1989. — 496 с. 10. Про електронний цифровий підпис: закон України // Урядовий Кур'єр. — № 138. — С. 3–6. 11. Шевчук А. В. Теоретичні основи побудови інформаційних технологій захисту поліграфічної продукції спеціального призначення: автореф. дис. на здобуття наук. ступеня д-ра техн. наук: спец. 05.13.06 / А. В. Шевчук. — Львів, 2004. — 34 с. 12. Шовгенюк М. В. Метод кодування графічних зображень та впровадження нової технології захисту цінних паперів / М. В. Шовгенюк, Л. А. Дідух // Наука та інновації. — К., 2009. — № 1. — С. 52–61.

ИДЕНТИФИКАЦИЯ ПЕЧАТНЫХ ДОКУМЕНТОВ СРЕДСТВАМИ ATEB-ФУНКЦИЙ

Предлагается метод защиты и идентификации, который базируется на параметрах ateb-функций и матрицах Уолша-Адамара. Защита документов образуется путем наложения фоновых сеток на основе ateb-функций. Разрабатывается алгоритм метода идентификации документов, который заключается в формировании матриц Уолша-Адамара электронного графического элемента со сравнением матриц в напечатанном документе.

IDENTIFICATION POLYGRAPHY DOCUMENTS PROTECTED BY TOOLS ATEB-FUNCTIONS

In the article the method of protection and identification, based on the parameters Ateb-functions and the Walsh-Hadamard matrices. Protection of documents produced by the imposition of background grids Ateb- functions. The algorithm of identification documents, which is the formation of the Walsh-Hadamard matrices of electronic graphic element of comparison matrix in the printed document.

Стаття надійшла 23.03.11

УДК 004.921

Л. Є. Шведова

Кримський інститут інформаційно-поліграфічних технологій Української академії друкарства

МЕТОДИ АНАЛІЗУ ЛОГІЧНИХ СИСТЕМ УПРАВЛІННЯ ПОВНОВАЖЕННЯМИ

Проведено аналіз логічних систем управління повноваженнями, на основі чого виявлено основні параметри, їх взаємозв'язки та задачі, які б дозволили уникнути порушень безпеки в інформаційній системі.

Логічна система, модель, управління повноваженнями, операція, об'єкт

Використання системи співвідношень, що описує стан системи управління повноваженнями (*SUP*), дозволяє реалізувати їх перетворення тільки в ті моменти, коли з'являються нові запити на обслуговування суб'єктів y_i. Для опису такої системи використовуються логічні способи подання компонент

SUP. Основною метою аналізу відповідних компонент є виявлення можливих аномалій, що може призвести до некоректного функціонування системи загалом. На рівні логічного подання *SUP*, до таких колізій належать:

виникнення суперечностей у системі;

виникнення конфліктів у системі;

зміна ефективності виводів, що формуються в процесі використання логічного подання системи.

Виникнення суперечностей у системі зумовлюється ініціацією нових суб'єктів та надання їм доступу до об'єктів, які відповідні суб'єкти потребують. Перш ніж аналізувати та досліджувати методи виникнення та виявлення можливих суперечностей, потрібно проаналізувати розширення інтерпретації уявлення про суперечність, яке зумовлюється предметною областю задач, для розв'язування яких передбачається використовувати *SUP*. Відповідно до узагальненого уявлення про істинність чи неістинність, що здебільшого пов'язана з конкретним розв'язком задач, які апроксимуються відповідними логічними співвідношеннями чи взагалі з можливістю досягнення необхідного розв'язку задачі. Отож потрібно розглянути інтерпретацію ситуацій, що виникають у *SUP*, які зумовлюються тим, що відповідна задача захисту не була розв'язана або її розв'язок виявився некоректним.

Однією з таких ситуацій є порушення цілісності. Воно виникає у разі, якщо суб'єкт y_i отримав доступ до об'єкта x_i, який не відповідає необхідним повноваженням, а тип дій в y_i на x_i відповідає запису нових даних W, заміні даних W^z, знищенню даних W^c чи доповненню даних W^D.

Ситуація, що відповідає порушенню конфіденційності полягає в тому разі, якщо y_i отримує доступ до x_i з правом читання даних і при цьому y_i не має повноважень на виконання таких дій з x_i. Це означає, що неуповноважений y_i прочитав інформацію з x_i несанкціоновано.

Ситуація, що відповідає порушенню адекватності або аутентифікації зводиться до наступного. Аутентифікація полягає у ідентифікації її джерела, за часом створення, змістом даних, часом використання уповноваженим користувачем, ідентифікації користувача і самої інформації на момент її використання. Відповідно до наведеної інтерпретації аутентифікації, можна стверджувати, що вона включає в себе цілісність даних і розширюється цілим рядом вимог виконання яких є обов'язковим, оскільки вони забезпечують актуальність інформації на момент її використання та на момент створення дають гарантію того, що інформація створена відповідним суб'єктом та ідентифікацію самої інформації на момент її використання.

З погляду системи *SUP* вимоги аутентифікації забезпечуються на різних етапах її функціонування. Ідентичність інформації джерелу забезпечується при реалізації санкціонованих повноважень суб'єкта y_k, який формує відповідну інформацію. При цьому у власному оточенні відповідного об'єкта x_i записуються параметри певних даних, до яких належать дані про час формування відповідної інформації та ідентифікатор y_k, який сформував

відповідну інформацію. Час використання створеної інформації може визначатися такими складниками:

часом використання інформації, що визначається джерелом її створення;

часом використання інформації, що встановлюється системними факторами;

часом використання інформації, що визначається санкціонованим користувачем або суб'єктом *SUP*.

У першому випадку час, який визначається джерелом створення інформації, записується у персональне оточення відповідного об'єкта x_i і цей параметр використовується як додатковий, що застосовується при визначенні повноважень суб'єкта y_j, який звернувся за доступом до x_i.

У другому випадку системні фактори можуть змінити час використання даних шляхом збільшення інтервалу їх актуальності, ліквідації цього параметра або знищенням відповідної інформації, якщо вона повністю втратила свою актуальність після моменту, вказаного джерелом, що формувало відповідну інформацію. Факторами системного характеру, які ініціюють зміни параметра часу є зміна рівня категорії відповідного об'єкта, що здійснюється на основі завершення часу протягом якого вказана категорія є актуальною; збільшення кількості суб'єктів, які звертаються до об'єкта, на величину Δn_i, що являє собою поріг та зміна всіх параметрів, які характеризують x_i в рамках *SUP*.

Якщо санкціонований суб'єкт звернувся до *SUP* за наданням йому повноважень з використання об'єкта x_i і такий y_j визначає час використання відповідної інформації, то система може в персональному оточенні відповідного x_i змінити параметр часу одним з тих способів, що використовуються у випадку ініціації таких змін системними факторами.

Додатковим параметром забезпечення ідентифікації інформації, що сформована джерелом y_i може бути застосування системними засобами функції хешування [1]. Необхідність додаткового забезпечення аутентифікації інформації визначається величиною категорії відповідного об'єкта x_i, в якому деякий суб'єкт y_k сформував відповідні дані.

У разі, якщо існує необхідність забезпечити незаперечність сформованих даних деяким суб'єктом y_j, він отримує від *SUP* персональний ключ, що може використовуватися суб'єктом y_i для реалізації цифрового підпису даних, які ним сформовані [2]. Алгоритм реалізації цифрового підпису реалізується в рамках *SUP* і за потреби суб'єктами, які ініціюють запити на використання тих чи інших об'єктів.

Суперечність, яка може виникати в системі опису стану *SUP* в рамках визначеної інтерпретації може призводити до порушень прав доступу. Відповідні порушення називатимемо суперечними ситуаціями, які можуть виникати в *SUP*.

Опис та аналіз поточного стану *SUP* реалізується на основі використання таких компонент та факторів:

об'єктів, що знаходяться в системі $\{x_1,..., x_n\}$;
суб'єктів, що активізуються в *SUP* $\{y_1,..., y_m\}$;
засобів опису активності y_i в *SUP*;
системою умов поточної активності y_i;
правилами перетворень опису поточного стану *SUP*.

Засоби опису активності суб'єктів y_i в *SUP* групуються на обчисленні оцінок суб'єктів та відповідних об'єктів, запити на використання яких формують суб'єкти, що активізуються. Отримані оцінки аналізуються і на основі такого аналізу суб'єкт отримує або не отримує повноваження на використання відповідного об'єкта. Для того, щоб можна було встановити відповідну оцінку, необхідно функції, за якими такі оцінки визначаються подати у явній формі. Таке подання функцій апроксимується засобами математичної логіки з окремими розширеннями.

Оскільки рішення про надання повноважень чи відмову в наданні їх суб'єкту y_i на використання об'єкта x_i здійснюється на основі певного порівняння $RO(y_i)$ та $RO(x_i)$, то доцільно апроксимувати логічними засобами не оцінки окремих компонент, а співвідношення, що пов'язує відповідні оцінки. Порівняння оцінок у рамках такого співвідношення може реалізуватися на основі використання порогових методів інтерпретації оцінок. Для того, щоб можна було здійснити інтерпретацію співвідношень між $RO(y_i)$ та $RO(x_i)$ на логічному рівні, необхідно визначити область значень для параметрів k_i та c_i і сформувати масштаб їх вимірювання. Оскільки йдеться про їх порівняння, то потрібно визначити одиниці їх вимірювання та спосіб відповідного вимірювання. Одиницями вимірювання в нашому випадку вважатимемо інтерпретацію відповідних параметрів, якою є міра значущості c_i для y_i та міра таємності k_i для x_i. Початкове значення міри таємності k_i встановлюється при інсталяції *SUP*. Аналогічна ситуація і у випадку з суб'єктом y_i. На відміну від наявного стану, що пов'язаний з оцінкою інформаційних компонент, суб'єктивність такої оцінки, характерна початковій стадії, доволі швидко змінюється завдяки активізації факторів, що обумовлюють відповідні зміни k_i. Величина k_i вимірюється цілими раціональними числами, що із зростанням означають відповідне зростання таємності.

Значущість c_i суб'єкта y_i визначаються такими компонентами:

декларованою частиною значущості, що відповідає величині таємності k_i об'єкта x_i, використання якого декларується на момент інсталяції *SUP*;

частиною, що визначається кількістю функцій захисту, які реалізуються у відповідного суб'єкта y_i;

частиною, що формується в процесі функціонування відповідного суб'єкта y_i в рамках *SUP*, що зумовлюється факторами, які призводять до збільшення чи зменшення загального значення значущості суб'єкта;

Формально значущість c_i суб'єкта y_i можна описати співвідношенням:

$$y_i(c_i) = \left(c_i^p + c_i^f\right)\varphi_a\left(c_i^a\right), \qquad (1)$$

де c_i^p — величина значущості y_i, що відповідає або дорівнює величині k_i об'єкта x_i, який приписується до y_i на початковій стадії ініціалізації *SUP*; c_i^f — величина значущості c_i, що визначається кількістю засобів захисту суб'єкта y_i і реалізується в рамках самого суб'єкта при його проектуванні; c_i^d — динамічна складова частина, яка обумовлюється факторами, що впливають на зміну величини значущості y_i в більшу або в меншу сторону. Слід зазначити, що на початковому етапі $c_i^d = 0$, а c_i^p та c_i^f є константами для y_i і незмінними протягом функціонування y_i. Тоді співвідношення для визначення значущості y_i можна формально записати так:

$$y_i(c_i) = \left(c_i^p + c_i^f\right) \cdot \left(c_i^d\right), \qquad (2)$$

якщо φ_{ci} являє собою операцію множення.

Вибір типу функцій φ_{ci} грунтується на аналізі предметної області інтерпретації роботи *SUP* та ситуацій, що пов'язані зі встановленням взаємодії суб'єктів y_i з об'єктами x_i. Використання співвідношення (2) забезпечує можливість зменшення величини значущості c_i таким чином, що загальну величину значущості y_i можна зменшити до рівня, меншого від складників $\left(c_i^p + c_i^f\right)$ або $c_i \le \left(c_i^p + c_i^f\right)$.

З точки зору інтерпретації $y_i(c_i)$ це означає, що значущість y_i в процесі функціонування *SUP* може знизитися до нуля незалежно від того, що y_i має певну кількість засобів захисту, які залишаються в складі суб'єкта чи він є активним чи ні. Стосовно c_i^f, то ця частина значущості в цьому випадку відображає величину суб'єктивної помилки при визначенні значущості $y_i(c_i)$.

Динамічний складник величини значущості суб'єкта c_i^d залежить від кількості об'єктів до яких звертаються y_i, і складається з кількості об'єктів доступ до яких суб'єкту було надано і відмовлено. Кількість x_i, використанню яких відмовлено у момент t_i, визначається тими об'єктами, в яких рівень таємності протягом інтервалу часу $\Delta t_i = t_i - t_0$, де t_0 — початковий момент роботи *SUP*, в який відбулася інсталяція *SUP*, змінився таким чином, що умова $c_i \ge k_i$ не виконується. Така ситуація можлива, тому що призначення $c_i = c_i^a$, де c_i^a — фіксоване значення c_i для y_i, виконується на момент t_0 і значення k_i у x_i на даний момент визначає допустимість співпраці y_i з x_i. Беручи до уваги вищевикладене, можна вважати, що k_i вимірюється умовними одиницями, для яких використовуються цілі числа, а c_i для y_i також вимірюються умовними одиницями, які збігаються з k_i. Значення c_i відрізняються від k_i тільки завдяки тому, що алгоритми обчислень значень c_i та k_i є різними. Це випливає з методів обчислення c_i та k_i, які змінюються у процесі роботи *SUP*, що оперують по суті спільними або взаємозалежними аргументами.

У співвідношеннях, що встановлюють k_i для x_i та c_i для y_i використовуються аргументи, які визначаються як дискретні змінні, що задаються в певних діапазонах. Наприклад, параметри m_i та η_i є ірраціональними

величинами, оскільки η_i є ірраціональним за способом його визначення, як деякого середнього арифметичного від цілих чисел, а m_i є також ірраціональним, оскільки кількість y_i, що звертаються за повноваженнями на використання x_i, не може безпосередньо впливати на зміну величини k_i. Отож m_i фактично являє собою певне порогове значення кількості y_i, що звертаються до x_i, яке визначається із співвідношення: $m_i = m_i^{\wedge}/\alpha^m$, де $m_i^{\wedge}$ — кількість y_i, що звернулися до *SUP* за повноваженнями про співпрацю з x_i за період часу τ_i або Δt_i; а α^m — коефіцієнт зведення кількості y_i, які зверталися за співпрацею з x_i, який визначає поріг кількості звернень, необхідних для того, щоб вони змогли призвести до зміни величини значення k_i. Аналогічна ситуація існує з параметрами n_i та p_i, які використовуються для визначення c_i. Відповідні визначення вказаних параметрів називатимемо їх нормалізацією.

Для спрощення опису поточної ситуації в *SUP* приймемо, що y_i та x_i, які є учасниками процесів у *SUP* і визначають ту чи іншу ситуацію, яку позначатимемо $u_i \in U$, де U — множина всіх можливих ситуацій у *SUP*, є певними функціями незалежних змінних, що відповідно до прийнятої інтерпретації дозволяють у кожний поточний момент обчислити значення c_i для y_i і k_i для x_i [4, 5]. Величини k_i та c_i визначаються на множинах цілих чисел і є сумісними в рамках своєї розмірності. Цей факт формально запишемо:

$$\left[\left((c_i \in C) \to R^{c}\right) \& \left((k_i \in K) \to R^{k}\right)\right] \& \left(R^{k} \cap R^{c} \neq \varnothing\right) \& \left(R^{c} \cup R^{k} = R^{c,k}\right),$$

де $R^{c,k}$ — множина всіх значень k_i та c_i.

Розглянемо конструктивну інтерпретацію суперечності, що може виникнути у *SUP* в результаті використання y_i і x_i. Приймемо, що ситуація u_i, яка на момент t_i склалася в *SUP* описується множиною співвідношень:

$$u_i(t_i) = \left\{(y_{i1} \to x_{i1}), (y_{ir} \to x_{ir}), \ldots, (y_{im} \to x_{in})\right\}.$$

Кожне співвідношення або кожна імплікація зумовлюється умовою, що визначається співвідношенням між c_{ij} та k_{im} для y_{ij} та x_{im} відповідно. Якщо окрема імплікація або редукція є автономною в $u_i(t_i)$, то всі окремі редукції, які позначатимемо $h_{ik}^{t} = (y_{ij} \to x_{ik})$, в рамках $u_i(t_i)$, являтимуть собою систему кон'юкцій. У цьому разі можна записати співвідношення:

$$u_i(t_i) = \&_{j,m}^{m} h_{ij} = h_{i1} \& h_{i2} \& \ldots \& h_{im} = L(h_{i1}, \ldots, h_{im}). \qquad (3)$$

Описана ситуація являє собою лише один з варіантів, який може існувати в *SUP*. У реальній системі *SUP* найчастіше існує ситуація, коли один y_i протягом інтервалу активізації відповідного суб'єкта співпрацює з різними x_i для яких на момент активізації y_i відповідні імплікації є допустимими. У

цьому випадку логічна формула, що описує $u_i(t_i)$, може бути подана співвідношенням:

$$u_i(t_i) = L_i(h_{i1}, \ldots, h_{im}),$$

де L_i — логічна функція, яка формується на основі використання логічних функцій $\{\&, \vee, \rightarrow, \neg\}$. Інтерпретація використання певних комбінацій логічних функцій у рамках однієї $L_i(h_{i1}, \ldots, h_{im})$ полягає у наступному. Вважатимемо, що деякий суб'єкт y_i активізує використання низки об'єктів $x_{i1}, \ldots, x_{ik}$ в момент часу t_i. У цей самий момент t_i або в деякий момент t_j, який потрапляє в інтервал часу Δt_i, протягом якого є активним суб'єкт y_i. Тоді може виявитися, що $y_i(c_i) > y_j(c_j)$, $x_i(k_i)$ та $x_j(k_j)$ збігаються з $y_i(c_i)$ та $y_j(c_j)$ на основі виконання умов, що визначаються співвідношеннями між k_i і c_i та k_j і c_j. При цьому y_i співпрацює також з x_j, що є допустимим, оскільки справджується співвідношення:

$$\{\{[y_i(c_i) > y_j(c_j)] \& [y_j(c_j) \geq x_j(k_j)]\} \rightarrow [y_i(c_i) > x_j(k_j)]\} \rightarrow$$
$$\rightarrow \{\{[y_i(c_i) \geq x_j(k_j)] \& (y_i \rightarrow x_j)\} \rightarrow (y_i \rightarrow x_j)\}.$$

У рамках наведеного співвідношення може існувати ситуація, що y_j, який співпрацює з x_j має повноваження типу запису даних, які відповідають рівню таємності k_j. Суб'єкт y_j, працюючи з x_j, має повноваження типу R, що дозволяє зчитувати дані з x_j. У співпраці з x_j суб'єкт y_j, завдяки цьому, що справджується співвідношення $[y_i(c_i) > y_j(c_j)] \& (c_i > k_j)$, використовує повноваження типу запису W, що може призвести до того, що в x_j будуть записані дані, рівень таємності яких рівний k_i, а $k_i > k_j$. Суб'єкт y_j, який має доступ до x_j типу k_j, може прочитати відповідні дані. Це призведе до того, що дані з x_i, які мають категорію k_i виявляться доступними для суб'єкта y_j, для якого, відповідно до вихідних даних, $c_j < k_i$. Така суперечність являє собою суперечність умов міграції даних, яка здійснюється в рамках сумісного використання різними суб'єктами y_i та y_j, які мають різні рівні значущості, наприклад $c_i > c_j$, що співпрацюють зі спільними об'єктами x_i та x_j, які також володіють різними рівнями таємності або різними значеннями категорій k_i та k_j, відповідно [3, 6].

З вищенаведеного прикладу випливає, що в *SUP* на момент t_i і, відповідно, на інтервалі одиничного періоду активізації різних суб'єктів $y_i, y_j \ldots, y_k$, може виникнути ситуація, що призведе до порушення конфіденційності, що з точки зору *SUP*, як системи, що керує доступом для забезпечення необхідного рівня безпеки, повинна недопускати порушень безпеки функціонування в рамках інформаційної системи (*IS*). Ситуація, в якій виявляється можливим порушення довільного типу, називається суперечною ситуацією. Очевидно, що в рамках *SUP* повинні розв'язуватися наступні задачі, які дозволили б уникнути порушень безпеки в *IS*, при управлінні повноваженнями. Такими задачами є:

задача виявлення в поточній ситуації використання повноважень суперечностей;

задача усунення суперечностей, які виникають у *SUP* і виявлені засобами SUP;

задача формування умов, виконання яких дозволило б в процесі реалізації управління повноваженнями системою *SUP* на наступних етапах її функціонування, уникнути можливості виникнення суперечностей, тип яких був виявлений раніше.

Типи суперечностей, що можуть виникати в рамках *SUP*, в процесі управління повноваженнями, можуть визначатися такими факторами:

рівнем інтерпретації системи;

способом аналізу поточної ситуації $u_i(t_i)$, що сформувалася на поточному етапі функціонування *SUP*;

мірою зниження рівня безпеки *IS*, що зумовлюється черговим етапом керування доступом суб'єктів $\{y_1,..., y_m\}$ до об'єктів $\{x_1,..., x_n\}$.

Рівень інтерпретації системи *SUP* визначається способом апроксимації опису поточного стану *SUP*. Різні способи опису апроксимації поточного стану *SUP* забезпечують різну точність відповідної апроксимації. Отже, апроксимації, в цьому випадку, є такими:

інтерполяція опису стану *SUP* засобами математичної логіки, яку позначатимемо (*ZML*);

інтерполяція опису стану *SUP* засобами математичної логіки, які розширені функціональними предикатами, що описують функції обчислення базових параметрів c_i і k_i, яку називатимемо інтерполяцією, що описується розширеними засобами подання ситуацій у *SUP* (*RZO*);

інтерполяція опису стану *SUP*, що забезпечує відображення залежності $u_i(t_i)$ від типів повноважень, які отримують y_i відносно x_i, яку позначатимемо (*ZTP*);

На кожному рівні інтерпретації використовуються не тільки різні засоби інтерпретації, але й реалізується різна міра точності опису $u_i(t_i)$ в *SUP*. При інтерполяції типу *ZML* точність відображення $u_i(t_i)$ визначається на рівні надання чи ненадання повноважень окремим y_i відносно x_i, і тоді опис $u_i(t_i)$ надається співвідношенням (3). У цьому випадку у процесі аналізу стану $u_i(t_i)$ виявляється факт наявності або відсутності суперечності, оскільки перевірка цього факту здійснюється на основі опису, що формується за даними *SUP*, які відображають наявні в момент t_i взаємозв'язки між y_i та x_i, що відображають активізацію y_i. Ця ситуація відповідає реєстрації факту порушення, що існує в системі *SUP*.

1. Алфёров А. П. Основы криптографии : учеб. пособие / А. П. Алфёров, А. Ю. Зубов, А. С. Кузьмин. — М. : Гелиос АРВ, 2001. — 480 с. 2. Коутинхо С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. — М. : Постмаркет, 2001. — 328 с. 3. Нечаев В. И. Элементы криптографии. Основы теории защиты информации / В. И. Нечаев. — М. : Высшая школа, 1999. — 109 с. 4. Новиков П. С. Конструктивная математическая логика с точки зрения

классической / П. С. Новиков. — М. : Наука, 1977. — 328 с. 5. Расева Е. Математика математики / Е. Расева, Р. Сикорский. — М. : Наука, 1972. — 591 с. 6. Шнайдер Б. Прикладная криптография. Протоколы, алгоритмы, тексты на языке Си / Б. Шнайдер. — М. : ТРИУМФ, 2002. — 816 с.

МЕТОДЫ АНАЛИЗА ЛОГИЧЕСКИХ СИСТЕМ УПРАВЛЕНИЯ ПОЛНОМОЧИЯ

Проведен анализ логических систем управления полномочиями, на основе чего выявлены основные параметры, их взаимосвязи и задачи, которые бы позволили избежать нарушений безопасности в информационной системе.

METHODS OF ANALYSIS LOGIC SYSTEMS MANAGEMENT AUTHORITY

The analysis of logical systems of authority, on the basis of which revealed the basic parameters, their relationships and problems that would prevent security breaches in information systems.

Стаття надійшла 27.04.2011