1. *Шовенгердт Р.А.* Дистанционное зондирование. Модели и методы обработки изображений / *Шовенгердт Р.А.* – М.: Техносфера. 2010. – 560 с.
2. *Орищенко В.И., Сонников В.Г., Свириденко В.А.* Сжатие данных в системах сбора и передачи информации. – М.: Радио и связь, 1985. – 184 с.
3. Методы передачи изображений. Сокращение избыточности. / *Под. ред. У.К. Прэтта.* – М.: Радио и связь, 1983. – 263 с.
4. *Пашков Д.П.* Анализ передачи специальной информации в бортовых системах космических аппаратов дистанционного зондирования Земли // Системи управління, навігації та зв'язку. – К.: ЦНДІНУ. – 2007. – Вип. 3. – С.32-34.
5. *Бабкин В.Ф., Крюков А.Б., Штарьков Ю.М.* Сжатие данных. – В кн.: Аппаратура для космических исследований. – М.: Наука, 1972. – С.172–209.
6. *Залмазон Л.А.* Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. – М.: Наука, 1989. – 496 с.
7. *Козелков С.В., Пашков Д.П.* Анализ алгоритмов сжатия и восстановления видеоданных оптико-электронных средств бортовых систем космических аппаратов дистанционного зондирования Земли // Международная научно-практическая конференция "Университетские микроспутники – перспективы и реальность" (19–23 июня 2006 р.) – Днепропетровск: – НЦАОМУ. 2006. – С. 14.
8. *Зив Дж.* Алгоритм универсального сжатия данных // Проблемы передачи информации. – 1996. – №2. – С. 47–55.
9. *Ахмед Н., Рао К.Р.* Ортогональные преобразования при обработке цифровых сигналов / *Под ред. И.Б. Фоменко.* – М.: Связь, 1980. – 248 с.
10. *Ватолин В.И., Ратушняк А., Смирнов М, Юкин В.* Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ–МИФИ, 2002. – 384 с.

Поступила 17.02.2011р.

УДК 004.921

Б. В. Дурняк, В. І. Сабат, Л. Є. Шведова, Ю.Ю.Білак

РОЗРОБКА СТРУКТУРИ СИСТЕМИ УПРАВЛІННЯ ПОВНОВАЖЕННЯМИ

Структура системи управління повноваженнями, що надаються суб'єктам по відношенню до об'єктів відображає фізичні можливості в реалізації зв'язку між окремими компонентами та реалізацію функціональних взаємодій між ними, яка можлива завдяки існуванню фізичних взаємозв'язків. Тому визначимо компоненти системи управління повноваженнями (*SUP*), які являють собою фізичні об'єкти відповідної системи. Крім фізичних компонент *SUP*, можуть існувати логічні компоненти, які відрізняються від фізичних тим, що в рамках однієї фізичної компоненти можна реалізувати цілий ряд логічних компонент. Оскільки більшість функцій *SUP* реалізуються в рамках стандартної компоненти, яка являє собою універсальний

обчислюваний засіб, то про структуру системи *SUP* будемо говорити на логічному рівні. В цьому випадку можна прийняти, що структура *SUP* може бути:

— статичною;
— динамічною;
— обумовлено-модифікованою.

Статична структура, яка описує взаємозв'язки між окремими компонентами *SUP*, не змінюється в процесі функціонування *SUP*. Слід зазначити, що існування взаємозв'язків між компонентами, не означає що між ними існує і функціональний зв'язок. Завдяки цьому можна затверджувати можливість існування різних логічних та функціональних структур в межах однієї фізичної структури. Тому в подальшому будемо говорити про структуру *SUP* розуміючи під нею лише логічну, або функціональну структуру.

Під динамічною структурою будемо розуміти таку структуру, яка може змінюватися по закінченому, наперед визначеному періоду роботи *SUP*. Спосіб зміни відповідної структури задається перед початком певного періоду, або ті чи інші зміни формуються на основі аналізу результатів функціонування *SUP* на протязі заданого періоду часу ΔT_i. Інтервал часу ΔT_i визначається періодом вирішення базової задачі, в розв'язку якої приймає участь система *SUP*. Очевидно, що аналіз результату функціонування *SUP* протягом часу ΔT_i реалізується на основі використання інтерпретації результатів, отриманих прикладною задачею, яка розв'язувалась в *IS*. Можна виділити такі основи аналізу роботи *SUP*:

— аналіз зв'язку результатів розв'язку прикладної задачі з процесом функціонування *SUP* в період ΔT_i;
— аналіз вибраних параметрів, які характеризують *SUP* незалежно від інтерпретації, що використовується в прикладних задачах;
— аналіз розвитку, або змін в структурі *SUP*.

Обумовлено-модифікована структура *SUP* являє собою таку структуру, яка може модифікуватися в довільний момент часу в рамках періоду ΔT_i. В цьому випадку можна виділити такі причини, що обумовлюють необхідність змін у структурі:

— виникнення в рамках *SUP* подій, визначених як такі, що мають негативну інтерпретацію;
— коли параметри, що характеризують *SUP* приймають недопустимі значення;
— зміни структури можуть ініціюватися процесами протидії виявленим атакам на *SUP*.

Зміна структури *SUP* у більшості випадків пов'язана із змінами, що реалізуються в окремих компонентах. При цьому компоненти в *SUP* складають основну та допоміжну групу компонент. До основної групи компонент відносяться:

— множини X та Y;
— система аналізу запиту L^A на отримання повноважень y_i відносно x_i;

— система параметрів, які характеризують *SUP* незалежно від прикладних задач, що розв'язуються в *IS*.

До допоміжних компонент відносяться:

— система визначення пріоритетів запитів на обслуговування, якщо виставлені запити між собою конфліктують з об'єкту повноважень x_i, чи з типу повноважень, що формуються відносно x_i;

— система граничних значень параметрів *SUP*;

— система опису атак на *SUP*, які можуть бути виявлені в рамках системи.

Найважливішим серед усіх елементів в системі *SUP* є визначення міри безпеки, яку гарантує дана система. Зрозуміло, що у випадку, коли необхідний рівень безпеки системи *SUP* є близький до нуля, то *SUP* перетворюється у систему управління ресурсами та задачами, які використовуються і функціонують в рамках *IS*. Будь-яка прикладна система, що складається з певної сукупності задач, в якості обов'язкової компоненти містить систему, або алгоритм управління відповідними задачами, а управління обчислювальними ресурсами здійснюється в рамках операційних систем, що складають основу будь-якої *IS*. Таким чином використання системи *SUP* є доцільним тільки в тому випадку, коли прикладні системи (*PS*), що реалізуються в *IS* потребують забезпечення безпеки їх функціонування. Якщо уявлення про безпеку функціонування *PS* і *IS*, відповідно розглядати в широкому розумінні цього терміну, то можна вважати, що безпека функціонування *PS* залежить від таких факторів:

— здатності всіх системних та інструментальних засобів, що використовуються, для реалізації процесів функціонування *PS*, забезпечувати очікувані чи штатні режими їхньої роботи;

— здатності засобів захисту системи *IS*, включаючи *SUP*, виявляти та протидіяти зовнішнім факторам, що ініціюють процеси втручання в роботу *IS* з ціллю порушити очікуваний спосіб її функціонування, або з ціллю несанкціонованого привласнення інформаційних компонент системи;

— внутрішніх факторів, що обумовлюються помилками які можуть виникати в *PS* чи діями санкціонованих факторів, які приймають участь у забезпечені процесу функціонування *IS*.

Перший фактор відноситься до групи, що прийнято називати причинами, які впливають на надійність системи *IS* і цей фактор досліджується окремо від факторів, які обумовлюють безпеку функціонування *IS* [1].

Останній фактор, в більший мірі стосується організаційних аспектів реалізації процесу функціонування *IS* до яких відносяться:

— якість та повнота тестування *PS*;

— адекватність організаційних та системних засобів до встановлених вимог.

Тому вищевказані фактори не розглядаються в рамках даної роботи, як такі, що впливають на безпеку функціонування *IS* в цілому. Слід зазначити,

що *PS* відрізняється від *IS* тим, що в склад *PS* не входять всі можливі чи необхідні системні та організаційні засоби, що забезпечують можливість функціонування *PS*. В подальшому при дослідженні безпеки, яку забезпечує *SUP*, будемо розглядати тільки другий фактор та засоби виявлення і протидії атакам, що розміщенні в *SUP*. Виходячи з основного призначення *SUP*, яке полягає в управлінні повноваженнями y_i відносно x_i, розглянемо перелік додаткових функцій, орієнтованих на виявлення та протидію несанкціонованим зовнішнім факторам, що ініціювали певну послідовність дій, яка реалізує атаку. Слід зазначити, що послідовність подій, які реалізують атаку та кожна подія окремо, являє собою події, що можуть виникнути в середовищі *IS* та її компонентах і окрема подія може бути такою, яка є допустимою у відповідному середовищі. Розглянемо можливі способи розширення базових функцій системи *SUP*, які пов'язані із забезпеченням безпеки функціонування відповідної системи:

— реалізація контролю додаткових даних, що пов'язані з наданням повноважень суб'єкту y_i;
— розпізнавання подій, які не є санкціонованими в системі *SUP* і допускають інтерпретацію, що співставляє такі події з можливими атаками;
— аналіз даних про результати надання повноважень системою *SUP*, які передаються від системних засобів *IS* та які пов'язуються з фактом надання повноважень системою *SUP*;
— використання додаткових компонент системи *SUP* для розв'язку задач забезпечення безпеки *IS* і, відповідно, *PS*;
— використання додаткових засобів, що входять у систему *SUP* і орієнтовані безпосередньо на виявлення та протидію атакам.

Додатковими даними, що аналізуються в *SUP* при наданні y_i повноважень на співпрацю, або використанні об'єкта x_i можуть бути:

— наявність пріоритету у суб'єкта y_i та його зв'язок з мірою значимості суб'єкта $c_i(y_i)$;
— типи повноважень W_i які сформують y_i та величина категорії $k_i(x_i)$ по відношенню до відповідних повноважень y_i, що визначаються значимістю суб'єкта $c_i(y_i)$;
— дані поточного стану матриці доступу $A[c_i(y_i), k_i(x_i)]$, що сформована на поточний момент часу.

До подій, що безпосередньо можуть бути пов'язаними з реалізацією атак належать події, пов'язані із зміною параметрів, які характеризують умови надання доступу, що ініціювались відразу після подій, в результаті яких у наданні доступу було відмовлено в рамках системи *SUP*. Різні події, що реєструються в рамках *SUP*, можуть мати різну міру ймовірності того, що остання визначає наявність атаки. Збільшення ймовірності виявлення атаки реалізується шляхом взаємозалежного аналізу послідовних подій, між якими можна встановити зв'язок. В цьому випадку з'являється додаткова можливість управляти рівнем безпеки *SUP*, шляхом встановлення різної довжини послідовних, взаємозв'язаних подій, яку необхідно аналізувати для того, щоб

можна було виявити атаку, чи прийняти факт, що атаки не має в поточній ситуації процесу функціонування системи *SUP*. Іншим регулюючим фактором міри безпеки, яку може забезпечити *SUP*, є ініціація або не використання окремих засобів чи функцій, що можуть в рамках *SUP* ініціюватися, які призначені виключно для виявлення атак, або їх проявів у середовищі *SUP*. Наступним прикладом подій, які допускають їх інтерпретацію як таких, що ініціюванні небезпеками і носять елемент атаки, є події, що полягають у виникненні аномалій в процесі функціонування *SUP*. Прикладом такої аномалії може бути конфліктна ситуація, що виникає в процесі функціонування *SUP*. При цьому не має ніякого значення природа відповідного конфлікту або форма в якій він проявляється. Наприклад, конфліктна ситуація може проявлятися у випадку, коли *SUP* надає суб'єкту y_i повноваження на запис даних в об'єкт x_j, а на наступному циклі роботи *SUP* надає повноваження суб'єкту y_i, на обнуління або витирання даних, які були введені на попередньому етапі управління суб'єктом y_j і, в тому числі, іншими суб'єктами, що співпрацювали з об'єктом x_i. Таким чином, наступним методом управління рівнем захисту *PS*, який забезпечується системою *SUP*, є аналіз умов надання повноважень суб'єктам y_i не тільки на рівні управління повноваженнями, а й на рівні аналізу типів повноважень, що ініціюються в процесі функціонування *SUP*.

Однією з додаткових компонент системи безпеки є компонента за допомогою якої можна виконувати такі функції в рамках *SUP*:

— визначати поточне значення рівня безпеки системи, яке позначатимемо μ;
— аналізувати додаткову інформацію, яка подається у *SUP* після реалізації відповідною системою дій з ціллю забезпечення заданого рівня безпеки системи;
— здійснення управління рівнем безпеки системи.

Для більш детального представлення алгоритму функціонування відповідної компоненти, необхідно визначити можливі методи обчислення величини μ. Для цього розглянемо зв'язок міри безпеки об'єкта з величиною його надійності (η). Приймемо, що у випадку, коли $\eta = 0$, то це означає, що у відповідний момент функціонування *SUP* остання є несправна. Рівень безпеки будемо визначати в діапазоні значень, що може забезпечувати ту чи іншу міру надійності. Приймемо, що для системи S_i забезпечується міра надійності $\eta_i=h_i$ і, у відповідності зі стандартом визначення міри надійності системи S_i, вона визначає здатність системи виконувати процеси функціонування у відповідності з умовами та вимогами, які описані та визначені технічною документацією протягом певного періоду часу [2]. Таким чином одним з важливих факторів, що можуть вплинути на зміну величини $\eta_i=h_i$, можна вважати атаки на відповідну систему. Основними засобами протидії цим факторам є засоби, які в сукупності складають систему захисту S_i. Оскільки система захисту (*SZ*) орієнтована на забезпечення безпеки функціонування S_i то можна стверджувати, що вона повинна забезпечити такий рівень захисту

$\mu_i=g_i$, який би не перевищував задану міру надійності $\eta_i=h_i$ системи S_i. Щоб цю тезу можна було використати, необхідно розглянути можливість вимірювання величини η_i і μ_i в однакових, або достатньо близьких одиницях виміру. У відповідності з уявленнями про методи забезпечення високої надійності в значній мірі вони реалізуються шляхом збільшення компонент, які є функціонально-надмірними та орієнтовані на підвищення рівня надійності. Прикладом таких методів може бути дублювання окремих блоків, резервування окремих підсистем та ін. Тому можна стверджувати що міра надійності η залежить від кількості засобів, якими доповнюється система в раках різних структурних рішень S_i. Формально фактор підвищення надійності можна записати у вигляді співвідношення:

$$\eta^S\left(S_j\right)=\sum\nolimits_{i=1}^{m}\alpha_i\eta_i\left(\xi_i\right)+F\left[\eta_1\left(\xi_1\right),...,\eta_m\left(\xi_m\right)\right], \tag{4.1}$$

де η^s – надійність, обумовлена структурними рішеннями побудови системи S_j; $\eta_i\left(\xi_i\right)$ – надійність окремої додаткової компоненти, що включається в склад S_j; F – функція, що визначає збільшення надійності за рахунок структурних взаємозв'язків між окремими $\eta_i\left(\xi_i\right)$; α_i – коефіцієнт узгодження обчислення надійності для окремих компонент ξ_i. Можна прийняти, що F є функцією, яка не змінюється в процесі функціонування S_j. Тоді, співвідношення (4.1) можна записати у вигляді:

$$\eta^S\left(S_j\right)=\sum\nolimits_{i=1}^{m}\eta_i^*+\Delta\eta^c, \tag{4.2}$$

де $\eta_i^*=\alpha_i\eta_i\left(\xi_i\right)$; $\Delta\eta^c$ = константа, яка відповідає збільшенню величини $\eta^S\left(S_j\right)$ за рахунок вибору певної F_i. В цьому випадку можна стверджувати, що $\eta^S\left(S_i\right)$ залежить від кількості окремих засобів, орієнтованих на збільшення $\eta_i^S\left(S_j\right)$, до якої додається константа $\Delta\eta^c$, якщо в процесі функціонування S_j не змінюється структура, що описується функцією F_i.

Аналогічно можна говорити про засоби захисту ξ_i, кожний з яких орієнтований на певний тип атак і таким чином, забезпечує певний рівень безпеки S_j. Можна записати наступну залежність:

$$\mu^S\left(S_j\right)=\sum\nolimits_{i=1}^{n}\beta_i\mu_i\left(\xi_i\right)+\Phi\left[\mu_1\left(\xi_1\right),...,\mu_n\left(\xi_n\right)\right], \tag{4.3}$$

де β_i – аналогія α_i, але стосується μ_i; Φ – аналог F із співвідношення (4.1). Аналогічно до співвідношення (4.2) можна записати:

$$\mu^S\left(S_j\right)=\sum\nolimits_{i=1}^{n}\mu_i^*+\Delta\mu^c, \tag{4.4}$$

Таким чином, при введені обмежень, які стосуються того, що ні F ні Φ в процесі функціонування не змінюються, то можна стверджувати, що η^S і μ^S може вимірюватися кількістю одиничних засобів підвищення надійності і підвищення безпеки, відповідно. Якщо $\alpha_i>\alpha_j$ та $i>j$, то можна стверд-

жувати, що $\eta_i^*(\xi_i) = q \cdot \eta_i^+(\xi_i)$ і, аналогічно, $\mu_i^*(\xi_i) = q^* \cdot \mu_i^+(\xi_i)$, де η^+ і μ^+ являють собою абстрактний одиничний засіб. Тому, можна стверджувати, що у випадку η і μ вони вимірюються кількістю деяких абстрактних засобів в окремій системі.

Інший підхід до визначення величини η і μ ґрунтується на використані методів ймовірнісних оцінок, що вказують можливість зменшення величини $\eta^v{}_i$ та $\mu^v{}_i$, відповідно, в процесі роботи системи S_i. Для реалізації таких методів необхідно володіти даними виникнення причин, що обумовлювали зниження рівня надійності, наприклад, вихід з ладу деякого вузла системи чи виникнення окремих несправностей та ін. На основі таких даних, що реєструвались протягом певного часу та на основі дослідження відповідної множини даних вибирається та чи інша модель, для обчислення статичних оцінок ймовірності зниження значення $\eta^v(S_j)$. Одним з базових обмежень, які обумовлюються вибраним підходом, є обмеження на характер ймовірнісні особливостей окремих даних та їх множин. Прикладом таких обмежень може бути вимога незалежності окремих ймовірних подій [3]. В цьому випадку, можна говорити про додаткову складову при визначенні величини $\eta(S_j)$, яка формально описується співвідношенням:

$$\eta^V(S_j) = -M_i\left[\eta_1(v_1), ..., \eta_m(v_m)\right], \tag{4.5}$$

де $\eta_i(v_i)$ – величина на яку змінюється надійність системи S_j при виникненні події V_i. Оскільки, за визначенням розглядаються події V_i, які призводять до зменшення рівня надійності, то $\eta^v(S_j) \le 0$. M_i – ймовірнісна модель, яка вибирається для визначення величини зміни параметра $\eta^v(S_j)$. В цьому випадку загальне співвідношення можна записати таким чином:

$$\eta(S_j) = \eta^S(S_j) - \eta^V(S_j). \tag{4.6}$$

Оскільки, відповідна компонента для $\mu(S_j)$ визначається аналогічно, то розглянемо аналогію між окремими компонентами $\eta(S_j)$ і $\mu(S_j)$. Аналогом, для подій V_i із співвідношення (4.6) у випадку міри безпеки є подія, що являє собою атаку U_i. Виникнення U_i розглядається як подія випадкова. Не виявлення і, як наслідок, не протидія зі сторони відповідних засобів таким атакам також є випадковою подією. Така послідовність окремих випадкових подій розглядається як одна випадкова подія, що полягає в успішній реалізації атаки, яка призводить до зменшення рівня безпеки $\mu(S_j)$ в системі. Формально це можна описати співвідношеннями, які аналогічні співвідношенням (4.5) та (4.6) для $\eta(S_j)$:

$$\mu^V(S_j) = -M_i\left[\mu_1(\omega_1), ..., \mu_m(\omega_m)\right],$$

де ω_i – подія, яка полягає у тому, що атака на S_j виявилася успішною.

$$\mu(S_j) = \mu^S(S_j) - \mu^V(S_j).$$

З вищенаведеного можна прийняти, що рівень безпеки функціонування системи не може перевищувати рівня її надійності, оскільки надійність і

безпека системи визначаються факторами, які розділені між собою в окремі множини факторів. Очевидно, що можна було сумістити відповідні уявлення, але прийняті в галузі захисту інформації уявлення про безпеку даних чи їх захист обумовлює некоректність такого суміщення [4]. У зв'язку з тим приймемо, що для кожної *IS*, чи прикладної системи *PS*, існує власний максимально-можливий поріг величини безпеки або міри захисту інформації. Формально це можна записати у вигляді:

$$\max \mu\left(S_i\right) \le \max \eta\left(S_i\right). \tag{4.7}$$

При обчислені складової $\mu(S_i)$, остання визначається деяким числом, яка характеризує кількість окремих засобів захисту та числом, яке завжди є додатнім і призводить до збільшення величини μ^S за рахунок певного способу об'єднання двох чи більшої кількості засобів. Відповідні числа, що характеризують надійність S_i формуються в частині η^S аналогічно. Тому, вони є сумісними з точки зору їх інтерпретації і тому їх можна порівнювати в рамках співвідношення (4.7). При цьому в рамках системи захисту *SZ* деякої S_i, кількість засобів захисту обчислюється не за їх фізичною присутністю в *SZ* а за активністю, яка проявляється в процесі функціонування *SZ* протягом встановленого циклу роботи *PS*. Таким чином існує можливість підвищення або зменшення рівня захисту $\mu(S_i)$ за рахунок активізації, чи відключення відповідних засобів захисту, в рамках реалізації деякого циклу функціонування *SP*. Змінювати величину $\mu(S_i)$ можна також за рахунок зміни способу організації взаємодії відповідних засобів захисту, який реалізується на алгоритмічному рівні реалізації відповідної взаємодії. На відміну від величини безпеки величина надійності S_i в процесі її функціонування не змінюється і управління відповідним параметром не здійснюється, хоча таке управління є можливим і може реалізовуватися способами аналогічним до тих, які використовуються при управлінні величиною безпеки S_i. Доцільність управління величиною μ_i обумовлюється тим, що використання засобів захисту потребує затрат ресурсів *IS*, що призводить до подорожчання послуг на використання обчислювальних ресурсів для користувача системи S_i. Зменшення рівня безпеки $\mu(S_i)$ не пов'язане із зміною величини $\eta^S(S_i)$ тому можна записати співвідношення:

$$\neg\left\{\left[\mu^S\left(S_i\right)=0\right]\rightarrow\left[\eta^S\left(S_i\right)<\max \eta^S\left(S_i\right)\right]\right\}.$$

З точки зору прийнятого підходу, можна говорити про доцільність зменшення $\eta^S(S_i)$, для *PS*, які не потребують високого рівня захисту інформації. Ці аспекти в рамках даної роботи не розглядаються.

Очевидно, що складова $\mu^V(S_i)$ і відповідно $\eta^V(S_i)$ може формуватися як така, що збільшує $\mu(S_i)$ та $\eta(S_i)$ відповідно. Це залежить від вибору типу статистичних даних.

1. *Василенко И. А.* Надежность технических систем / *Под. ред. И. А. Василенка.* – Красноярск : МГП «Раско», 2001.
2. ГОСТ 27.002-89. Надежность в технике. Термины и определения.

3. *Посшнев С. В.* Компьютерный анализ и интерпретация эмпирических зависимостей / *С. В. Посшнев, Е. В. Овечкина, М. В. Вашенко, А. В. Каплан, В. Е. Каплан.* – М. : БИНОМ, 2009.
4. *Соколов А. В.* Защита информации в распределенных корпоративных сетях и системах / *А. В. Соколов, В. Ф. Шаньгин.* – М. : ДМК Пресс, 2002.

Поступила 17.02.2011р.

УДК 683.06

Б.В. Дурняк, О.Ю-Ю. Коростіль, М.Е.Шелест

РОЗШИРЕННЯ СЕМАНТИЧНИХ ПАРАМЕТРІВ ТЕКСТОВИХ МОДЕЛЕЙ

Аннотация

Вводятся и исследуются дополнительные семантические параметры, которые характеризуют текстовые фрагменты и используются для исследования различных моделей, которые с различной мерой приближения описывают текстовые модели.

Ключевые слова: текстовые модели, семантические параметры, интерпретационные семантические параметры, структурные семантические параметры.

Текстові моделі (TM_i) призначені не тільки для опису соціальних об'єктів (SO_i), або інших об'єктів, які важко описати формальними засобами, для статичного їх відображення, а і для опису їх взаємодії з зовнішніми факторами та взаємодії між собою. Це обумовлює необхідність розширення асортименту параметрів, що їх описують. Оскільки, мова йде про текстові форми опису, то розширенню підлягають семантичні параметри. Перетворення, опис яких повинні забезпечувати відповідні розширення параметрів є наступними:

- додавання фрагментів тексту до існуючого текстового опису деякого об'єкту,
- елімінація окремих фрагментів з тексту,
- перестановка фрагментів тексту в межах текстового опису всієї моделі.

Для реалізації таких перетворень, необхідно розв'язати наступні задачі:

- визначення фрагменту тексту, найменший розмір якого може представляти собою одну фразу φ_i, з точки зору його семантичної значимості, або семантичних характеристик, якими цей фрагмент співвідноситься з найближчим його оточенням,

