

УДК 004.9

## ІНФОРМАЦІЙНІ ЗАСОБИ КОМПОНЕНТ ВИЗНАЧЕННЯ РИЗИКУ

Б. В. Дурняк, Т. М. Майба

Українська академія друкарства,  
вул. Під Голоском, 19, Львів, 79020, Україна

*Розглянуто фактори, які призводять до зростання ризику функціонування системи управління, а також причини їх виникнення. Проаналізовано найважливіші функції системи захисту.*

**Ключові слова:** ризику, система захисту, атака, засоби захисту.

**Постановка проблеми.** Традиційні методи зниження ризику функціонування системи управління полягають у виконанні ряду процедур з усунення факторів, що призводять до його зростання. Оскільки такі фактори вважаються негативними, то до них належать будь-які порушення, які стосуються реалізації процесу функціонування системи управління. У цьому випадку причинами виникнення відповідних факторів вважатимемо атаки на інформаційну систему управління *ISU* [1].

**Мета статті** — розроблення системи моніторингування *ISU* як складової частини системи захисту, яка виявляє факт існування в *ISU* аномалій.

**Виклад основного матеріалу дослідження.** Така аномалія, або інтруз  $Jt(a_i)$ , що виникає в результаті дії атаки  $A_i$  на *ISU*, може проявлятися у недопустимих змінах значень параметрів процесу управління, коли  $x_i \geq \delta x_i$ . Такий ефект виникає на стадії безпосередньої дії  $Jt(a_i)$  на процеси функціонування системи  $F(Pr_i)$ , що призводить до підвищення ризику зниження рівня якості функціонування *ISU*. Тому в процесі моніторингування ( $MPr_i$ ) аналізується наявність аномалій, які являють собою програмну реалізацію  $Jt(a_i)$ , що впроваджені відповідними атаками. В багатьох випадках  $Jt(a_i)$  не активізується миттєво після впровадження. Це зумовлено тим, що сам процес впровадження проявляє себе в середовищі *ISU* у вигляді аномальних подій. Щоб підвищити ймовірність успіху атаки  $A_i$ , доцільно активізувати впроваджений  $Jt(a_i)$  через деякий інтервал часу, щоб безпосередньо не пов'язувати його прояв з реалізацією успіху атаки  $A_i$ . Залежно від цілі  $A_i$  остаточне формування  $Jt(a_i)$  може відбуватися в середовищі *ISU* протягом деякого часу та зі зміною місця попереднього перебування  $Jt(a_i)$  в просторі середовища *ISU* або середовища всієї системи (*SS*). Процес моніторингування може виявляти у різні періоди моніторингу аномалії в різних місцях *SS*. Це не означає, що в *SS* впроваджена деяка кількість  $Jt(a_i)$ . Процес моніторингування реалізується в *SS* відповідно до певної траєкторії, що формується на основі таких факторів:

- стратегії моніторингування;
- системи координат, яка використовується в *SS* для визначення певних точок цілого середовища.

Стратегія формується на основі цілого ряду критеріїв, які певним чином між собою узгоджені і відображають спосіб структуризації  $SS$ . Найпоширенішим критерієм поділу  $SS$  є визначення областей пам'яті, в яких розміщуються програмні засоби різного функціонального призначення. Такі області можуть мати пріоритети в  $SS$ . Наприклад, область системного програмного забезпечення має найвищий пріоритет і т. д. Локалізація місць виявлення аномалій дає змогу реалізовувати ефективні процедури протидії активізації аномалій та елімінацію відповідних аномалій. Наприклад, виявлення аномалій в області розміщення системних програм інформує про те, що вплив аномалій на систему може мати більший рівень небезпеки, ніж вплив аномалії на фрагменти прикладних програм. Виявлення аномалії в області адрес передачі управління між різними компонентами системи може свідчити про те, що атака орієнтована на підміну окремих програм на програми інтрузи або на забезпечення можливого несанкціонованого доступу із штатних засобів реалізації діалогу між системою та неуповноваженою стороною, наприклад небезпекою  $Nb_i$ . Очевидно, що можливість детальнішої локалізації точок у просторі середовища  $ISU$  дає змогу не тільки точно локалізувати ту чи іншу аномалію, але й отримати додаткову інформацію про характер можливих способів впливу аномалії, або  $Jt(a_i)$ , на об'єкт атаки загалом.

Розглянемо структуру області пам'яті  $ISU$ , яка буде ідентифікуватися з середовищем  $ISU$ . Позначимо таку структуру у вигляді деякого графа  $G^P$ , в рамках якого існують підграфи  $G^{Pm}$ , в цих підграфах може бути чергова система підграфів  $G^{P(m,k)}$  і т. д. Наявність виділеної множини підграфів визначається критеріями виділення чергового рівня підграфів  $G^{P(i)}$ . Припустимо, що критерій  $K_i$  породжує систему підграфів  $G(K_i)$ . Така структуризація області пам'яті  $ISU$  уможлиблює оптимізацію процесу моніторингу [2].

Виявлення причин аномалії є важливою функцією системи захисту, або  $SUB$ , оскільки аномалії в програмному середовищі можуть виникати не тільки в результаті реалізації атаки на  $ISU$ , а і в результаті наявності в окремих програмних компонентах умов реалізації процесу управління, якого не могло бути передбачено на етапі проектування програмних засобів. Такі зміни можуть виникати внаслідок непередбачуваного втручання у процес управління обслуговуючого персоналу, виникнення несправностей в об'єкті управління, змін у функціонуванні апаратних засобів, управління якими здійснюється в  $ISU$  і з інших причин, що можуть виникнути в результаті дії непередбачуваних факторів на весь  $TPP$ . Виникнення наведених вище причин і, відповідно, аномалій відображає особливості управління, що здійснює  $ISU$  технічними об'єктами, що забезпечують реалізацію  $TPP$ . Для ефективною виявлення причин аномалій приймемо обмеження, які будуть використовуватися при цьому виявленні:

- атака, що реалізується на деякий об'єкт, призначена для того, щоб дія відповідного  $Jt(a_i)$  була максимально ефективною щодо можливої цілі атаки;
- $Jt(a_i)$ , що формується деякою атакою  $A_p$ , має реалізуватися таким чином, щоб виявлення  $Jt(a_i)$  було достатньо складним або потребувало реалізації складних процедур аналізу середовища;

- час ефективного впливу  $Jt(a_i)$  на процеси ISU повинен бути мінімалізованим;
- активізація  $Nb_p$ , генерація або формування  $A_p$  повинні проводитися так, щоб це не сприяло підвищенню ймовірності виявлення  $Jt(a_i)$ , що є наслідком відповідних дій зовнішніх факторів, які виникають на рівні функціонування зовнішніх процесів  $OPr_i$ ;
- формування інтруза реалізується так, щоб він був якомога подібнішим до оточення.

Врахування кожного з наведених факторів під час пошуку  $Jt(a_i)$  передбачає проведення складного аналізу, оскільки кожна із зазначених умов виникнення атаки на об'єкт є досить складною і багатопараметричною. Щоб уникнути необхідності подолання відповідних складностей, приймемо деякі положення щодо системи ISU.

*Положення 1.* Один цикл функціонування ISU відповідає повній логічній схемі, яка відображає всі події, що повинні відбутися в процесі реалізації відповідного циклу функціонування.

*Положення 2.* Логічні змінні відповідної схеми можуть відображати результати функціональних перетворень, що реалізуються в рамках відповідних логічних схем.

Припустимо, що деякий цикл управління фрагментом технологічного процесу описується на логічному рівні формулою [3]:

$$L_i = L(x_{i1}, \dots, x_{im}); \quad x_{ij} \in \{0,1\},$$

де  $x_{ij}$  — логічні змінні, що ідентифікують параметри моделі, яка описує фрагмент ТРР, або:

$$M(\varphi_i) = F(p_{i1}, \dots, p_{im}); \quad p_{ij} \rightarrow x_{ij}; \quad [p \in \{\alpha, \beta\}] \rightarrow [(1) < \vee (0)].$$

Для друкарських технологій характерна відсутність аналітичних залежностей між окремими параметрами, які належать до різних фрагментів процесу. Це призводить до заміни останніх апріорними співвідношеннями або іншими формами опису залежностей між експериментальними даними, які представляються у вигляді таблиць та алгоритмів. Типовим прикладом реалізації такої функції слугує функція вибору послідовних значень з ряду таблиць. Прикладом такої функції може бути функція зіставлення, що здійснюється у вигляді, який описує співвідношення:

$$[m(i, j) \rightarrow n_1(a_1 i_1, b_1 j_1)] \Rightarrow [n_1(i_1, j_1) \rightarrow n_2(a_2 i_2, b_2 j_2)] \rightarrow \dots \quad (1)$$

$$[n_{k-1}(i_{k-1}, j_{k-1}) \rightarrow n_k(a_k i_k, b_k j_k)]$$

де  $[m(i, j)]$  — прямокутна таблиця даних з рядками  $i$  та стовпцями  $j$ ,  $m$  — ідентифікатор таблиці вхідних даних, що є табличною функцією, яка ідентифікується ідентифікатором  $m$ ,  $n_r(a_r i_r, b_r j_r)$  — таблиця  $n_r$  з рядками  $i$  та стовпчиками  $j$ ,  $a_r, b_r$  — номери рядка та стовпця, що визначають місце знаходження елемента  $x_{ij}(n, u)$ , який відповідає вхідному елементу  $x_{ij}(m)$ . Як видно зі співвідношення (1), така таблична функція може бути багатокроковою, де індекс  $k$  вказує на номер кроку, який полягає у переході  $m(i, j) \rightarrow n_k(a_k i_k, b_k j_k)$ . Очевидно, що структура таблиць в (1) може бути складнішою. Наприклад, в одному рядку може бути декілька рівнів або підрядків. Тоді номер рядка описується у вигляді  $n[i(k), j]$ , де таблиця  $n$  в рядку під номером  $i$  має  $k$  підрядків. Аналогічна ситуація може бути і у випадку стовпців таблиці  $n$ ,

або  $n[i(k), j(e)]$ , де  $k$  — підрядки рядка  $i$ ,  $e$  — підстовпці стовпця  $j$ . Здебільшого використовуються симетричні структури стовпчиків. Розглянемо визначення, яке описує симетричні та несиметричні структури стовпців.

*Визначення 1.* Симетричною є така таблиця, в якій структура рядків і стовпців поширюється на всі рядки і стовпці таблиці.

Формально це описується співвідношенням:

$$m(s) = m\{\forall i[i(k)] \ \&\forall j[j(r)]\},$$

де  $m(s)$  — симетрична таблиця,  $k$  — підрядки, яких є  $k$  і які є у всіх рядках і таблиці  $m(s)$ ,  $r$  — підстовпці стовпця  $j$ , які є у всіх стовпцях  $j$  таблиці  $m(s)$ .

Очевидно, що структура таблиць може бути не симетрична, що позначається  $s(n)$ . Це означає, що підрядки  $k$  або підстовпці  $r$  можуть бути не у всіх рядків чи стовпців. Функцію (1) будемо також називати функцією переходів, маючи на увазі, що йдеться про переходи від одних даних, які пов'язані з управляючими або псевдоуправляючими параметрами  $x_{ij}^{ps}(i, j)$ , до значень проміжних аргументів  $x_{ij}^{pr}(i, j)$ , від яких переходимо до кінцевих аргументів, які позначатимемо  $x_{ij}^{pk}(i, j)$ . Формально такий ланцюг переходів можна записати у вигляді:

$$x_{ij}^{ps}(i, j) \rightarrow x_{ij}^{pr}(k, e) \rightarrow \dots \rightarrow x_{ij}^{pk}(q, h).$$

Очевидно, що першим елементом такого ланцюга може бути не псевдопараметр  $x_{ij}^{ps}(i, j)$ , а параметр, що зумовлює необхідність використання управляючого параметра в процесі керування. Формально це можна записати у вигляді:

$$x_i^{pkr}(i, j) \rightarrow x_i^{pr}(k, e) \rightarrow \dots \rightarrow x_i^{pu}(q, h),$$

де  $x_i^{pkr}(i, j)$  — критичний параметр, який зумовлює потребу здійснювати управління,  $x_i^{pu}(q, h)$  — параметр управляючий, який визначає величину зміни управляючого параметра щодо його поточного значення або необхідне значення управляючого параметра.

Потреба використовувати послідовність таблиць під час визначення  $x_i^{pu}$  та цілий ряд аргументів, які беруть участь у визначенні значення  $x_i^{pu}$ , що записується у вигляді:

$$x_i^{pu} \Leftrightarrow y = f(x_i^{pr}, x_{i+1}^{pr}, \dots, x_{i+m}^{pr}, x_i^{pk}).$$

Функції  $y_i = f_i(x_{i1}, \dots, x_{im})$  визначаються на основі створення моделей відповідних реалізованих процесів при побудові загальної моделі  $M(ISU)$ . Заміна аналітичних функцій  $y_i = f_i(x_{i1}, \dots, x_{im})$  на табличні функції супроводжується потребою розв'язувати задачу, використовуючи аналітичні функції. Табличні функції, на відміну від аналітичних, будемо позначати:

$$y_i = F(\tau_1, \dots, \tau_m),$$

де  $F$  — таблична функція,  $\tau_i$  — окрема таблиця в табличній функції. Для повнішого відображення табличної функції запишемо її у вигляді:

$$y_i = F[\tau_1 * \varphi_1(\tau_i), \tau_2 * \varphi_2(\tau_{i2}), \dots, \tau_m * \varphi_m(\tau_{im})],$$

де  $\varphi_i(\tau_j)$  — функція, що описує зв'язок між таблицею  $\tau_i$  та таблицею  $\tau_j$ , \* — знак, що визначає зв'язок таблиці  $\tau_i$  з функцією  $\varphi_i(\tau_j)$ .

Однією із задач, які необхідно розв'язувати, використовуючи табличні функції, або  $\tau$ -функції, є визначення способу активізації функції. Очевидно, що в процесі функціонування  $M(ISU)$  змінюються значення аргументів, що записуються у

відповідних таблицях, які позначатимемо  $TB_i$ . Таким чином, множину значень аргументу  $x_i$  записують у таблиці  $TB(x_i)$ . У системі управління аргументами  $\tau$ -функцій можуть бути дані з таких джерел:

- з каналів, що з'єднують підсистему зовнішніх пристроїв, які обслуговують поліграфічне обладнання;
- з пультів оператора, що може втручатися в процес функціонування системи;
- дані можуть появлятися внаслідок перетворень, які реалізуються програмно в рамках моделі  $M(ISU)$ .

У кожен момент реального часу процесу управління параметри, які є аргументами  $TB(x_i)$ , можуть змінюватися. У системі  $ISU$  така зміна реалізується активізацією клітини таблиці, в якій міститься відповідне значення певного параметра. Активізація полягає у зміні коефіцієнтів у координатах, що визначають елемент у  $TB(x_i)$ . Для першого і другого джерела така активізація є тривіальна. Третій тип активізації величини значення параметра здійснюється на основі використання оберненої  $\tau$ -функції. Введемо визначення оберненої  $\tau$ -функції.

*Визначення 2.* Обернена  $\tau$ -функція визначає залежність між координатами значення  $\tau$ -функції та координатами її аргументів, що формально описується співвідношенням:

$$(\zeta_1^a, \dots, \zeta_k^a)[x_i] = F(\zeta_1^y, \dots, \zeta_k^y)[y_i],$$

де  $\zeta_i^a$  — координати аргументу в  $TB(x_i)$ ,  $\zeta_i^y$  — координати значень функції в  $TB(y_i)$ .

*Твердження 1.* Довільну  $TB(x_i)$  з довільною лінійною структурою можна перевести в  $TB^L(x_i)$  з одномірною структурою по відношенню до  $\zeta_i$ .

Доведення твердження ґрунтується на перенумерації клітинок  $TB(x_i)$  впорядкованою множиною чисел. Припустимо, що маємо впорядковану за величиною значень множину чисел  $\eta_i(e_1, \dots, e_n)$ . Якщо структура  $TB(x_i)$  лінійна, то кожна координата  $\zeta_i^a$  представляє лінійну функцію  $\zeta_i^a = ke_i + c$ , де  $k$  і  $c$  — константи. Якщо має місце  $\zeta_i^a = ke_i + c$ , то всі значення  $\zeta_i^a(n)$  можна впорядкувати за збільшенням значення  $\zeta_i^a$ . Тоді запишемо, що  $\zeta_i^a = \{e_{i1}\zeta_{i1}^a, e_{i2}\zeta_{i2}^a, \dots, e_{ik}\zeta_{ik}^a\}$  можна впорядкувати таким чином:  $\{\zeta_i^a, \dots, \zeta_{i-1}^a, \zeta_{i+1}^a, \dots, \zeta_{i+k}^a\}$ . Аналогічно, нумерація кожної координати збільшується лінійно, тому і всі підмножини  $\{\zeta_{ik}^a, \zeta_{(i+1)k}^a, \dots, \zeta_{(i+m)k}^a\}$  також можна впорядкувати за зростанням індексу  $i$  від  $i, k$  до  $(i+m), k$ .

Складну структуру таблиці можна представити як ряд вкладених таблиць, що формально описується співвідношенням:

$$TB(i, j, \dots, k)[x] = \{[TB_{i(j-1)}^{nm}][TB_{k(l-1)}^{er}, \dots, [TB_{s(q-1)}^{gh}(x)] \dots]\}.$$

Відповідно до наведеного твердження, будь-яку лінійну структуру довільної  $TB(i, j, \dots, k)$  можна звести до таблиці з одномірною структурою, що формально описується у вигляді співвідношення:

$$\{[TB_{i(j-1)}^{nm}][TB_{k(l-1)}^{er}, \dots, [TB_{s(q-1)}^{gh}(x)] \dots]\} \Rightarrow TB[i_1, i_2, \dots, i_m](x).$$

Враховуючи твердження (1), можна визначити обернену  $\tau$ -функцію. Беручи до уваги уявлення про лінійність структури  $TB[i_1, i_2, \dots, i_m](x)$  при заміні аргументу  $x_i$  у співвідношенні  $y = f(x_i)$ , що представлено у вигляді  $\tau$ -функції, визначення  $y = f[x_i(a_{ik}, b_{ik})]$  можна реалізувати на основі використання співвідношення:

$$\Delta n(b) = \Delta n(a)[(b_2 - b_1)/(a_2 - a_1)], \quad (2)$$

де  $\Delta n(b)$  — зміна позиції клітини в  $TB_i(y)$  на основі зміни позиції клітини в  $TB_j(x)$ ,  $a_2, a_1$  — позиції клітини в  $TB_i(x)$ , що відповідають зміненому та попередньому значенню  $x_p$ , відповідно,  $\Delta n(b), \Delta n(a)$  — величина зміни позиції клітини в таблиці  $TB_i(b)$  при зміні клітини в  $TB_j(x)$ , відповідно,  $b_2, b_1$  — позиції клітини в таблиці  $TB_j(b)$  до і після проведених змін, відповідно. Співвідношення (2) застосовують під час обчислення обернених значень  $\tau$ -функцій у разі зміни аргументу  $x_p$ , якщо використовується співвідношення  $y = f(x_i)$ .

Виявлення аномалій на рівні логічних моделей  $ML(ISU)$  реалізується на основі відомих у математичній логіці положень про наявність логічних суперечностей між логічними змінними чи фрагментами логічних формул [4]. Оскільки  $ML$  в цьому випадку описують предметну область  $TPP$ , то до складу відповідних правил перетворень  $\Xi$ , що становлять систему виводу  $\exists$  вносять перетворення, які відображають особливості предметної області. Такі особливості зумовлюють потребу використання  $\tau$ -функції як опису процесів функціонування  $TPP$  в рамках моделі  $M(ISU)$ . Оскільки йдеться про розширення логічних функцій виводу, то розглянемо виникнення особливостей, що проявляються на логічному рівні значень, в рамках яких можливе використання певних логічних функцій і, як наслідок, логічних правил перетворень. Наприклад, якщо область визначення змінних  $x_i$  і  $x_j$  визначається діапазоном  $[\alpha, \beta]$  і на цій зоні реалізується відображення для цих змінних такого типу:  $x_i \{ \alpha_p, \beta_i \} \rightarrow [0, 1]$  і  $x_j \{ \alpha_j, \beta_j \} \rightarrow [0, 1]$ , а також допустимими є логічні операції  $\{ \&, \rightarrow \}$ , то у разі розширення  $\{ \alpha_p, \beta_i \} \rightarrow \{ \alpha_i^*, \beta_i^* \}$  до змінних  $x_p, x_j$  може використовуватися лише множина операторів, що описується так:  $\{ \vee, \rightarrow \}$ . Наступним може бути обмеження кількості диз'юнктивів, які можуть створювати кон'юнктивні члени, а в протилежному випадку буде обмежена кількість кон'юнктивів, які можуть створювати диз'юнктивні члени. Інтерпретація першого обмеження не потребує додаткових роз'яснень, оскільки воно ґрунтується на природних обмеженнях інтерпретації бінарного значення змінної  $x_i$ . Друге обмеження ґрунтується на тому, що кількість елементів диз'юнкції чи кон'юнкції може обмежуватися технічними можливостями окремих поліграфічних пристроїв або кількістю фізичних компонент, які використовуються в  $TPP$ .

Ще однією важливою задачею, пов'язаною з використанням  $\tau$ -функцій, є організація таблиць  $TB_i$  у випадках, коли наявна функція  $y = f(x_p, x_j, \dots, x_m)$ . Це означає, що цілий ряд  $TB_i$  визначає певне значення  $y_i$ . В цьому випадку недостатньо будувати взаємозв'язок між  $TB_i(x)$  і  $TB_j(y)$  на основі взаємозв'язків між адресами двох таблиць. Для розв'язання такої задачі введемо визначення, що стосуються  $\tau$ -функцій.

**Визначення 3.** Кожна  $\tau$ -функція має активну клітину, котра відповідає поточному значенню параметра  $x_p$ , яке називається активним у момент часу  $t_i$  функціонування процесу  $y_i$ .

Формально це визначення описується співвідношенням:

$$\tau_i^*[x_i(a_p, b_i)] \rightarrow TB_i(a_p, b_i) = x_i^*,$$

де  $\tau_i^*$  — активне значення  $\tau$ -функції при  $x_i(a_p, b_i)$ , що відповідає випадку, коли елемент таблиці  $TB_i$ , який знаходиться в клітині з координатами  $(a_p, b_i)$ , відповідає поточному значенню параметра  $x_p$ .

*Визначення 4.* Функція  $\tau_i(y_i)$  приймає активне значення в процесі функціонування  $TPP$ , якщо  $y_i = f(x_p, x_j, \dots, x_m)$ , для відповідної  $\tau$ -функції має місце  $\tau_i[x_i(\Delta a_p, \Delta b_i)]$ , де  $\Delta a_p, \Delta b_i$  визначають діапазон значень аргументу, що перебуває у відповідному  $TB_i(x)$  в клітинах, адреси яких визначаються діапазонами  $\Delta a_p, \Delta b_i$ .

Наведене визначення стосується ситуації, коли деяка функція  $y_i = f(x_p, x_j, \dots, x_m)$ , яка не може бути реалізована безпосередньо щодо свого можливого математичного алгоритму, оскільки вона є неявною, реалізується у вигляді  $\tau$ -функції, яка на основі поточних даних аргументів відповідно до таблиць цих даних визначає відповідні значення функції на множині її можливих значень, які описуються у відповідній таблиці  $TB_i(y)$ .

У класичному випадку вважають, що відома множина значень аргументів, представлена комплектами даних, кожний з яких забезпечує певне значення для  $y_i$ . Формально це можна записати у вигляді:

$$\{y_p, \dots, y_n\} \rightarrow \{x_l^1, \dots, x_k^1\}, \{x_l^2, \dots, x_e^2\}, \dots, \{x_l^m, \dots, x_g^m\}.$$

Для визначення одного з можливих значень  $y_i$  треба підібрати з наведених комплектів значень такі набори аргументів  $\{x_j^1, \dots, x_{j+q}^1\}, \{x_l^2, \dots, x_e^2\}, \dots, \{x_i^m, \dots, x_{i+r}^m\}$ , які визначають одне зі значень аргументу  $y_i$ , що формально можна записати у вигляді:

$$\{x_j^1, \dots, x_{j+q}^1\}, \{x_l^2, \dots, x_e^2\}, \dots, \{x_i^m, \dots, x_{i+r}^m\} \rightarrow y_i.$$

Позначимо кожний з комплектів значень аргументів символами  $\{x_i\}, \{x_j\}, \dots, \{x_k\}$ , при цьому  $\{x_i\} = h_1, \{x_j\} = h_2, \dots, \{x_k\} = h_n$ , де  $h_1, h_2, \dots, h_n$  — перелік значень, які приймають аргументи в кожній групі. Розглянемо наступне твердження.

*Твердження 2.* При використанні  $\tau$ -функцій для визначення значення функції  $y_p$  для якої аргументами є параметри  $\{x_p, \dots, x_m\}$ , якщо  $y_i \rightarrow h_y(1)$ , то серед усіх параметрів аргументів хоча б один їх комплект складається з одного елемента, або  $\{x_j\} = h_y(1)$ .

Формально це твердження можна записати у вигляді:

$$\exists(y_i \in \{y_{i+1}\}) [y_i = \tau(x_1), \dots, \tau(x_m)] \rightarrow \forall(x_i \in \{x_i^1\}, \dots, \forall(x_j \in \{x_j^m\}) \exists x_k^j [\{x_i^j\} = h_j(1)].$$

Вважатимемо, що має місце  $y = y_i^* \rightarrow \{y_i^*\} = g_i(1)$ . Оскільки функція  $y_i = \tau_i(x_i), \dots, \tau_m(x_m)$ , то в  $[TB_i(x_i) \& \dots \& TB_m(x_m)]$  для  $(x_i) = h_i(\gamma_i > 1), \dots, (x_m) = h_m(\gamma_m > 1)$ , це означає, що всі  $TB_i(x_i)$  не є одиничними. Оскільки  $\{y_i^*\} = h_i(1)$ , то серед  $\{x_i\}, \dots, \{x_m\}$  повинна бути така  $TB_p$ , в якій тільки з одного  $x_i^* = \zeta$  можна перейти до  $\{y_i^*\} = h(1)$ . Припустимо, що така вимога не виконується. Тоді між усіма  $\{x_i^1\}, \dots, \{x_j^m\}$  існують такі  $\tau$ -функції, які як аргументи використовують  $\{x_i^1\}, \dots, \{x_j^m\}$ . Нехай серед усіх  $\tau$ -функцій існує  $\tau$ -функція, яка поєднує  $y_i^*$  з одним із комплектів  $\{x_j^k\}$ , який безпосередньо зв'язаний з представниками комплекту  $\{y_i\}$ . Оскільки  $\{y_i^*\} = h(1)$  реалізує одну імплікацію, то це означає, що комплект значень параметра, який є посилкою для  $y_i^*$ , відповідає умові  $\{x_j^*\} = h_j(1)$ .

Можна розширити це твердження і довести, що за умови, коли  $\{x_i^1\} = h(\xi > 1)$  при переходах з допомогою  $\tau$ -функцій кількість імплікацій зменшується. У класичному випадку у функцію  $y_i = f(x_p, \dots, x_m)$  підставляється така кількість комплектів значень змінних, яка необхідна для того, щоб за алгоритмом, що реалізує функцію  $f$ , обчислити деяке значення  $y_i^*$ . Це значення  $y_i^*$  може не відповідати тому значенню  $y_i^z$ ,

яке нам потрібне для реалізації процесу управління. В цьому випадку необхідно досліджувати поведінку функції, щоб вийти з тою чи іншою точністю на  $y_i^Z$  [5]. Ми задаємо потрібне значення  $y_i^Z$ , стосовно якого відомо, що воно допустиме, і на основі використання  $\tau$ -функції, знаючи всі можливі діапазони значень аргументів, знаходимо відповідні цьому випадку значення аргументів і, відповідно, значення функції:  $\{x_1^*\} = h_1(1)$ ,  $\{x_2^*\} = h_2(2)$ , ...,  $\{x_m^*\} = h_m(k)$ .

Тому для забезпечення однозначності в інтерпретації використовуваної  $\tau$ -функції введемо її визначення.

*Визначення 5.*  $\tau$ -функція являє собою функцію, яка визначає відповідність між таблицею значень деякої змінної  $x_p$ , яку визначаємо за допомогою таблиці  $TB_i(x_i)$ , та значенням функції  $y_p$ , аргументом якої є змінна  $x_i$ .

**Висновки.** Таким чином визначення 5 описується співвідношенням:

$$y_i = \tau[TB_i(x_i)],$$

або в явній формі цей запис можна представити у вигляді співвідношення:

$$y_i = \tau\{x_i[(a_{i1}, a_{i2}, \dots, a_{ik}), (b_{i1}, b_{i2}, \dots, b_{im})]\},$$

де  $x_i$  — аргумент функції  $y_p$ ,  $a_{ij}$  — номер рядка або підрядка в таблиці значень  $TB_i(x_i)$  аргументу  $x_p$ ,  $b_{ij}$  — номер стовпця або підстовпця, на перетині якого з рядком  $a_{ij}$  знаходиться в таблиці  $TB_i(x_i)$  значення параметра  $x_m^*$ , яке зумовлює згідно з функцією  $f$ , або  $y_i^* = f(x_i)$ , відповідне значення  $y_i^*$ . Таким чином,  $\tau$ -функція, по суті, замінює аналітичну функцію  $f$  залежності  $y_i = f(x_i)$ . Отже, як впливає з наведеного матеріалу,  $\tau$ -функція може бути розширена довільною кількістю аргументів.

### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лукацкий А. В. Обнаружение атак / А. В. Лукацкий. — СПб. : БХВ-Петербург, 2001.
2. Лавров С. С. Автоматическая обработка данных, хранение информации в памяти ЭВМ / С. С. Лавров, Л. И. Гончарова. — М. : Наука, 1971.
3. Гиндикин С. Г. Алгебра логики в задачах / С. Г. Гиндикин. — М. : Наука, 1975.
4. Шенфилд Дж. Математическая логика / Дж. Шенфилд. — М. : Наука, 1975.
5. Кудрявцев Л. Д. Курс математического анализа / Л. Д. Кудрявцев. — М. : Высшая школа, 1988.

### REFERENCES

1. Lukackij, A. V. (2001). Obnaruzhenie atak. SPb.: BHV-Peterburg (in Russian).
2. Lavrov, S. S., & Goncharova, L. I. (1971). Avtomaticheskaja obrabotka dannyh, hranenie informacii v pamjati JeVM. Moscow: Nauka (in Russian).
3. Gindikin, S. G. (1975). Algebra logiki v zadachah. Moscow: Nauka (in Russian).
4. Shenfeld, Dzh. (1975). Matematicheskaja logika. Moscow: Nauka (in Russian).
5. Kudrjavcev, L. D. (1988). Kurs matematicheskogo analiza. Moscow: Vysshaja shkola (in Russian).



**INFORMATION MEANS OF COMPONENTS OF RISK DEFINITION**

B. V. Durnyak, T. M. Maiba

*Ukrainian Academy of Printing,  
19, Pid Holoskom St., Lviv, 79020, Ukraine  
maiba@ukr.net*

*The article reviews the factors that lead to the risk increase of management system functioning and their causes. The most important functions of security system have been analyzed.*

**Keywords:** risks, security system, attack, security means.

*Стаття надійшла до редакції 11.03.2016.*

*Received 11.03.2016.*