УДК 004.056.52

ВИКОРИСТАННЯ ФОРМАЛЬНИХ ЗАСОБІВ ОПИСУ ПРОЦЕСІВ НАДАННЯ ПОВНОВАЖЕНЬ

Анатолій Давиденко, Олександр Суліма

В роботи розглянуто системи надання повноважень, які можуть мати різноманітну інтерпретацію, починаючи від представлення їх у вигляді матриць повноважень до представлення їх у вигляді приписування тих чи інших ролей користувачам, що звертаються за наданням повноважень. А саме проведено аналіз параметрів, що характеризують інформаційні системи типу з метою вибору найбільш адекватних формальних засобів для їх опису. Сформульовано ряд положень та визначень, які спрощують подібний аналіз в подальшому та визначена низка обов'язкових вимог щодо проведення цього аналізу. А саме дане визначення важливостіданих як параметру, який характеризує частоту використання даних за заданий період, на протязі якого відповідні дані використовуються. Також визначено мірутаємності даних через міру небезпеки, до якої може привести не санкціоноване використання даних при розв'язуванні задачі. Розглянуто поняття аномалії і доведено взаємозв'язок предметної області інтерпретації деякої системи на структурному рівні.

Ключові слова: *захист інформації, системи надання повноважень, формалізація засобів опису.*

1. Введення і постановка задачі

Системи надання повноважень можуть мати різноманітну інтерпретацію, починаючи від представлення їх у вигляді матриць повноважень аж до їх представлення у вигляді приписування тих чи інших ролей користувачам, що звертаються за наданням повноважень. Це свідчить про те, що для формального опису самих систем можна використовувати досить широкий спектр формальних засобів [1]. Для того, щоб використовувати найбільш адекватні формальні засоби по відношенню до інформаційних систем типу DIS, необхідно провести детальний аналіз параметрів, що характеризують систему.

Перший параметр, або перша особливість полягає у залежності між мірою таємності даних та кількістю користувачів, які можуть такими даними користуватися. Якщо позначити кількість користувачів, що звертаються за даними x_i символом h_i, а міру таємності даних x_i позначити $r_i(x_i)$, то можна записати наступну залежність:

$$r_i(x_i) = k_{Rz} / m h_i(\alpha), \qquad (1.1)$$

де m – кількість користувачів h_i, кожний з яких може мати певний рівень власної міри безпеки, яка описується величиною, α, $0 \prec \alpha \le 1$, k_{Rz} – коефіцієнт пропорціональності, який визначає рівень максимальної міри таємності. Якщо $\alpha = 1$ і $m = 1$, то $r_i(x_i) = \max r_i(x_i) = K_{RZ}$. Використання коефіцієнта α дозволяє величину зміни рівня захищеності представити як неперервну величину, яка може приймати проміжні значення між дискретними значеннями рівня таємності. Коефіцієнт α може використовуватися лише в тому випадку, коли кількість користувачів $m \succ \beta$, де, наприклад, $\beta \succ 4$. В загальному можна написати наступну умову, якій повинна задовольняти величина $\alpha : \sum_{n=1}^{m} h_i(\alpha) \ge 1$. Формулу (1.1) можна записати у наступному вигляді:

$$r_i(x_i) = K_{RZ} / \sum_{i=1}^{m} h_i(\alpha_i). \qquad (1.2)$$

Виходячи з цієї особливості, може скластися враження, що необхідний рівень таємності $r_i(x_i)$ може визначатися кількістю користувачів і не залежати від інших факторів, наприклад, міри небезпеки пониження рівня таємності. Цей фактор, в рамках даного підходу, також повязується з користувачем за рахунок використання параметра α_i. Цей параметр представляє собою дробову величину, використання якої приводить до того, що використання даних x_i користувачем $h_i \alpha$, якщо $\alpha \ne 1$, обумовлює ріст міри захищеності, який стає більшим $K_{RZ,}$ або $r_i(x_i) \succ K_{RZ.}$. З точки зору інтерпретації співвідношення (1.1), це означає наступне. Якщо $\alpha_i = 0{,}5$ для $h_{i,}$ то особистий параметр, що характеризує пониження рівня безпеки через надання h_i даних x_i, характеризує властивістю самого користувача, який може інформацію про ці дані розповсюдити між іншими користувачами, які можуть бути не уповноваженими до отримання даної інформації. Таким чином, якщо виявиться, що у відповідності з (1.1), або з (1.2) встановлений рівень таємності з допомогою коефіцієнта K_{RZ}

зріс, то цей факт повинен знайти своє відображення в засобах захисту, які повинні такий рівень захисту для x_i збільшити. Формально, це може описуватися у вигляді наступного логічного співвідношення зростання таємності[2]:

$$\{[K_{RZ} / h_i(\alpha_i)] \to (K^*_{RZ} \succ K_{RZ})\} \to [r_i(x_i) \to [r^*_i(x_i) = [K^*_{RZ} / h_i(\alpha_i)]]].$$

Приведене співвідношення описує зміни, які повинні відбутися в системі надання повноважень $(SNP,)$ якщо виникає ситуація, коли h_i має доступ до даних $x_{i,}$ але його характеристика власної міри безпеки α_i, яка задається в рамках самої системи DIS, не надає йому змоги отримати повноваження на виконання певних дій з даними $x_{i,}$ що мають міру таємності $r_i(x_i)$.

Друга особливість полягає у тому, що міра таємності з часом зменшується в залежності від того, які дії чи зміни відбуваються з x_i. [3] Якщо x_i використовуються часто, то таке зменшення $r_i(x_i)$ протікає скоріше в часі, якщо x_i використовується не часто, то зміни відбуваються повільніше. Якщо x_i взагалі не використовується, то зміна значення $r_i(x_i)$ може відбутися раптово через певний проміжок часу. Формально це описується наступними співвідношеннями:

$$\{(m(x_i) = 0) \& (\delta t_i(x_i)) \geq \Delta T_i(x_i)\} \to [(r_i(x_i) = 0) \& (x_i \notin DIS)],$$
$$[(m(x_i)/\Delta t) \to 0] \to [r_i(x_i) \to \min r_i(x_i)]. \quad (1.3)$$

Приведена особливість, як і особливість попередня, визначає міру таємності, або $r_i(x_i)$ не залежно від абсолютної вартості даних x_i. Говорити про такого типу вартість даних є сенс тільки в тому випадку, коли можуть виникнути задачі, длярозв'язку яких можуть виявитися відповідні дані необхідними. Для встановлення таких фактів, необхідно проводити аналіз описів інтерпретації відповідних даних. Приймається, що тільки такий опис повністю може описувати рівень активності даних, рівень їх значимості, який оцінюється мірою $r_i(x_i)$. Інтерпретаційний опис даних представляє собою наступне формальне представлення x_i, що описується співвідношенням:

$$j(x_i) = < a_{i1} * ... a_{in} > \mathrm{I} < \lambda_{i1}, ..., \lambda_{im} >,$$

де a_{ij} – окремі фрази, чи слова на мові користувача, які в сукупності, у відповідності з граматикою відповідної мови, описують в повній мірі величину x_i, яка фактично є лише ідентифікатором $j(x_i)$, λ_{ij}-параметри, які використовуються для доповнення інтерпретаційного опису, що формується з допомогою $a_{i1}, ..., a_{in}$. Будь який інтерпретаційний опис $j(x_i)$ може бути не повним. На момент формування DIS приймається, що $j(x_i)$ є повним в рамках задач, на які орієнтована система DIS. Це означає, що система надання повноважень $SNP,$ для розв'язку задач, може використовувати $j(x_i)$ і, відповідно задачі, для розв'язування яких користувач передбачає використовувати відповідні дані $x_{i.}$

2. Аналіз рівня таємності

У відповідності із співвідношенням (1.3), $r_i(x_i) \to \min r_i(x_i)$, якщо кількість запитів x_i зменшується, або зменшується інтенсивність цих запитів, що не до кінця повно відображає досліджуваний фактор. Тому, введемо наступне положення.

*Положення*1.1. Рівень таємності довільних даних x_i з часом зменшується не залежно від інтенсивності використання x_i для розв'язку задач.

У зв'язку з цим, виникає необхідність розділити уявлення про значимість даних x_i та міру їх таємності. Розглянемо наступні визначення, яких будемо дотримуватися в рамках даної роботи.

Визначення 1.1. Важливістю даних x_i будемо називати параметр, який характеризує частоту використання даних за заданий період, на протязі якого відповідні дані використовуються. Формально, це визначення описується співвідношеннями:

$$\aleph(x_i) = [m_j(x_i)/\Delta t_j] + \sum_{j=1}^{N} \Delta t_j,$$

де $\aleph(x_i)$ - значимість даних, що ідентифікуються змінною $x_{i,}$ m_j - кількість запитів на використання даних x_i за встановлений проміжок Δt_i, N- деяке число $N \succ n$, де n - довільне ціле число визначає кількість Δt_i, що відповідає часу, на протязі якого використовується x_i.

Визначення 1.2. Міра таємності $r_i(x_i)$ даних x_i визначається мірою небезпеки, до якої може привести не санкціоноване використання x_i, при розв'язуванні задачі $z(x_i)$.

Міра небезпеки, яку будемо позначати символами nb_i,визначається для середовища, в рамках якого описується ціль $c_i(z_i)$ задачі $z_i(x_i)$. Міра небезпеки $nb_i(x_i)$ не означає, що ця міра безпосередньо визначає величину таємності $r(x_i)$. Це зв'язано з тим, що визначення міри небезпеки розв'язку несанкціонованої задачі, яка використовує дані x_i, для певної предметної області, представляє собою досить складну задачу, в якій необхідно враховувати цілий ряд факторів та їх різні інтерпретації. Тому, в більшості випадків, оцінка $nb_i(x_i)$ проводиться експертним способом. В якості експерта вибирається фахівець, який є знайомим з відповідною предметною областю, в якій розв'язується задача [4]. Відповідний експерт на основі представленої шкали рівнів таємності, визначає величину $r_i(x_i)$ в DIS. Якщо DIS використовується в різних предметних областях W_i, то $r_i(x_i)$ вибирається по тій предметній області W_i, для якої величина $r_i(x_i)$ є максимальна. Зниження рівня таємності $r_i(x_i)$ з часом їх існування будемо називати старінням параметру $r_i(x_i)$. Зниження рівня важливості $\aleph(x_i)$ будемо називати старінням даних x_i. Процес старіння в одному і другому випадку будемо позначати символом S і формально цей процес будемо описувати наступними співвідношеннями

$$S[r(x_i)] = f_r(m_i(x_i), \Delta T(x_i)).$$

Для випадку старіння значимості даних $\aleph(x_i)$, відповідний вираз в неявній формі записується аналогічно: $S[\aleph(x_i)] = f_\aleph(m_i(t_i))$. Оскільки старіння $r_i(x_i)$ та $\aleph(x_i)$ представляють собою процеси, то необхідно описати логіку перебігу цих процесів. Такий опис представляє собою наступні співвідношення:

$$[r(x_i) \& (\Delta t_i(x_i) \to \Delta T_i)] \to [(r(x_i) \to 0)],$$
$$[\aleph(x_i) \& (m(x_i) \to 0)] \to (\aleph(x_i) \to 0).$$

Очевидно, що ці співвідношення можна представити в аналітичній формі, але ця форма буде залежати від W_i та інших факторів, тому, в даному випадку, не будемо їх формувати. Задачі, що розв'язуються на основі використання даних DIS, тісно пов'язані не тільки з установою, що є власником DIS, а із параметрами, що характеризують $x_i \in DIS$. Одним зтаких параметрів є параметр таємності $r(x_i)$. В найпростішому випадку такий зв'язок представляє безпосередню залежність між $r(x_i)$ то $r[z_i(x)]$, яка представляє собою наступне:

$$[r(x_i) \& (x_i)] \to \{(r(x_i)) = r[z(x_i)]\}.$$

Такий підхід не є оптимальним, оскільки він приводить до необхідності надавати $r(x_j)$ де $x_j \in DIS$, якщо $x_j \in z(x_i, x_j)$. Оскільки в рамках $z_i(DIS)$ можуть існувати запити не тільки на дані, а і на процеси, які будемо позначати $y_i = e(x_{i1},..., x_{im})$, то і відповідні процеси, які використовують x_i з $r_i(x_i)$ також повинні отримувати високий рівень таємності. Для вирішення цієї проблеми, якщо $r(z_i(x_i)) \prec r(x_i)$, то вся задача, або фрагмент задачі, в якому використовується x_i передається для розв'язку до додаткових засобів DIS. Крім того, система SNP розв'язує задачу визначення можливостітимчасового пониження $r_i(x_i)$ до $r_i^*(x_i)$, де $r*(x_i) \prec r(x_i)$, яке можливо за рахунок того, що дані, які отримані в результаті розв'язку задачі $z(x_i,..., x_k)$ не розкривають, або не понижують таємності $r(x_i)$. Ця задача зводиться до аналізу міри оберненості алгоритму, який використовує $z(x_i,..., x_k)$. Це не означає, що SNP повинна проводити цей аналіз самостійно. Достатньо, щоб користувач, при зверненні за повноваженнями стосовно x_i, надавав системі відповідну інформацію. Це означає, що SNP повинна використовувати не тільки інформацію, що характеризує задачі а і інформацію, яка стосується алгоритму самої задачі z_i. Важливими даними, що використовуються SNP є дані про задачу, які полягають у наступному:

- ціль розв'язку задачі $c(z_i)$,
- наявність повноважень у h_i на розв'язок z_i,
- параметри задачі z_i,
- інші зовнішні засоби, які повинна використовувати задача z_i в процесі розв'язку,
- додаткові параметри, що можуть стосуватися користувача відповідної задачі.

Ціль розв'язку задачі оцінюється окремими параметрами, які приписуються їй незалежно від

DIS, з якою ця задача передбачає співпрацювати. Параметри цілі визначаються на основі W_i, в рамках якої розв'язується задача. Прикладом таких параметрів можуть служити міра таємності цілі $r(c_i(z_i))$, міра значимості цілі $\aleph[c_i(z_i)]$, міра відповідності предметної області цілі задачі $W_i[c_i(z_i)]$ предметній області на обслуговування якої орієнтована DIS, або $W_j(DIS)$. Очевидно, що DIS може бути орієнтована на цілий ряд предметних областей, або $DIS_i(W_i, W_{i+1},..., W_m)$. Наявність повноважень у h_i є додатковими характеристиками користувача, які не пов'язані безпосередньо з ідентифікацією та аутентифікацією користувача. Повноваження користувача $p(h_i)$ визначаються наступними параметрами задачі

– мірою таємності задачі $r(z_i)$,

– мірою значимості задачі $\aleph(z_i)$,

– параметрами, що характеризують ціль задачі $p[c(z)]$,

– мірою актуальності задачі для $W_i(DIS)$, якщо основна предметна область інтерпретації задачі $W_j \neq W_i$, яку будемо позначати $a[z_i(W_i)]$,

– кількість таємних даних, що використовуються в задачі, що мають високі рівні таємності з вибраного діапазону цих рівнів $kr_i(x_i,..., x_n)$.

Формально це можна записати у вигляді:

$$p(h_i) = f\{r_i(z_i), \aleph_i(z), p[c(z_i)], a[z_i(W_i)], kr_i(x_i,..., x_n)\}.$$

Параметр $p(h_i)$ не мусить бути залежним від всіх компонент. У випадку, коли параметр $p[c(z_i)]$ представляє собою рівень таємності цілі $r[c(z_i)]$, то існує можливість співставити його з $r(x_i)$, який передбачається використовувати для розв'язку задачі z_i. Аналогічно, актуальність задачі можна привести до параметра значимості задачі. Приведені випадки записуються у вигляді

$$p[c(z_i)] \to r[c(z_i)] \to r(x_i,..., x_m);$$
$$a[z_i(W_i)] \to \aleph_i(z_i).$$

Параметр $kr_i(x_i,..., x_n)$ є більш складним. Ця складність обумовлюється тим, що,при визначенні рівня таємності, не допустимо встановлювати між ними лінійну залежність, а спільне використання різних x_i, x_j, x_k з найвищими рівнями таємності $r_i(x_i), r_j(x_j), r_k(x_k)$ не обов'язково приводить до того, що $r_e(x_e) = F(x_i, x_j, x_k)$ буде приймати максимальне значення рівня таємності з уже встановлених рівнів. Формально, це описується наступним співвідношенням:

$$\{r_e(x_e) = Ae[r_i(x_i), r_j(x_j), r_k(x_k)]\} \to$$
$$\to \{\{r_e(x_e) = \max[r_i(x_i), r_j(x_j), r_k(x_k)]\} \vee$$
$$\{[r_e(x_e) \succ \max(r_i(x_i), r_j(x_j), r_k(x_k))]$$
$$\vee [r_e(x_e) \prec \max(r_i(x_i), r_j(x_j), r_k(x_k))]\}\}.$$

Співвідношення $r_e(x_e) = \max[r_i(x_i), r_j(x_j), r_k(x_k)]$ відповідає присвоєнню максимальної міри таємності результату перетворень $F[r_i(x_i), r_j(x_j), r_k(x_k)]$. Алгоритм Ae_i, вибирає серед заданих для x_i, x_j, x_k мір таємності, який відповідає для $r_e(x_e) = [r_i(x_i), r_j(x_j), r_k(x_k)]$. Ситуація, коли міра таємності $r_e(x_e) \succ \max[r_i(x_i), r_j(x_j), r_k(x_k)]$ є більш складна і потребує більш детального аналізу. Міри таємності в DIS визначаються не тільки для даних а й для фрагментів алгоритмів, які можна вважати окремими функціями, що використовуються в рамках розв'язку задач доступу і, в першу чергу, в рамках розв'язку задач надання повноважень користувачам в DIS. Такі функції будемо називати φ_i. Система мір таємності $R\{r_i,..., r_m\}$ та система значимостей $\Im\{\aleph_1,..., \aleph n\}$ визначаються на основі використання описів текстових інтерпретацій всіх даних $j(x_1),..., j(x_n)$, які розміщаються в DIS та основі текстових описів інтерпретацій всіх елементів бібліотеки всіх функцій $\varphi_i = \{j(\varphi_1),..., j(\varphi_k)\}$. Основою для цього є опис інтерпретації предметних областей, до яких відносяться DIS, або $W_i(DIS)$. Для вирішення задачі визначення рівнів таємності та значимості використовуються критерії для r_i та $\aleph_i$, а процеси визначення конкретних значень $r_i(x_i)$ та $\aleph_i(x_i)$ реалізуються шляхом використання семантичного аналізу [4]. В даному випадку, розглянемо задачу, яка полягає у визначенні міри таємності r_i, яка є вища від встановлених рівнів таємності, при формуванні DIS, для даних $x_i \in DIS$ та $\varphi_i \in DIS$.

Перш ніж доводити можливість виникнення необхідності приведення міри таємності

$r_i(x_i) \succ r_j(x_j)$, до $r_j(x_j) = \max$, розглянемо цю ситуацію на якісному рівні. Уявлення про таємність r_i тих, чи інших даних є необхідним лише для того, щоб не допустити можливих аномалій на деякому фрагменті $W_i(DIS)$. Введемо визначення аномалії для W_i.

Визначення 1.3. Аномалією An_i в W_i будемо називати наступні ситуації, що можуть виникати в W_i:

- виникнення структурної суперечності в W_i,
- виникнення логічної суперечності в W_i,
- виникнення семантичної суперечності в W_i.

Структурна суперечність відповідає такій ситуації, коли в рамках структури W_i не може бути розв'язана задача, яка на структурному рівні полягає у побудові шляху від однієї вершини структури до довільної іншої вершини. Ця аномалія суперечить принципу зв'язності предметної області W_i.

3. Аналіз предметної області

Розглянемо наступне положення.

Положення 1.2. Предметна область інтерпретації деякої системи є завжди зв'язна на структурному рівні.

Структурна аномалія може мати місце в тому випадку, якщо існує в структурі вершина, з якої не має виходу. Необхідність виходу з довільної точки повязується з відкритістю предметної області $W_i(DIS)$. Логічна аномалія al в DIS ілюструє той факт, що в рамках W_i існує логічна не відповідність між різними компонентами W_i. Введемо наступне положення.

Положення 1.3. Предметна область W_i не вміщає логічних суперечностей.

Оскільки логічна суперечність пов'язана з семантичною суперечністю відповідної області інтерпретації, то їх на якісному рівні розділяти не будемо. Оскільки, будь який опис предметної області формується для того, щоб в рамках відповідної області розв'язувався певний клас задач, то формувати її таким чином, щоб могли виникнути умови, що не дозволяють розв'язувати задані задачі не доцільно. Відповідні аномалії можуть виникати лише в тих випадках, коли W_i розширяється в процесі її використання.

Твердження 1.1. Якщо в DIS існує $R = \{r_1,...,r_m\}$ така, що $r_1 \prec r_2 \prec ... \prec r_n$, то система R може бути розширена $r_{mt} \succ r_m$.

Приймемо, що в SNP існує $R = \{r_1 \prec r_2 \prec ... \prec r_m\}$. Обмежимося двома рівнями r_i і r_j. Це означає, що існує $r_i(x_i)$ і $r_j(x_j)$. Кожна міра r_i і r_j визначаються на основі використання критеріїв $k_1,...,k_m$. Оскільки r_i і r_j представляють собою деякі константи, а k_i - представляють собою опис певних умов, що зв'язані з $r_i,...,r_m$, то в рамках W_i повинні існувати правила з допомогою яких можна пов'язати k_i та r_i. Приймемо, що такими правилами є $P_1, P_2,..., P_k$. Оскільки $r_i(x_i)$, то це означає, що існує $j(x_i)$. Інтерпретація $j(x_i)$ виводиться з $J(W_i)$ у відповідності з системою залежностей $x_i = f(x_j, x_{j+1},..., x_m)$. Оскільки всі $x_i \in W_i$ мають $j(x_i)$, то і всі $f_i(x_j,..., x_m)$ мають інтерпретацію $j[f_i(x_j,..., x_m)]$. Критерії k_i формуються в рамках W_i. Це означає, що правила $P_i[k_i, r_i, (x_j,..., x_m)]$ є виводимі в системі $\{\{k_1,..., k_m\}, \{r_1,..., r_k\}, W_i\}$. Приймемо, що в W_i реалізується деякий алгоритм $Al_i(x_i, x_j)$ такий, що $Al_i(x_i, x_j) \to x_i^*$. При цьому, $x_i^* \notin DIS$. Оскільки кожний k_i визначає окремий діапазон значень на $R = \{r_1,..., r_m\}$ і $r_1 \prec r_2 \prec ... \prec r_m$, то для x_i^* може існувати $j(x_i^*)$, яка приводить до виникнення суперечності в W_i. Для усунення відповідної суперечності, необхідно реалізувати розширення W_i. Оскільки x_i^* виникло в результаті виводу $Al_i(x_i, x_j) \to x_i^*$, то $x_i^* \in W_i$. Це означає, що $J(W_i) \to j(x_i^*)$. Критерії k_i представляють собою описи інтервалів, які розміщуються на відрізку їх визначення без розривів. Тому, для розширення критеріїв є дві можливості. Додавання відрізку перед k_1 і додавання відрізку після k_m. Розширення k_1 в сторону k_{i-1} не має сенсу, оскільки це приведе до того, що $x_i^* \in \{x_{i1},..., x_{ir}\}$ для яких r_1 визначає вільний доступ до даних. Але такі x_i^* не можуть

привести до аномалії в W_i, оскільки вони є базовими для W_i. Тому, необхідно проводити розширення k_m до k_{m+1}. Тоді, k_{m+1} визначає рівень таємності r_{n+1}, для якого виконуються співвідношення $r_{n+1} \succ r_n$. Оскільки $Al(x_i, x_j)$ не є суперечливим, то аномалія до якої приводить x_i^* є семантична. Для усунення цієї аномалії використовується надання x_i^* нової категорії рівня таємності r_{m+1}. Для побудови $j[r_{m+1}(x_i^*)]$ використовується вивід, що формується на основі використання наступних компонент:

– $j[Al_i(x_i, x_j)]$ - текстова інтерпретація алгоритму Al_i,

– $j[k_1,...,k_m]$ - текстова інтерпретація критеріїв,

– $j(x_i)\,\&\, j(x_j)$ - текстові інтерпретації даних з DIS, що формуються на основі $J[W_i(DIS)]$.

Тоді можна записати наступне співвідношення:

$$\{j[Al_i(x_i, x_j)\,\&\, j(k_1,...,k_m)\,\&\, J[W_i(DIS)]]\} \rightarrow \rightarrow j[r_{m+1}(x_i^*)].$$

Міра таємності деяких даних залежить від кількості задач, які для свогорозв'язку використовують дані відповідного рівня таємності. Оскільки, рівень таємності $r(x_i)$ залежить від кількості користувачів, що звертаються до DIS за відповідними даними, то можна прийняти наступну інтерпретацію. Кожна окрема задача z_i приписується окремому користувачу h_i. В цьому випадку ми приходимо до ситуації яка уже розглядалась і полягає у тому, що міра таємності знижується із збільшенням кількості користувачів, що використовують відповідну таємну інформацію x_i.

Приймемо, що не існує можливості окремі задачі приписувати окремому користувачу. В цьому випадку, результатирозв'язку кожної окремої задачі використовуються в W_i. Кожне з таких використань розширює W_i, оскільки привносить нову інформацію в W_i, яка має свою власну інтерпретацію, або $x_k = f(x_i, x_m)$ приводить до того, що $[j(x_k)\,\&\, j(f(x_i, x_m))] \rightarrow j(x_k)$, при цьому, $j(x_k) \in J(W_i)$, а f_i визначає задачу z_i. При збільшенні кількості $z_i[r_m(x_k)]$ збільшується кількість текстових описів $J(x_i)$, що розширяють $J(W_i)$. [5] Це означає, що між $(x_{k1}^*,..., x_{km}^*)$ та середовищем W_i появляються додаткові зв'язки.

Тому, кількість елементів з W_i, що на структурному та логічному рівні отримають зв'язок з $\{x_{i1}^*,..., x_{im}^*\}$, збільшується. У відповідності з прийнятною тезою, рівень таємності r_i залежить від кількості користувачів, які можуть звертатися за x_{ki}^*, оскільки збільшення зв'язків між елементами еквівалентне збільшенню можливих задач, які можуть розглядатися в рамках деякої системи.

4. Висновки

Параметри, що визначають взаємозв'язки між даними, суттєво впливають на роботу SNP. Якщо дані x_i мають $r_i(x_i)$, а x_j мають $r_j(x_j)$ та $r_i \prec r_j$, то може виявитися, що користувач h_i використовуючи x_i, завдяки існуванню $x_j = \varphi(x_i)$ може не санкціоновано дістатися до x_j. Щоб цього не допустити, SNP повинна перевіряти можливість реалізувати функції типу $\varphi(x_i)$ в оберненому напрямку. Це означає, що SNP повинна аналізувати близькість різних даних в DIS. В даному випадку, віддаль між різними елементами x_i і x_j з DIS визначається мірою складності перейти від одних даних до інших за рахунок зв'язку між ними. Якщо така віддаль є недостатня для забезпечення заданої дисципліни розподілу даних по мірі r_i, то необхідно вводити на відповідний зв'язок рівень таємності r_i.

ЛІТЕРАТУРА

[1]. Зайченко Ю.П. Основи проектування інтелектуальних систем. / Ю.П. Зайченко – К.: Слово, 2003

[2]. Зима В.М. Безопасность глобальных сетевых технологий / В.М. Зима, А.А. Молдовян, Н.А. Молдовян – СПб.: БХВ-Петербург. 2000.

[3]. Коростіль О. Ю.-Ю. Засоби опису методів синтезу текстових моделей з текстовими інформаційними потоками / О. Ю.-Ю. Коростіль // Моделювання та інформаційні технології : зб. наук. пр. ІПМЕ ім. Г. Є. Пухова НАН України. – К., 2012. — Вип. 63. — С. 95–104. Мендельсон Э. Введение в математическую логику. / Э. Мендельсон – М.: Наука, 1971.

[4]. Тихомиров Н.П., Дорохина Е.Ю. Econometrika. М.: Екзамен, 2007.

REFERENCES

[1]. Zaichenko Yu.P. Fundamentals of Intelligent Systems. / Yu.P. Zaichenko - K .: Slovo, 2003

[2]. Zyma V.M. Safety of Global Network Technologies / V.M.Zyma, A.A. Moldovyan, N.A. Moldovyan - St. Peterburg .: BHV-Peterburg. 2000.

[3]. Korostil A. Yu.-Yu. Means describe methods of synthesis of text models with text information streams / A. Yu.-Yu. Korostil // Modelling and Information Technology: Coll. Science. pr. IPM them. GE Puchov NAS of Ukraine. - K., 2012. - Vol. 63 - P. 95-104. E. Mendelson Introduction to matematycheskuyu logic. / E. Mendelssohn - M .: Science, 1971.

[4]. Tikhomirov N.P., Dorohyna E.Y. Econometrics. M .: Examination, 2007.

ИСПОЛЬЗОВАНИЕ ФОРМАЛЬНЫХ СРЕДСТВ ОПИСАНИЯ ПРОЦЕССОВ ПРЕДОСТАВЛЕНИЯ ПОЛНОМОЧИЙ

В работе рассмотрен широкий спектр систем предоставленияполномочий от систем с представлениемих в виде матриц полномочий, до систем с определениемописаниятехили иных ролей пользователям, обращающихся за предоставлением полномочий. А именно проведен анализ параметров, характеризующих информационных систем типа *DIS* с целью выбора наиболее адекватных формальных средств для их описания. Сформулирован ряд положений и определений, которые упрощают подобный анализ в дальнейшем и определен ряд обязательных требований что к проведению этого анализа.А именно данно определение важности данных как параметра, который характеризует частоту использования данных за заданный период, в течение которого соответствующие данные используются. Также определена мера секретности данных через степень опасности, которой может привести не санкционированное использование данных при решении задачи . Рассмотрены понятие аномалии и доказана взаимосвязь предметной области интерпретации информационной системы на структурном уровне.

Ключевые слова: защита информации, системы предоставления полномочий, формализация средств описания.

USE OF FORMAL FACILITIES OF DESCRIPTION OF PROCESSES OF GRANT OF RIGHTS ACCESS

This work covers the rights accesssystems that can have a variety of interpretations, from representing them as an access rights matrix to their representation in the form of attribution of certain roles to users who request access rights. Namely, we performed the analysis of parameters that characterise the DIS-type information systems in order to choose the most appropriate means of their formal description. We have formulated a number of statements and definitions that simplify such analysis in future and determined a number of mandatory requirements to conduct this analysis.And namely importance of data is defined as a parameter that characterizes the frequency of use of the data for a predetermined period during which the corresponding data is used. Also picked measure data privacy through the degree of danger , which can lead to not authorized use of data in solving the problem . We consider the concept of anomalies and proved the relationship domain interpretation of the information system at the structural level.

Keywords: informationsecurity, authorization systems, formalization of description tools.

Давиденко Анатолій Миколайович кандидат технічних наук, ст. наук. співр., заст. директора Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
E-mail: davidenkoan@gmail.com

Давыденко Анатолий Николайович кандидат технических наук, с. н. с., зам. директора Института проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины

Davydenko Anatolii candidate of engineering science, senior researcher, Deputy director ofPukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine

Суліма Олександр Андрійович , молодший науковий співробітник Інституту проблем моделювання в енергетиці імені Г.Є. Пухова Національної акаде-мії наук України.
E-mail: rfitfo@gmail.com

Сулима Александр Андреевич, младший научный сотрудник Института проблем моделирования в энергетике имени Г.Е. Пухова Национальной ака-демии наук Украины.

Sulima Oleksandr, junior researcher of Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine.