УДК 004.921

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

ЗАГАЛЬНА ОРГАНІЗАЦІЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ЗАСОБІВ ДЛЯ СТВОРЕННЯ СИСТЕМИ УПРАВЛІННЯ ПОВНОВАЖЕННЯМИ

Сукупність інформаційних засобів та інших компонент, що складають інформаційну технологію, можна використовувати для побудови системи управління доступом до обчислюваних ресурсів таким чином, щоб в процесі її використання можна було управляти рівнем безпеки системи. В рамкам можливостей розробленого підходу управлінням рівнем безпеки може мати такі особливості:

— рівнем безпеки можна управляти динамічно, змінюючи його в процесі реалізації процедур доступу, не очікуючи завершення певного циклу роботи системи *SUP* чи циклу роботи системи *PS*;
— управління безпекою може мати вибірковий характер, що дозволяє забезпечувати різні значення відповідного рівня безпеки різним користувачам, яким відповідають різні PS_i;
— оцінка величини рівня безпеки системи в кожному конкретному випадку має спрощену інтерпретацію, яка безпосередньо проектується на засоби захисту, на компоненти, які використовуються для реалізації відповідного захисту, і ця величина носить конструктивний або технологічній характер відносно самої *SUP*;
— інтерпретація міри захищеності може формуватися таким чином, щоб вона носила, по можливості, найбільш приязний для користувачів зміст;
— та чи інша інтерпретація міри безпеки системи може впливати на її величини та на способи її забезпечення в рамках системи *SUP*;
— процеси захисту можуть реалізуватися не тільки виключно засобами захисту, але й функціональними компонентами, шляхом зміни параметрів їх функціонування чи зміни режимів, або способів реалізації окремих процесів;
— зміна рівня безпеки не обумовлюється факторами, що впливають на зменшення величини надійності, оскільки останні призводять до загального зниження рівня безпеки, який не управляється засобами захисту системи *SUP*.

Однією з основних компонент системи *SUP* є компонента яка приймає рішення про надання, або відмову у наданні повноважень. Використовуючи загальноприйняту термінологію, будемо називати її матрицею доступу до ресурсів [1]. В рамках даної роботи матриця доступу M_i буде являти собою певну схему, яка об'єднує суб'єктів з об'єктами в процесі функціонування *SUP*. Основними системами цієї схеми є система визначення наявності

певних повноважень в ситуації, що відповідає поточному моменту t_i процесу функціонування системи. В рамках цього елементу здійснюється визнання можливості надання суб'єкту y_i повноважень W_i відносно об'єкта x_i. Цей елемент являє собою систему виводу деякої логічної функції, яка описує ситуацію, що склалася на момент t_i в *SUP* відносно y_i та x_i. При цьому, система логічних функцій описує залежності, що є актуальним в момент t_i для y_i та x_i. Така формула описується співвідношенням:

$$L(x_i, y_i) = L(y_i, x_i, t_i, P_i, W_i, d_i, a_i),$$

де P_i – поточне значення пріоритету суб'єкта y_i; W_i – тип повноважень, наприклад, читання, запис, зміна статусу об'єкта і т.д.; d_i – параметри, що характеризують y_i чи x_i на момент t_i, наприклад активність y_i; a_i – параметри, що характеризують критичні особливості суб'єкта або об'єкта, наприклад, міра відмов у наданні повноважень протягом деякого інтервалу часу $\Delta t_i = t_i - t_{(i-m)}$, L – логічна функція, яка використовує базові логічні зв'язки з множини $\{\&, \cup, \urcorner, \rightarrow\}$ [2]. Це означає, що на момент аналізу значення кожної змінної в L інтерпретується на множині $\{0,1\}$, значення яких визначається на множині обмежень, які складаються для кожного учасника процесу організації надання повноважень, якими є y_i та x_i. Інтерпретація всіх елементів системи *SUP* описується в текстовій формі. Цей опис, в залежності від подій, що можуть відбуватися в *SUP*, методами розширення текстових описів іншими текстовими фрагментами, заміни одних текстових фрагментів іншими, перестановки окремих текстових фрагментів в межах текстового опису та елімінації окремих текстових фрагментів. Ці перетворення описуються співвідношеннями:

$$h_i\left[J(x_i)\right] = h_i^p\left[n_1, n_2\right](g_{i1}, ..., g_{im}) \rightarrow \left(g_{i1}, ..., g_{i(j+1)}, g_{ij}, ..., g_{im}\right),$$

де h_i – функція перетворення текстового фрагмента $J(x_i)$; індекс p в h_i^p означає, що перетворення полягає у перестановці фрагментів тексту, які визначаються номерами n_1 і n_2. Таким чином, кожна функція h_i має параметри, які визначають в тій чи інший системі координат фрагменти $J(x_i)$ над якими передбачається проводити перетворення. У випадку $h_i^p\left[n_1, n_2\right]$ n_1 і n_2 визначають перестановку двох фрагментів з номерами n_1 і n_2 в межах $J(x_i)$. Після кожного перетворення $J(x_i)$, останнє перевіряється на предмет виявлення колізій в текстових описах. Якщо відповідні колізії виявлено то бітова інтерпретація відповідного x_i змінюється на протилежну. В таких випадках x_i приймає значення логічної змінної, що має інтерпретацію фальшивої величини, що переважно позначається цифрою «0».

Кожне перетворення $J(x_i)$ реалізується або реєструється в системі *SUP*. Такі події можуть бути зовнішніми та внутрішніми. До внутрішніх подій

відносяться всі події які реалізуються в *SUP* і обумовлюються процесами надання повноважень. Прикладом таких подій є відмова у наданні повноважень, зміна пріоритету суб'єкта, переведення об'єкта x_i в статус суб'єкта y_i та ін. Зовнішніми подіями є події введення в *SUP* нових суб'єктів, чи об'єктів, яке здійснюються через систему доступу *IS*.

Наступною компонентою яка включає в схему що описується матрицею *M* є компонента що реалізує визначення пріоритетів для суб'єктів y_i. Поточні пріоритети суб'єктів y_i в рамках матриці *M* визначаються порядком їх розміщення у першому стовпчику матриці, де вони розміщуються починаючи з другого рядка. У випадку, якщо б робота *SUP* по наданню повноважень виконувалась послідовно, шляхом переходу від одного y_i до іншого y_{i+1} і відразу ж, у випадку встановлення y_i запиту на повноваження, останній отримував би його, то черговий y_{i+1}, який виставив запит на співпрацю з цим же об'єктом змушений би чекати своєї черги. В рамках даної роботи на одному такті функціонування *SUP* всі y_i, які виставили запити на отримання повноважень аналізуються на предмет можливості надання їм таких повноважень. Це є особливо актуальним в тих випадках, коли кілька суб'єктів виставляють запити на роботу з одним і тим же об'єктом. В цьому випадку, в роботу включається система визначення пріоритетів для групи суб'єктів, у яких запити співпадають. Система визначення пріоритетів, в процесі аналізу суб'єктів аналізує такі характеристики:

- поточне значення пріоритету P^T, володіє y_i;
- функціональне значення пріоритету P^F для y_i;
- динаміку зміни пріоритетів в y_i (P^D);
- величину прикладного пріоритету P^P;
- величину пріоритету об'єкта P^O, до якого звернулися відповідні суб'єкти, яка формується на основі категорії k відповідного об'єкта та пріоритетів P^T всіх суб'єктів $y_i,\ldots, y_k$, які в поточний момент t_i звернулися за повноваженнями до одного і того ж об'єкта x_i.

Поточне значення пріоритету суб'єкта y_i визначається номером рядка, на якому розміщується y_i в матриці *M*. Цей пріоритет визначає послідовність в якій обслуговуються всі суб'єкти y_i на черговому циклі функціонування *SUP* оскільки номер пріоритету є унікальним, то номера пріоритетів інших суб'єктів змінюються у відповідності до прийнятої дисципліни, наприклад, суб'єкт який володів номером пріоритету, який присвоєно суб'єкту y_i отримує його попередній номер, або відбувається циклічна зміна пріоритетів у всіх суб'єктів починаючи від номера, який буд присвоєний суб'єкту y_i і т.д.

Функціональне значення пріоритету визначається мірою функціональної активності, яку проявляє суб'єкт y_i протягом деякого поточного періоду часу ΔT. Величина цього параметра впливає на величину поточного пріоритету і може ініціювати його зміну. Це означає, що у випадку, коли P^T є досить високим, а P^F – низьким, то система управління пріоритетами ініціює зміну пріоритеті для y_i таким чином, щоб P^T понизився до рівня який визначається

величиною P^F. Очевидно, що P^F може призводити до збільшення рівня P^T, якщо має виконується співвідношення, коли $P^T < P^F$.

Динаміка зміни пріоритетів в y_i, що позначається P^D є важливим параметром суб'єктів, оскільки характеризує y_i протягом часу, який є більшим від ΔT_i. Переважно цей параметр описує величину зміни P^T від одного циклу до іншого, оскільки ΔT_i вибирається таким чином, щоб величина циклу функціонування PS_i рівна $T_i(PS_i)$ була більша ΔT_i. динаміка зміни пріоритету P^D дозволяє проводити аналіз змін, що характерні окремим циклам роботи PS_i. На основі цього аналізу можна виявити факти підміни легального PS_i нелегальним, вияснити факт заміни одного PS_i іншим PS_j і т.д. Таким чином, P^D відносно PS_i носить глобальний характер і, завдяки цьому, стає можливим виявляти ознаки можливих атак на *IS* в цілому.

Прикладний пріоритет P^P є досить специфічним і відображає вимоги прикладних задач до пріоритетів в тих суб'єктів, які до них відносяться. У зв'язку з цим поточні пріоритети P^T, функціональні пріоритети P^F розглядаються в рамках груп суб'єктів, що об'єднуються за ознаками приналежності тій чи іншій прикладній задачі або SP_i. Пріоритет P^P, по визначенню має найвищий ступінь значимості відносно P^T і P^F. Зміна величини P^P може реалізовуватися лише засобами управління користувачами, які реалізуються на рівні управління задачами. В цьому підході значення пріоритету складається з двох показників: пріоритету PS_i та оперативного пріоритету. Для функціонального розширення можливостей управління об'єктами, крім уявлення про категорію об'єкту, використовується уявлення про пріоритет об'єкту P^O. Категорія об'єкту k_i визначається на основі аналізу даних, які знаходяться у відповідному об'єкті x_i, в процесі проведення якого розв'язується задача визначення актуальності чи значимості відповідних даних для прикладних систем, які можуть відповідні x_i використовувати в процесі функціонування PS_i. Критерії важливості тих чи інших даних для різних *PS* можуть бути різними для відображення цього аспекту використовується уявлення про пріоритет типу P^O. Пріоритети, як зазначалось вище , можуть змінюватися протягом інтервалу часу ΔT_i і тому вони є, в певному розумінні, оперативними показниками значимості суб'єктів. З точки зору вибору поточного суб'єкта для надання йому тих чи інших повноважень. Пріоритети P^P встановлюються на початковому етапі підготовки PS_i до функціонування в тому випадку, якщо відомо, що деякі об'єкти y_i будуть використовувати відповідні x_i, які належать іншим прикладним задачам. Якщо такої інформації немає, то початкове значення P^O=0. Якщо в процесі функціонування PS_i і PS_j, де $y_i \in PS_i$, а $x_j \in PS_j$ виявиться, що y_i звертається до *SUP* за повноваженнями на співпрацю з x_i, то в залежності від додаткових умов, які сформовані PS_j відносно власних об'єктів, *SUP* може надати повноваження для співпраці з x_i. Така співпраця може відображати організацію взаємозв'язку між відповідними PS_i і PS_j. В останньому випадку, використання пріоритетів P^P в класі пріоритетів різних прикладних систем задається в

рамках реалізації логіки співпраці між PS_i і PS_j.

Поточне значення пріоритетів для y_i таким чином пов'язане з функціональним типом пріоритетів. Величина функціонального пріоритету обчислюється на основі аналізу активності y_i. Як тільки виявляться, що $P^F \geq \alpha P^T$, то P^T заміняється новим значенням, яке відповідає P^F, а нове значення P^F обчислюється на поточному інтервалі ΔT_i. Пріоритет P^D є параметром, який змінюється в процесі функціонування *SUP* і безпосередньо, при наданні повноважень відповідному суб'єкту не використовується. Пріоритет P^P визначає порядок, або послідовність аналізу суб'єктів, які відносяться до окремого PS_i. Пріоритет P^O використовується системою *SUP* в тому випадку, коли суб'єкт y_i формує запит на послідовне використання ряду об'єктів $x_{i1},x_{i2},\ldots,x_{ik}$, з певними категоріями, значення яких дозволяють використання їх суб'єктом y_i значимість якого є c_i. Можливість послідовного використання суб'єктом ряду об'єктів на основі одного замовлення є новою і розглядається тільки в даній роботі. Умовою такого режиму надання повноважень суб'єкту y_i в *SUP* може бути надання y_i особливих повноважень відносно об'єктів. $x_{i1},\ldots,x_{ik}$, наприклад, якщо k_{ij} менша за c_i суб'єкта y_i у задане число разів, що записується таким чином:

$$\left[c_i\left(y_i\right) > m_i k_{i1}\left(x_{i1}\right)\right],\ldots,\left[c_i\left(y_i\right) > m_r k_{ir}\left(x_{ir}\right)\right],$$

де m_j – величина кратності значення k_{ij} для x_{ij}.

Розглянемо схему загальної організації процесу функціонування системи управління повноваженнями, яка наведена на рис. 4.1 і включає базові функціональні блоки *SUP*.

На рис. 4.1 використовуються такі скорочення:

IZP(Ci) – ініціація запиту на повноваження суб'єктом y_i;

Ki(Xi)≤Ci – перевірка, чи категорія ФОРМ є менша значимості c_i, яка характеризує суб'єкт y_i;

VOXi – вибір об'єкту x_i;

RNPYi – реалізація надання повноважень суб'єкту y_i відносно об'єкта x_i;

W(y)→D(Ci) – перевірка чи операція W_i, яку передбачає реалізовувати суб'єкт y_i є допустима для x_i;

Z(i) – M? – перевірка, чи всі запити на надання повноважень суб'єктам y_i проаналізовані;

VPNZ – обчислення по формулі L_i з ціллю визначення можливості надання повноважень суб'єкту y_i;

L(x,y) – перевірка, чи існує формула, що описує умови надання повноважень суб'єкту y_i відносно об'єкта x_i,

L(yi) – перевірка чи формула, що описує суб'єкт y_i не має аномалій;

VALF – визначення типу аномалій в L_i;

VLP – вивід логічної формули, що описує можливість надання повноважень суб'єкту y_i відносно об'єкта x_i;

AN – перевірка чи є аномалії у виведеній формулі;

UALF – усунення аномалій в логічній формулі;
VNP – відмова в наданні повноважень;
MZNP – модифікація запиту на надання повноважень;
ZIZ – завершення циклу надання запитів;
VDOW – визначення доступних об'єктів для суб'єкта y_i на повноваження W_i,
MLFY – модифікація логічної формули L для суб'єкта y_i;
DOV – перевірка чи додатковий об'єкт для y_i визначено;
FNTP – формування нового адреса для виробу чергового суб'єкта.

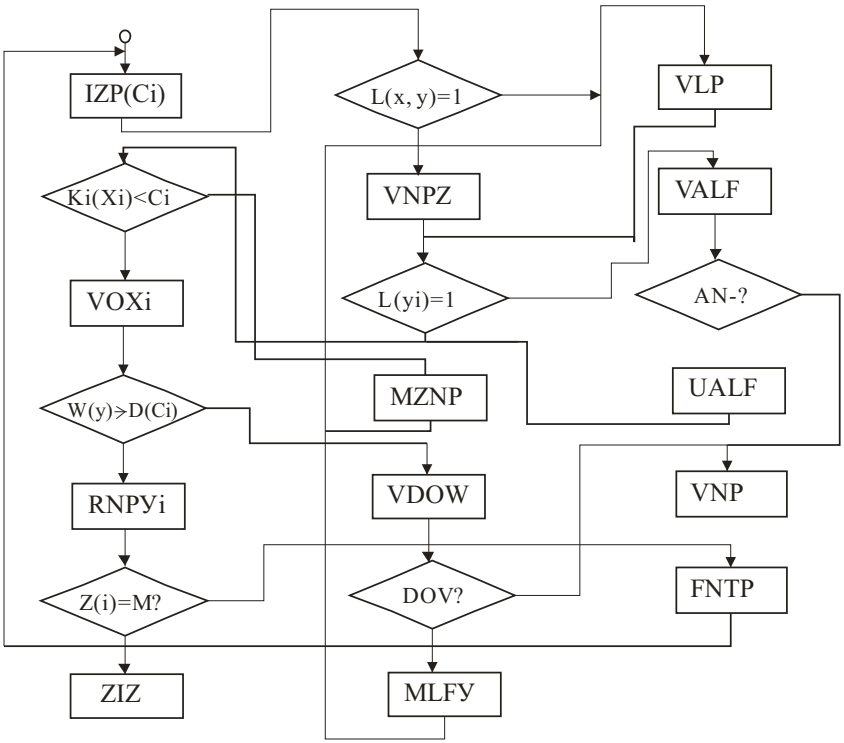

Рис. 1. Загальна схема організації процесу функціонування системи управління повноваженнями

Наведена на рис. 1 блок-схема відображає процес реалізації надання повноважень суб'єктам y_i, у випадку, коли останні сформували запити на отримання відповідних повноважень. В рамках *SUP*, окрім зазначених процесів, реалізується аналіз ситуації, що склалася в рамках системи і в першу чергу відображає рівень безпеки системи *SUP*. Тому розглянемо схему організації *SUP* в якій відображається аналіз рівня безпеки і на підставі

відповідного аналізу реалізуються процеси протидії виявленим атакам та процеси управління рівнем безпеки . Така схема наведена на рис. 4.2.

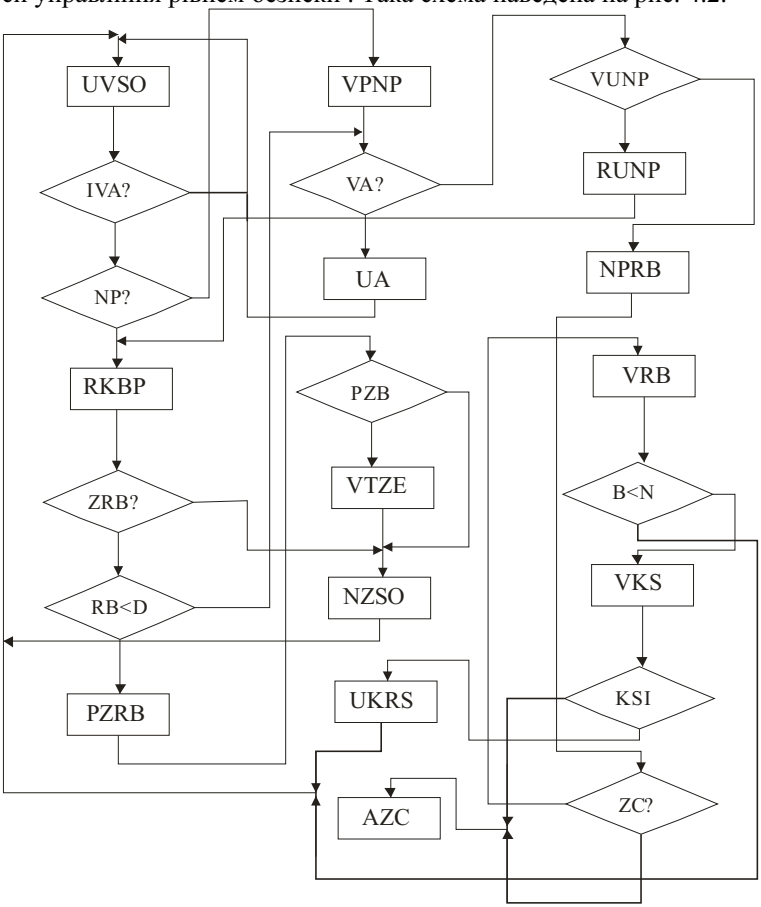

Рис. 2. Функціональна схема управління безпекою *SUP*

UVSO – управління взаємозв'язком суб'єкта з об'єктом;

IVA – перевірка чи активізована ініціація взаємодії чергового суб'єкта y_i з об'єктом x_i;

NP – перевірка чи надання повноважень є можливим;

RKBP – реалізація контролю безпеки, який проводиться перед наданням повноважень;

ZRB – перевірка чи змінився рівень безпеки при наданні поточних повноважень;

RB<D – чи рівень безпеки нижчий від допустимого;

PZRB – аналіз причин зниження рівня безпеки;

PZB – чи появилась загроза безпеці в *SUP*;

VTZE – виявлення типу загрози і її елімінація;

NZSO – встановлення зв'язку між суб'єктом і об'єктом;
VPNP – виявлення причини неможливості надання повноважень суб'єкту;
VA – чи виявлена аномалія;
UA – усунення аномалії;
VUNP – аналіз умов, які забезпечують можливість надання повноважень суб'єкту;
RUNP – реалізація умов надання повноважень;
NPRN – зниження рівня безпеки *SUP*;
VRB – визначення рівня безпеки *SUP*;
B ≤ N – чи рівень безпеки нижчий рівня надійності;
VRS – виявлення конфліктної ситуації *SUP*;
KSI – чи розпізнана конфліктна ситуація;
UKRS – усунення конфліктної ситуації;
AZC – аварійне завершення циклу;
ZC? – чи завершено цикл?

1. *Бенинч В. Е.* Введение в математическую теорию актуальных расчетов / *В. Е. Бенинч, В.Ю. Королев, С. Я. Шоргин.* – М. : МАКС-Пресс, 2002.
2. *Королев В. Ю.* Теория вероятности и математическая статистика / *В. Ю. Королев.* – М. : Проспект, 2005.

Поступила 14.03.2011р.

УДК 683.06

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

МЕТОД РЕАЛІЗАЦІЇ ПРОЦЕСУ ВИВОДУ ТЕКСТОВИХ ФРАГМЕНТІВ З ТЕКСТОВИХ МОДЕЛЕЙ

Аннотация

Исследуются методы реализации процесса вывода новых текстовых фрагментов в рамках текстовых моделей, которые используются для моделирования процессов функционирования сложно формализуемых объектов. В качестве таких объектов рассматриваются социальные объекты.

Ключевые слова: текстовая модель, вывод, текст, семантические параметры.

Однією з цілей створення та використання текстових моделей (TM_i) є управління об'єктами, які ними описуються. Однією з базових концепцій процесу управління текстовими моделями, яка представляє собою безпосередню реалізацію процесу управління, полягає у тому, що до текстового опису текстової моделі TM_i додається той чи інший фрагмент

