное пособие для вузов / А. А. Большаков, Р. И. Каримов. – М., 2007. – 522 с.
10. *Schruben, D.*, Schruben, L. (2000), Graphical simulation modeling using SIGMA, Custom Simulations, 653 p.

11. *Yeh, T.*, Lee, J., Darrell, T. (2007), Adpative vocabulary forest for dynamic indexing and category learning, ICCV, 232 p.

12. *Boiman, O.*, Shechtman, E., Irani, M. (2008), In defense of nearest-neighbor based image classification, CVPR, 113 p.

13. *Breslin, C.* Gales, M.J.F(2007), "Complementary system generation using directed decision trees," in Proceedings, 154 p.

14. *Bloch, I.*, Bretto, A. Mathematical Morphology on Hypergraphs: Preliminary.

15. *Definitions* and Results. In: Debled-Rennesson, I., Domenjoud, E., Kerautret, B.,Even, P. (eds.) (2011), DGCI 2011. LNCS. – Vol. 6607. – P. 429–440. Springer, Heidelberg.

16. *Bloch, I.*, Bretto, A. (2013), Mathematical morphology on hypergraphs, application to similarity and positive kernel. Computer Vision and Image Understanding 117(4). – P. 342–354.

УДК 331.543-047.22:005.311.6-044.3

О.І. Лактіонов, аспірант
Полтавський національний технічний університет імені Юрія Кондратюка, м. Полтава, Україна

МОДЕЛЬ ОЦІНЮВАННЯ РІВНЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ФАХІВЦІВ СУЧАСНИХ ВИСОКОТЕХНОЛОГІЧНИХ ВИРОБНИЧИХ ПРОЦЕСІВ

А.И. Лактионов, аспирант
Полтавский национальный технический университет имени Юрия Кондратюка, г. Полтава, Украина

МОДЕЛЬ ОЦЕНИВАНИЯ УРОВНЯ ПРОФЕССИОНАЛЬНОЙ КОМПЕТЕНТНОСТИ СПЕЦИАЛИСТОВ СОВРЕМЕННЫХ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ

Oleksandr Laktionov, PhD student
Poltava National Technical Yuri Kondratyuk University, Poltava, Ukraine

MODEL OF EVALUATION OF LEVEL OF PROFESSIONAL COMPETENCE OF SPECIALISTS OF MODERN HI-TECH PRODUCTIVE PROCESSES

Запропоновано модель оцінювання рівня професійної компетентності фахівців сучасних високотехнологічних виробничих процесів, яка описує всі складові, необхідні для розроблення автоматизованої системи, що дозволить реалізувати технологію оцінювання рівня компетентності співробітника.

***Ключові слова**: компетентність, виробничі процеси, автоматизовані системи, модель.*

Предложена модель оценивания уровня профессиональной компетентности специалистов современных высокотехнологических производственных процессов, которая описывает все составляющие, необходимые для разработки автоматизированной системы, что позволит реализовать технологию оценивания уровня компетентности сотрудника.

***Ключевые слова**: компетентность, производственные процессы, автоматизированные системы, модель.*

The model of evaluation of level of professional competence of specialists of modern hi-tech productive processes is offered in the article, which describes all constituents, necessary for development of CAS, which will allow to realize technology of evaluation of level of competence of employee.

***Key words**: competence, manufacturing processes, automated system, model.*

Аналіз останніх досліджень і публікацій. Для підвищення ефективності сучасних високотехнологічних виробничих процесів необхідно мати оцінювати компетентність фахівців з автоматизації цих процесів, які дозволяють якісно проводити підбір і розставлення кадрів по ключових позиціях підприємства [1–8].

Постановка проблеми. Для оцінювання компетентності фахівців, як засіб контролю, можна застосовувати автоматизовані системи контролю знань і вмінь комп'ютеризованих систем навчання, які є діалектичним розвитком технічних засобів контролю знань на вищому якісному рівні. Досвід роботи в цьому напрямі, аналіз досліджень [1] показують, що розроблення і впровадження таких систем вимагає появи нових методів, моделей і технологій контролю (оцінювання), для яких необхідно, передусім, здійснити формалізацію складових процесу оцінювання індивідуальної компетентності фахівця з автоматизації виробничих технологічних процесів.