7. *F. Feng and B. W. Croft*. "Probabilistic techniques for phrase extraction." *Inf. Process. Manag.*. vol. 37. no. 2. pp. 199-220. Mar. 2001.
8. *Z. Wu and M. Palmer*. "Verb semantics and lexical selection.- in *Proc. 12nd Anna. Meeting Assoc. Comput. Linguist.*. Las Cruccs. NM. Jun.27-30. 1994. pp. 133-138.
9. *C. C. Kung*. "Personalized XML information service system with automatic object-oriented ontology construction." M.S. thesis. Dept. Comput. Sci. Inform. Eng.. Nat. Cheng Kung Univ.. Tainan. Taiwan. 2000.

Поступила 16.9.2013р.

УДК 623.746-519

Б.В. Дурняк, О.Ю-Ю. Коростіль

ЗАГАЛЬНА ОРГАНІЗАЦІЯ ФУНКЦІОНУВАННЯ СИСТЕМИ ТЕКСТОВИХ МОДЕЛЕЙ

Аннотация. Рассматривается общая организация функционирования системы текстовых моделей. Проводится анализ всех задач, которые решаются на основе использования системы текстовых моделей. К таким задачам относятся задачи управления, задачи мониторинга, задачи тестирования социальных объектов и задачи обеспечения их эволюционного развития.

Ключевые слова: модель, тестирование, мониторинг, анализ, текстовые модели, социальные объекты.

Загальна організація функціонування системи моделювання соціальних об'єктів є багатоплановою і суттєво залежить від характеру задач, які планується з її допомогою розв'язувати. Тому, необхідно більш детально визначитися з окремими задачами, які планується з її допомогою розв'язувати і на прикладі однієї з них реалізувати схему функціонування такої системи. До таких з адач можна віднести наступні задачі, які на загальному рівні полягають у наступному, або вони допускають слідуючі інтерпретації:

- задачі моніторування деякого соціального середовища,
- задачі управління сукупністю SO_i,
- задачі формування сукупності визначених типів SO_i,
- задачі діагностики соціальних процесів, що проявляються в середовищі деякої сукупності SO_i,
- задачі забезпечення еволюційного розвитку деякої сукупності SO_i.

Задачі моніторування сукупності SO_i, що позначється, як деяка система SSO_i, можуть представлятися не коректними при використанні засобів моделювання типу TM_i для опису SO_i у зв'язку з тим, що текстові моделі TM_i та їх сукупність STM_i, не мають безпосереднього фізичного зв'язку з об'єктами моделювання $SO_i \in SSO_i$. Тим не менше, використання STM_i в

задачах моніторування є доцільним в силу наступних причин. Нехай маємо деяку систему $SSO_i = \{SO_1, \dots, SO_n\}$. Це означає, що можна побудувати засоби моделювання окремих SO_i у вигляді їх формалізованих описів на природній мові користувача, або самих SO_i. Моніторинг грунтується на даних та інформації, яка не залежно від STM_i на першому етапі вибирається з мережі інформаційного середовища, яким все в більшій мірі користується широке коло користувачів. Джерела отримання інформації про деяке соціальне середовище є досить різноманітними, що приводить до того, що відповідна інформація також є різнородною. Для того, щоб можна було таку інформацію адекватно і ефективно використовувати, необхідно мати засоби, які в достатньо адекватний спосіб дозволяють таку інформацію аналізувати та проводити, з її використанням, необхідні дослідження. Текстові моделі TM_i та їх STM_i разом з обслуговуючими засобами дозволяють забезпечувати адекватний та ефективний аналіз відповідних даних. Суттєвим фактором використання таких засобів є те, що вони дозволяють в максимально можливій мірі забезпечитися від суб'єктивного впливу тих осіб, які приймають участь у такому аналізі. На основі моніторування SSO_i існує можливість розв'язувати наступні задачі:

- прогнозування можливих змін в SSO_i,
- формування достатньо адекватного образу про стан окремих SO_i та SSO_i в цілому,
- задачу формування тренду розвитку SSO_i.

Задача управління сукупністю соціальних об'єктів є досить актуальною, оскільки вона з тією, чи іншою величиною успішності розв'язується у будь якому соціальному середовищі. Можна стверджувати, що неуникненність цієї задачі визначається фактом існування деякої соціальної системи і соціальних груп, що складають таку систему. На відміну від задачі моніторингу, задача управління є двохсторонньою і друга сторона цієї задачі полягає у необхідності здійснення управляючих дій на відповідне середовище SSO_i і окремі SO_i. В рамках системи STM_i, у зв'язку з задачею управління SO_i, існує можливість розв'язувати наступні задачі:

- формувати інформаційні потоки IP_i, що використовуються як засіб управляючої дії на SO_i,
- аналізувати результати дії IP_i на SO_i шляхом моделювання такої дії на модель SO_i, якою є текстова модель TM_i,
- модифікувати IP_i з ціллю підвищення ефективності його дії на SO_i завдяки моделюванню такої дії на TM_i,
- формувати адекватну стратегію управління SSO_i з допомогою системи IP_i, що передаються різним SO_i однієї соціальної системи SSO_i,
- визначати загальний характер змін, що відбуваються в SSO_i з точки зору визначення міри його еволюційності.

Особливо важливою перевагою використання системи текстових моделей є можливість не тільки якісно, а і кількісно оцінити міру змін в

окремих SO_i та в SSO_i в цілому, що дозволяє класифікувати відповідні зміни, як зміни еволюційного розвитку, чи як деградуючі зміни і визначати систему SSO_i як таку, що знаходиться в стані застою. Використання саме текстових моделей для дослідження соціальних об'єктів обумовлено тим, що текстова модель дозволяє найбільш повно відображати різні аспекти SO_i, якщо останні виявляються важливими в тих, чи інших ситуаціях.

Очевидно, що задача управління, виходячи з своєї суті, повинна використовувати як окремий фрагмент задачу моніторування соціальної системи.

Задача формування деякої сукупності SO_i може розглядатися в наступних аспектах:

- при існуванні в SSO_i, яка складається з певних типів SO_i, шляхом управління SO_i з SSO_i та, відповідно, їх модифікацією, формуються нові типи SO_i, які відрізняються від попередніх,
- формування SO_i в деякому середовищі SSO_i у випадку, коли відсутня початкова інформація про SO_i, реалізується на основі створення TM_i відповідних типів з подальшим формуванням таких IP_i, які б активізували процеси, що приводили б SO_i до необхідної їх модифікації.

Останній спосіб використовується в тих випадках, коли реальні соціальні середовища є різноплановими, є без окреслених основних властивостей, або слабо згуртовані по відношенню до тих, чи інших типів в SO_i. Для реалізації цього підходу необхідно використовувати текстові моделі, оскільки, завдяки їм можна чисельно оцінити характеристики SO_i і, таким чином, можна встановити, чи відповідна соціальна система може бути віднесена до системи з слабо окресленими соціальними об'єктами. Ця задача досить суттєво може бути пов'язана з задачами моніторингу та задачами управління SSO_i. Моніторинг систем SSO_i необхідний для того, щоб можна було визначитися з тим, чи іншим підходом до її розв'язку, а задача управління, по суті, в певній мірі є задачею формування системи SSO_i потрібного типу, який визначається типами SO_i. Задача формування певного типу SSO_i відрізняється від задачі управління тим, що задача створення певного типу соціального середовища є скінченою задачею, яка завершується після того, коли можна в результаті аналізу даних про SO_i стверджувати, що SSO_i відповідного типу є створена і стала вона відомою для системи моделей STM_i, яка з певною адекватністю описує відповідну SSO_i. У випадку задачі управління, остання є в певному сенсі не скінченою, якщо ціль управління, з точки зору його завершення, не є чітко визначеною. В більшості випадків ціллю задач управління є забезпечення процесу функціонування SSO_i тим, чи іншим способом. При чому, процес такого функціонування повинен мати еволюційний характер, що означає позитивний характер такого функціонування.

Задача діагностики соціальних середовищ визначається як окрема задача

у зв'язку з тим, що в даному випадку існують дані про такі параметри та їх значення, які приймаються негативними і їх необхідно виявляти в SSO_i з ціллю їх елімінації, чи протидії їх проявам. Ця задача, як і задача управління, завжди розв'язується в довільних типах SSO_i рядом різноманітних засобів, що передбачені в SSO_i. Прикладом стандартного підходу до розв'язку таких задач, може служити використання правоохоронних органів, які, переважно, використовуються у всіх типах SSO_i. Соціальна природа довільних типів SSO_i полягає у тому, що в них завжди можуть виникати негативні процеси, що не відповідають встановленим правилам функціонування не тільки SSO_i, а і окремих SO_i.

Завдяки використанню системи STM_i, при розв'язку задач діагностики та задач протидії негативним процесам в SSO_i, виникає додаткова можливість по виявленню та прогнозуванню виникнення негативних змін в окремих SO_i та негативних процесів за рахунок моделювання цих негативних процесів окремих SO_i в TM_i. Справа у тому, що для виникнення негативних подій та процесів необхідні відповідні передумови, що характеризуються змінами значень параметрів, які описують SO_i. Виникнення таких змін може бути спрогнозоване в рамках системи STM_i на основі їх моделювання, не залежно від процесів, що в текучий період часу відбуваються в SSO_i. У випадку відповідного передбачення можливостей таких змін, засоби протидії негативним процесам можуть управлятися самими передумовами їх виникнення, що, в більшості випадків, є значно ефективнішим, ніж протидія негативним процесам, що уже виникли і обумовлюють ті, чи інші зміни в SO_i, які, переважно інтерпретуються, як певні втрати, чи певні негативні та не допустимі події в SSO_i.

Задача забезпечення еволюційного розвитку деякої системи SSO_i інтерпретується як задача позитивного характеру незалежно від конкретних параметрів, що її характеризують [1,2]. Позитивні, чи негативні ознаки процесу функціонування та розвитку SSO_i визначаються певними концепціями, на основі яких формуються стратегії розвитку, чи сратегії функціонування. Відомими такими концепціями, які досить поширені, є концепції, що грунтуються на певній системі правил, які грунтуються на запрпонованих положеннях та аксіомах, які в соціології часом називаються догмами. В більшості випадків такі концепції представляють собою систему віри, яка не обумовлюється законами природи оточуючого середовища. Такі аспекти розглядати не будемо, оскільки вони відносяться до соціальної психології [3, 4]. Приймемо, що задана певна концепція, або система аксіом, на основі якої визначені критерії, правила та умови, що визначають процес функціонування SSO_i як такий, що є еволюційним і, відповідно, має позитивну інтерпретацію. Такий підхід до визначення еволюційного розвитку в окремій SSO_i не є абсолютно правильним [5]. Тому, однією з таких концепцій, яку приймемо як основу для формування еволюційного розвитку, полягає у наступному. Нехай деяка система SSO_i функціонує в деякому

середовищі W_i. Це середовище описує не тільки самі компоненти SSO_i, а і зовнішнє оточення, яке діє на SSO_i. Тоді, однією з компонент концепції еволюційного розвитку є умова, або вимога збалансованої взаємодії SSO_i з зовнішнім оточенням. В загальному випадку, подібного типу компонент може бути значно більше і всі вони повинні орієнтуватися на забезпечення збалансованості і стабільності процесів функціонування SSO_i в середині системи та процесів взаємодії системи SSO_i з оточуючим середовищем, яке в необхідній мірі відображається в предметній області інтерпретації, яка відноситься до системи SSO_i в цілому.

Для відображення методів загальної організації процесів функціонування системи STM_i, що моделює відповідну систему SSO_i, розглянемо задачу управління відповідними об'єктами, оскільки остання є в значній мірі базовою для більшості задач, що коротко проаналізовані, та інших задач, які можуть розв'язуватися засобами STM_i. Задачу управління системою STM_i і, відповідно, SSO_i будемо розглядати в рамках наступних умов.

1. Приймемо, що текстові моделі TM_i з STM_i з необхідною точністю описують відповідні соціальні об'єкти SO_i.
2. Задана ціль управління окремо виділеним SO_i.
3. Механізми реалізації оберненого зв'язку, в даному випадку, розглядатися не будуть.
4. Не будемо розглядати детально механізми взаємодії між окремими SO_i, які можуть бути мотивовані цілями управління, оскільки управління будемо розглядати лише одним вибраним соціальним об'єктом.
5. Приймемо, що управляючий інформаційний потік IP_i формується в рамках засобів, що є зовнішніми по відношенню до TM_i і, відповідно, до SO_i, які умовно будемо називати джерелом інформації DI_i.

При розв'язуванні задач управління, здійснюється перехід від TM_i та текстового опису IP_i, до логічних схем, що інтерполюють TM_i та IP_i. На логічному рівні реалізується вивід модифікованої моделі TM_i*, що формується з TM_i та IP_i. Проводяться перевірки отриманої схеми, що описує інтерполяцію функціонування процесу управління TM_i з допомогою IP_i та перевіряються значення логічних функцій інтерполяції. Крім того, проводиться семантичний аналіз синтезованої текстової моделі TM_i*.

В доповнення до задачі управління, розглянемо розширення системи на соціальні об'єкти, які є кінцевими об'єктами процесу моделювання засоби оберненого зв'язку між STM_i та SSO_i.

В рамках такого розширення розглянемо всі допоміжні компоненти, які приймають участь в реалізації процесу управління реальними SO_i, що грунтуються на використанні STM_i.

Можна стверджувати, що STM_i представляє собою засіб для відображення розподіленої системи SSO_i, що використовується системою формування стратегій управління сукупністю соціальних об'єктів. Таке

відображення представляє собою сукупність текстових моделей, які описують відповідні SSO_i. Загальна система реалізації управління соціальними об'єктами включає систему моніторингу відкритих засобів комунікації, якими користуються елементи соціальних об'єктів. Така система є ключовим елементом оберненого зв'язку між SO_i і SSO_i в цілому та STM_i. Оскільки функціональна компонента формування та активізації управляючих дій у вигляді інформаційних потоків IP_i призначена для реалізації відповідного управління, то загальна система управління зв'язана з STM, системою моніторування ($SMZK$) та компонентою DIP.

В рамках даної системи системи приймаються наступні положення.

Положення 1. Елементи SO_i, або, що найменше, SO_i в цілому мають доступ хоча би до одного типу двохстороннього відкритого засобу комунікації.

Така комунікація може реалізовуватися на рівні окремих елементів SO_i, на рівні цілих SO_i і не являється закритою в рамках окремих SO_i, чи SSO_i в цілому. Це означає, що $SMZK$ має доступ до повідомлень, які не пересилаються в рамках SO_i, чи SSO_i і $SMZK$ не являється компонентою SSO_i, як і всі підсистеми, що зв'язані з відповідною системою комунікації.

Положення 2. В рамках SSU розв'язується задача розширення можливостей використання відкритих засобів комунікації для елементів SO_i на тих, чи інших умовах.

Наприклад, на сьогоднішній час, ряд компонент засобів комунікації та окремі засоби комунікації надаються елементам SO_i на безкоштоній основі. Для ефективного використання систем на базі STM, засоби комунікації, що використовуються в SSO_i, персоналізуються. Перевагою даного підходу до реалізації системи управління SSO_i є те, що персоналізація засобів комунікації не є обов'язковою, оскільки завдяки окремим TM_i можна, по параметрах та характеристиках окремого повідомлення, ідентифікувати той чи інший тип елемента SO_i. Для цього необхідно використати модель TM_i, що описує відповідну систему SO_i, яка, на ряду з іншим, описує особливості тих, чи інших комунікатів.

Положення 3. В рамках SSU формуються та розв'язуються проблеми стимулювання розв'язку таких задач в галузі інтернет зв'язку та телекомунікації, які дозволяли б підвищувати ефективність реалізації системи управління SO_i та SSO_i, особливо в частині інтенсифікації процесів комунікації в соціальному середовищі.

Особливістю системи управління соціальними об'єктами є те, що остання грунтується на використанні засобів, які надаються потенціальним користувачам, як такі, що не мають безпосереднього відношення до подібних систем, а тільки надають користувачам можливість користуватися такими послугами зв'язку. Умови надання можливостей комунікації формуються таким чином, щоб користувачі були зацікавлені у їх використанні. Можна стверджувати, що рівень надання комунікаційних послуг в деякому

соціальному середовищі в значній мірі визначає можливість управління відповідним середовищем.

1. *Гуц А.К., Фролов Ю.В.* Математические методы в социологии. М.: ЛИБРОКОМ. 2008, -235 с.
2. *Редько В.Г.* Эволюция, нейронные сети, интеллект. Модели и концепции эволюционной кибернетики. Москва: ЛИБРОКОМ. 2009, - 224 с.
3. *Акофор Р., Эммери Ф.* О целеустремлённых системах. М.: Мир, 1999. – 233 с.
4. Социальная информатика: основания, методы, перспективы. / Под ред. Н.И. Лапина. М.: Книжный дом. 1998. -321 с.
5. *Белотелов Н.В., Бродский Ю.И., Павловский Ю.К.* Математическое моделирование и гуманитарный анализ. Москва: ЛИБРОКОМ. 2000, -345 с.

Поступила 23.10.2013р.

УДК 681.142.2; 622.02.658.284; 621. 325

М. Б. Ступень, аспірант кафедри АСУ, НУ “Львівська політехніка”

ПІДВИЩЕННЯ КРИПТОЛОГІЧНОЇ СТІЙКОСТІ ШИФРУВАННЯ З ВИКОРИСТАННЯМ ДРОБОВО-ЛІНІЙНИХ ПЕРЕТВОРЕНЬ

У статті описано методи підвищення криптологічної стійкості системи шифрування. Описано математичне доведення підходу підвищення стійкості шифрування при використанні дробово-лінійних перетворень, зокрема з використанням кватернарних дробово-лінійних перетворень.

*Ключові слова***:** стійкість, шифрування, зображення, кватернарна форма.

This article describes methods for improving the stability of cryptology encryption. A mathematical proof approach increased resistance encryption using fractional-linear transformations is described, in particular using quaternary fractional linear transformations.

Keywords: resistance, encryption, image, quaternary form

В статье описаны методы повышения криптологической устойчивости системы шифрования. Описано математическое доказательство подхода повышения устойчивости шифрования при использовании дробно-линейных преобразований, в частности с использованием четвертичных дробно-линейных преобразований.

Ключевые слова: устойчивость, шифрование, изображения, четвертичная форма.

Вступ. Проблема стійкості криптографічної системи.

Проблема обгрунтування стійкості криптографічної системи зводиться до доведення відсутності поліноміального алгоритму, який розв'язує задачу зламування системи. Однак тут виникає ще одна й дуже серйозна перешкода:

