УДК 004.921

Б. В. Дурняк
Українська академія друкарства
Л. Е. Шведова
Кримський інститут інформаційно-поліграфічних технологій УАД

МЕТОДИ ФОРМУВАННЯ ПРАВИЛ УПРАВЛІННЯ ПОВНОВАЖЕННЯМИ

Визначено задачі взаємодії об'єктів із суб'єктами в системі управління повноваженнями, на основі яких сформовано правила і схеми таких взаємодій, які б не призводили до виникнення конфліктів у процесі функціонування інформаційної системи.

Правила, управління, повноваження, методи формування

Важливою компонентою системи управління повноваженнями (SUP) є складова, що забезпечує реалізацію взаємозв'язку між суб'єктами та об'єктами в процесі функціонування інформаційної системи (IS). У рамках цієї складової повинні вирішуватися задачі, пов'язані із забезпеченням таких типів взаємодій суб'єктів y_i з об'єктами x_i, як:

визначення актуальності відповідних повноважень у суб'єкта;

аутентифікація суб'єкта відносно об'єкта, і навпаки;

встановлення впливу відповідної взаємодії на рівень захисту системи;

виявлення неявних наслідків зниження рівня безпеки системи, що зумовлюються взаємодією уповноважених суб'єктів з відповідними об'єктами;

модифікації правил взаємодії та перетворень.

Задача визначення актуальності повноважень суб'єкта y_i відносно об'єкта x_i, за дозволом використання якого звернувся суб'єкт, розв'язується в різних типах систем, наприклад, у системі доступу користувачів до ресурсів обчислювальної мережі. Традиційний підхід до розв'язання цієї задачі полягає в наступному. У межах SUP існує матриця доступу A, яка може динамічно змінюватися і вміщає поточну інформацію про наявність або відсутність повноважень y_i відносно x_i. При цьому в A описуються типи повноважень. Більш ефективний метод розв'язання цієї задачі, досліджений у процесі даної роботи, полягає в тому, що умови доступу $y_i \rightarrow x_i$ розподіляються між матрицею доступу та суб'єктом y_i й об'єктом x_i. Завдяки такому розподілу з'являються певні особливості в управлінні повноваженнями:

підвищення безпеки роботи *SUP* за рахунок того, що вся інформація про наявність повноважень і, відповідно, доступу не зосереджена в одному місці, яким є матриця доступу A;

з одним і тим же об'єктом x_i на момент запиту доступу з боку об'єкт міг використовуватися іншим суб'єктом y_j, який отримав доступ до x_i і, відповідно,

може здійснювати в ньому ті чи інші зміни, що можуть призвести до виникнення конфліктів або суперечностей;

якщо рівень таємності для об'єкта x_i позначити як k_i, а суб'єкту властива значимість c_i та y_i має доступ до x_i, у результаті якого в ньому дописана інформація з рівнем таємності k_j, де $k_j > k_i$, то x_i потрібно поділити на дві складові x_i^1 і x_i^2 з різними k_i^1 і k_i^2; коли ж ці дві компоненти зв'язані між собою, то x_i повинен змінити свій рівень таємності з k_i на k_j (така зміна більш ефективна, якщо вона реєструється в рамках оточення об'єкта x_i, а не централізовано).

Наведені аргументи можуть бути розширені на основі аналізу різних ситуацій, виникання яких можливе в процесі функціонування *SUP*.

Приймемо *наступне визначення*. Взаємодія з x_i реалізується на основі аутентифікації суб'єкта та перевірки актуальності його повноважень. Кожний суб'єкт y_i, що отримав доступ до *I*S, одержує від *SUP* персональний ключ r_i, який є актуальним протягом періоду активного існування y_i в системі. Розглянемо детальніше розподіл даних або функцій між матрицею доступу *A,* суб'єктами й об'єктами та їхнім оточенням [1]. У даному випадку оточення об'єктів і суб'єктів сприймаємо як єдине ціле. Відповідне оточення складається з двох компонент: мобільної та власної. Власна компонента є невід'ємною частиною x_i чи y_i, а мобільна надається на час використання системою *SUP* на певний період. Персональна компонента вміщає дані про об'єкт, що характеризують його в поточний момент часу. До таких параметрів відносяться:

значення величини категорії, яка на даний момент відображає відповідний стан об'єкта;

міра поточної активності x_i чи y_i;

поточне значення ідентифікатора повноважень.

Активна компонента являє собою суб'єкт, який для функціонування використовує новий об'єкт, тоді відповідний об'єкт також знаходиться в стані активного функціонування. Міра активності визначається за кількістю суб'єктів та об'єктів, з якими протягом певного інтервалу часу відповідний суб'єкт взаємодіє. Аналогічно визначається й активність об'єкта. Під поточним значенням ідентифікатора розуміється:

наявність персонального ключа з числа активних на даний момент персональних ключів r_i;

рівень значущості класу суб'єкта c_i.

Значення величини категорії відносно значимості класу c_i суб'єкта y_i є підпорядкованим останньому [5]. Це означає, що об'єкти в цілому також підпорядковані суб'єктам. Тому взаємодію між y_i та x_i будемо розглядати як таку, що ініціюється відповідними запитами з боку y_i.

Загальна схема реалізації взаємодії y_i та x_i полягає в наступному. Суб'єкт y_i, який ініціалізується в результаті виникнення відповідних факторів, звертається до матриці доступу A, котра вміщає системні координати всіх об'єктів, що існують в рамках *IS*. Матриця доступу A надає персональний ключ r_i суб'єкту y_i, якщо останній ініціюється вперше протягом заданого інтервалу часу Δt_i.

Окрім того, матриця A ініціює для y_i функцію обслуговування взаємодії y_i з x_i. Кожен суб'єкт, що ініціюється в *IS,* повинен мати початковий показник величини значущості його класу c_i. На першому етапі реалізації такої взаємодії здійснюється аутентифікація y_i відносно певного x_i. Вона відбувається таким чином, що можна описати у вигляді послідовності:

1) y_i формує блок даних, в яких містяться значущість класу c_i, ідентифікатор y_i і коди типів повноважень w_i, що шифрується ключем r_i.

2) Об'єкт x_i, використовуючи функцію обслуговування φ_i, за допомогою відкритого ключа r_i^{-1} розшифровує отриманий блок даних і порівнює значущість класу c_i зі своєю категорією k_i.

3) Якщо $k_i \le c_i$, то y_i визначається як суб'єкт, що може працювати з об'єктом x_i. Якщо $k_i > c_i$, то $\varphi_i(x_i)$ аналізує умови, які встановлюють можливість співпраці y_i з x_i. До таких умов відносяться співвідношення:

$$(k_i - c_i) \le d_i(y_i, x_i); \tag{1}$$

$$\left[RO(y_i) \,\&\, RO(x_i)\right] \to \left[\left(c_i^* \ge k_i^*\right) \vee \left(k_i \le c_i^*\right) \vee \left(k_i^* \le c_i\right)\right]; \tag{2}$$

$$\alpha\left[y_i\left(W^1, ..., W^m\right)\right] \to \left[k_i\left(W^{i*}\right) \le c_i^*\right]. \tag{3}$$

4) Якщо співвідношення (1)–(3) не виконуються, то y_i отримує відмову в співпраці з x_i, а в матриці доступу фіксується факт звертання y_i до x_i.

Розглянемо детальніше наведені умови. Умова (1) означає, що різниця між k_i і c_i може мати певний поріг, який визначає можливість надання суб'єкту повноважень для використання x_i, коли ця різниця нижча за відповідний поріг або виконується умова $k_i > c_i$. Такий поріг $d_i(y_i, x_i)$ визначається на основі аналізу параметрів, що мають відношення до y_i та x_i. Один з цих параметрів визначає, наскільки змінився параметр, який встановлює значущість класу, що формально описується співвідношенням

$$\left(c_i^j(y_i) - c_i^{j-1}(y_i)\right) = \left[\delta(c_i, y_i) \,\&\, \left(\delta(c_i, y_i) > 0\right)\right].$$

Наступний параметр, який визначає $d_i(y_i, x_i)$, указує на кількість звертань y_i до x_i, котрі не були дозволені в рамках системи управління доступом, що реалізується системою повноважень. Обчислення цього параметра можна здійснювати на основі використання уявлень про інтенсивність ініціації суб'єкта y_i. При цьому необхідно враховувати тільки ті ініціації, які стосувалися запиту взаємодії y_i з x_i, що формально можна записати співвідношенням

$$m_j(y_i) = \sum_{i=1}^{n} \left[(i \to j) = e_i\right].$$

Наступним параметром, що бере участь у визначенні порога $d_i(y_i, x_i)$, є оцінка часу, протягом якого існує певний рівень взаємності або категорії в об'єкта x_i. Формально такий параметр можна описати співвідношенням

$$\tau\left(x_i, k_j\right) = \sum_{r=1}^{m} \Delta t_r\left(k_j\right),$$

де Δt_r — елементарний відрізок часу, протягом якого x_i має категорію k_j. Наведене співвідношення не відображає моменту, коли k_j повинен зменшитися. Найпростіший спосіб усунення недоліку встановлення деякого порогового значення для $\tau\left(x_i, k_j\right)$ — $\Delta\tau\left(x_i, k_j\right)$, після якого $\left(k_j \to k_{j-1}\right)$. Але в цьому випадку таке порогове значення повинне встановлюватися, а сама функція при досягненні вказаного порогу буде мати розрив. Більш об'єктивним способом розв'язання цієї задачі є використання функції для $\tau\left(x_i, k_j\right)$ у вигляді схеми

$$\tau\left(x_i, k_j\right) = \left[B\left(\sum_{r=1}^{m} \Delta t_r\left(k_j\right)\right)\right] \Big/ \left[B + \sum_{r=1}^{m} \Delta t_r\left(k_j\right)\right],$$

де B — деякий коефіцієнт зміни величини $\tau\left(x_i, k_j\right)$ при збільшенні кількості відрізків часу Δt_r. Вибір величини параметра B визначає динаміку процесу функціонування SUP щодо змін, які стосуються об'єкта x_i.

Співвідношення (2) загалом означає наступне. Оцінки $RO\left(x_i\right)$ та $RO\left(y_i\right)$ описуються функціональними залежностями, які можуть з різною мірою точності апроксимувати реальні залежності між параметрами, аргументами та величиною оцінки, що є результатом відповідних залежностей. У межах певного наближення для такої апроксимації можна використовувати логічні функції. Якщо взяти до уваги, що кінцевим підсумком відповідних перетворень є встановлення можливості або неможливості взаємодії y_i з x_i, для реалізації потрібного співвідношення необхідно сформувати певну інтерпретацію змінних, які використовуються у вказаному співвідношенні.

Оцінка об'єкта $RO\left(x_i\right)$ залежить від значення категорії k_i, котра присвоєна x_i та інтерпретується як різна міра таємності x_i від часу актуальності категорії k_i, кількості суб'єктів, що зверталися за використанням об'єкта x_i, й узагальненого класу суб'єктів, які зверталися за використанням x_i з урахуванням тих суб'єктів, що не отримали доступу. Кожен з цих параметрів допускає наступні бінарні інтерпретації.

Величина категорії або рівень таємності k_i існує під час аналізу стану x_i або не існує, що допускає використання двох значень $\{0,1\}$. Ситуація, коли x_i набуває інакшого значення рівня таємності k_j, описується в рамках іншого рівняння. Час актуальності поточного рівня таємності t_i допускає інтерпретацію, що означає, чи вичерпався час інтервалу Δt_i чи ні, що відображається бінарними значеннями. Зміна рівня таємності x_i приводить до встановлення нового інтервалу актуальності відповідної категорії k_j, що аналізується іншим логічним рівнянням або спричиняє потребу у формуванні чи виводі нового α_j.

Оскільки величина k_i може подаватись у дискретній формі, то доцільно ввести пороги дискретизації для величини m_i. Ураховуючи, що зміна величини m_i відбувається дискретно, порогом дискретизації m_i можна вважати Δm_i, що

визначає кількість суб'єктів, необхідну для відповідної зміни категорії k_i. Це призводить до неможливості використання бінарної інтерпретації m_i, через те що інша величина Δm_i відноситься до іншої логічної функції. Таким чином, якщо $m_i \geq \Delta m_i$, параметр m_i у логічній інтерпретації переходить із значення одиниці до значення нуля, або $(m_i = 1) \rightarrow (m_i = 0)$.

Аналогічна ситуація існує й щодо параметра η_i^*, оскільки її змінювання викликають дискретні зміни кількості y_i, кожен з яких має дискретну величину значущості класу c_i. Єдина відмінність $\Delta\eta^*$ від Δm полягає в тому, що $\Delta\eta^*$ може набувати дискретного значення.

Оцінка суб'єкта $RO(y_i)$ визначається: параметром k_i, до якого звертається відповідний суб'єкт; кількістю різних об'єктів, що використовуються суб'єктом n_i; інтенсивністю ініціації суб'єкта ρ_i. Перший параметр збігається з відповідним параметром k_i з оцінки x_i. Параметр n_i є дискретним, і для його бінарної інтерпретації використовується порогове значення Δn_i, перевищення якого параметром n_i викликає зміну бінарного значення параметра. Параметр ρ_i за способом його бінарної інтерпретації аналогічний параметру η_i^* з оцінки $RO(x_i)$.

Виходячи з вищенаведених інтерпретацій, можна записати такі логічні формули, що описують сформульовані вище умови (2) та (3):

$$\begin{aligned}&\left\{L_x\left[x_i^L(k_i), x_i^L(t_i), x_i^L(m_i), x_i^L(\eta_i^*)\right] \& L_y\left[y_i^L(n_i), y_i^L(\rho_i)\right]\right\} \rightarrow \\ &\rightarrow \left\{\left[y_i^L(c_i^*) \& x_i^L(k_i^*)\right] \vee \left[x_i^L(k_i) \& y_i^L(c_i^*)\right] \vee x_i^L(k_i^*) \& y_i^L(c_i)\right\}.\end{aligned} \tag{4}$$

Антицидент наведеного співвідношення являє собою диз'юнкт кон'юнктів, кожний з яких описує істинну кон'юнкцію при інтерпретації її елементів, що забезпечувала б виконання співвідношення між відповідними змінними, наведеними у формулі (2). Явний вигляд логічних формул L_x та L_y формується на основі інтерпретації співвідношень між відповідними логічними змінними, які приймаються в предметній області *IS* та системи *SUP*. Наприклад, якщо змінна m_i перейшла встановлений поріг значень, то ініціюється зміна величини k_i в її логічному відображенні таким чином, що $x_i^L(k_i)$ в L_x стає рівним нулю і формула L_x переходить у формулу L_x^1 так, щоб значення L_x^1 залишилося рівним одиниці, якщо зміна значення m_i в L_x привела до зміни значення L_x. Залежності між x_i^L та x_j^L в L_x не є однорідними. Це означає, що не для всіх $x_i^L \in L_x$ змінювання x_i^L приводить до зміни x_j^L. Наприклад, зміна рівня таємності k_i не спричиняє змінювання величини m_i, яка визначає кількість суб'єктів, що звертаються до x_i, оскільки це може бути пов'язано із зниженням актуальності даних відповідного об'єкта x_i.

Для опису всієї предметної області Q_i, в якій функціонує n суб'єктів, у рамках *SUP* використовується n логічних рівнянь типу (4). При зміні кількості суб'єктів змінюється число відповідних рівнянь. Природним розширенням (4) є відображення роботи одного суб'єкта y_i з цілим рядом об'єктів $x_{1i}, ..., x_{im}$.

Система *SUP* в цілому при використанні наведеного формалізму описується за допомогою системи логічних співвідношень, кількість яких відповідає числу активних y_i, що описуються системою співвідношень і складаються з логічних виразів, один з яких наведено нижче:

$$\left[L_y\left(y_{i1}^L,...,y_{im}^L\right)\&\,L_x\left(x_{i1}^L,...,x_{ik}^L\right)\right]\to V_{i=1}^r\left(y_i^c\,\&\,x_i^k\right). \quad (5)$$

Відповідно, система відображає стан *SUP*, що відповідає інтервалу Δt_i. Зміна логічного значення змінної в лівій частині наведеного співвідношення може викликати зміну значення формули в цілому. Це, в свою чергу, приводить до модифікації формули (5), яка формується шляхом логічного виводу $\alpha\left(L_y,L_x\right)\to\alpha^*\left(L_y,L_x\right)$. Ініціація такого виводу відбувається у випадку, коли $\left[\alpha\left(L_y,L_x\right)=1\right]\to\left[\alpha\left(L_y,L_x\right)=0\right]$.

Ціль модифікації $\alpha\left(L_y,L_x\right)$ полягає в тому, щоб $\alpha^*\left(L_y,L_x\right)$ стала рівною одиниці, що виражається у вигляді

$$\Phi\left\{\left[\alpha\left(L_y,L_x\right)=0\right]\right\}\to\left[\alpha^*\left(L_y,L_x\right)=1\right].$$

Іншою причиною модифікації системи α є активізація нового суб'єкта y_j у рамках *SUP*. Процес активізації y_j передбачає визначення хоча б одного x_j, на зв'язок з яким відповідний y_i претендує.

Розглянемо детальніше співвідношення (3), що описує залежності між різними типами повноважень. Прийнята ієрархія між типами повноважень обумовлюється можливим зв'язком між ними й типами порушень, що можуть відбуватися при несанкціонованих взаємодіях суб'єктів з об'єктами. Ці порушення можуть виникати через неузгодженість типів повноважень з рівнями таємності і величиною значущості окремих суб'єктів. Можливість виникнення таких ситуацій зумовлюється умовами, що існують у предметній області. Наприклад, окремі фрагменти даних, які можуть записуватися в деякий об'єкт x_i, можуть мати рівень таємності k_i, а суб'єкти y_i, відповідно, використовувати певні повноваження для доповнення даних *WD* величиною значущості c_i. Сукупність відповідних даних може мати вищий рівень таємності, що вимагатиме від об'єкта x_i вищої категорії $k_j > k_i$; y_i з нижчою значущістю c_i відносно об'єкта y_j, який має повноваження до x_i типу заміни даних *WZ* або знищення даних *WZ*, може читати дані, серед яких є фрагменти, дописані суб'єктами y_j, де $c_j < c_i$. Такі показники можуть понижувати рівень таємності загальних даних з точки зору їх реальної значущості для предметної області або для задач, в яких ці дані використовуються. Слід зазначити, що міра таємності за своєю суттю визначається значущістю задач, які використовують дані відповідних об'єктів x_i для предметної області, у котрій ці задачі розв'язуються [4]. На відміну від типів повноважень таку предметну область позначатимемо символом *Q*. Практично, у більшості Q_i і, відпо-

відно, в *IS* та *SUP*, міра значущості тих чи інших задач для Q_i визначається користувачами, які ці задачі розв'язують і використовують результати їх розв'язків [2]. При початковому формуванні *SUP* встановлення c_i, k_i та величин інших параметрів, що характеризують y_i та x_i з точки зору функцій *SUP*, здійснюється фахівцем, який описує відповідну Q_i. Для того щоб в процесі функціонування $IS \subset Q_i$ елімінувати або зменшити міру суб'єктивності при зміні параметрів c_i, k_i та інших, необхідно ввести критерії, які визначали б можливість автоматичної зміни параметрів, що використовуються при функціонуванні *SUP*. Як приклад таких критеріїв можуть бути умови, що відображають специфіку окремих Q_i та їхніх класів. При цьому доцільно формувати такі умови, які б існували для більш широкого класу предметних областей Q_i. До них належать:

міра зміни значень ключових параметрів відповідних Q_i, до яких можуть привести зміни параметрів, що характеризують y_i та x_i;

міра змін у системі логічних співвідношень, що описують SUP у різні періоди часу Δt_i;

міра змін параметрів, що використовуються в системі SUP і характеризують повноваження y_i та x_i;

зміна активності суб'єктів y_i протягом заданих інтервалів часу Δt_i;

кількість відмов у наданні системою SUP повноважень на використання об'єктів тощо.

Вищезазначені умови, на основі яких можуть бути сформовані критерії змінювання значень параметрів *SUP,* можуть бути розширені. Використання їх дозволяє поєднати проблеми безпеки відповідних *IS* із значущістю задач, що розв'язуються в її рамках.

При використанні систем логічних співвідношень типу (5) для управління системою *SUP*, виходячи із специфіки правил виводу, застосовуваних для модифікації $\left(L_x \,\&\, L_y\right)$, аксіом, що формуються як незмінні для даної *SUP* закономірності, й інших елементів, які являють собою розширення логічних функцій у межах *SUP*, можуть виникати ситуації, котрі допускають інтерпретації негативного характеру. До них відносяться:

виникнення суперечностей, які не обов'язково обмежуються їх логічною інтерпретацією [3];

поява конфліктів між окремими суб'єктами, ініціація яких може реалізовуватися в одні й ті ж інтервали часу;

виходи фрагментів логічних формул за межі предметної області інтерпретації;

поява неповноти логічних формул, що описують окремі процеси, ініційовані SUP;

виникнення необхідності в розширенні інтерпретацій, прийнятих на етапах інсталяції *SUP*.

Суперечності, які можуть виникати в процесі роботи *SUP* і мають інтерпретацію, ширшу за прийняту в математичній логіці, зумовлюються

наступним. Нехай в одній із формул (5) для y_i існує взаємозв'язок між параметрами k_i і c_i, який допускає інтерпретацію, що описує кон'юнкцію. В іншій формулі цього ж типу зв'язок між k_i і c_i, що відповідають суб'єкту y_i, описується логічний зв'язок, характерний для імплікації і має відповідну логічну інтерпретацію. Оскільки суб'єкти y_i і y_j відносно логічних функцій, що описують зв'язки між їхніми параметрами, ідентичні, то така розбіжність може означати потребу в розширенні інтерпретації відповідних зв'язків для y_i і y_j, що повинно усунути відповідну форму суперечності в системі логічних формул.

Для системи *SUP* виникнення конфліктів досить поширене явище, оскільки різні суб'єкти в один і той же інтервал часу Δt_i можуть звертатися за таким же об'єктом x_i і при цьому матимуть повноваження, використання яких є суперечними. Наприклад, суб'єкти y_i та y_j звертаються за поданням повноважень на співпрацю з x_i, і тип повноважень полягає в дописуванні даних і витиранні фрагментів даних і т. д.

1. Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин. — СПб., 2000. — 384 с. 2. Ван Гилборг Х. К. А. Основы криптологии. Профессиональное руководство и интерактивный учебник / Х. К. А. Ван Гилборг. — М. : Мир, 2006. — 471 с. 3. Кузнецов О. П. Дискретная математика для инженера / О. П. Кузнецов, Г. М. Адельсон-Вельский. — М.: Энергоатомиздат, 1988. — 480 с. 4. 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. 5. Тайли Э. Безопасность персонального компьютера / Э. Тайли. — Мн. : ООО «Понурри», 1997. — 480 с.

МЕТОДЫ ФОРМИРОВАНИЯ ПРАВИЛ УПРАВЛЕНИЯ ПОЛНОМОЧИЯМИ

Определены задачи взаимодействия объектов с субъектами в системе управления полномочиями, на основе которых сформированы правила и схемы таких взаимодействий, которые бы не приводили к возникновению конфликтов в процессе функционирования информационной системы.

METHODS OF FORMING OF RULES OF MANAGEMENT PLENARY POWERS

The tasks of co-operation of objects are certain with subjects in control system by plenary powers, which rules and charts of such co-operations, which would not result in the origin of conflicts in the process of functioning of the informative system, are formed on the basis of.

Стаття надійшла 12.05.11