УДК 004.056.52

О.А. Суліма, м.Київ

РОЗРОБКА АЛГОРИТМУ НАДАННЯ ПОВНОВАЖЕНЬ ЗАДАЧАМ НА ВИКОРИСТАННЯ ДАНИХ

Abstract. Carried out realization the algorithm of analysis on the basis of numeric data parameters. For all introduced parameters determining ways to them values introduced metric measurement of values and concerted of scale measurement various parameters.

Актуальність

В роботах [1 – 3] обґрунтовано актуальність, поставлено та розв'язано задачу, розроблення технології адаптивного захисту систем доступу до мережевих інформаційних ресурсів. Основу технології складають модельні описи поточної поведінки споживачів послуг комп'ютерної мережі та методи динамічного налаштування параметрів систем захисту інформаційних ресурсів для підтримки бажаного рівня їх захищеності від шкідливих дій споживачів.

Актуальною є задача розширення функціональних можливостей даної технології за рахунок побудови алгоритму надання повноважень задачам на використання даних.

Постановка задачі

Алгоритм надання повноважень (ANP) реалізує всі операції, які є необхідні, при реалізації процесу доступу до таємних даних. Користувач, після отримання доступу до системи, вводить необхідні дані про задачу Za_i і фрагменти алгоритму її реалізації, які потребують таємну інформацію, для свого функціонування. Таким чином, не залежно від користувача, задача Za_i безпосередньо ідентифікується в системі надання повноважень, для отримання даних. Запит потрібних даних представляє собою текстові описи їх інтерпретації $D_w^z = [x_i^z, \dots, j(x_{ik}^z)]$. Система надання повноважень (SNP) вміщає крім самих даних не тільки їх значення , а і інтерпретаційні описи цих даних $D_i^s = [j(x_1^s), \dots, j(x_m^s)]$. Система SNP по $j(x_1^s)$ визначає відповідні дані $j(x_{i1}^s)$. На основі інтерпретаційного опису $j(x_i^z)$ система визначає відповідні параметри даних. Наприклад, якщо має місце $\sigma[j(x_1^s) * j(x_i^z)]$, які семантично відрізняються більше ніж на δσ, то пошук даних продовжується. Якщо серед всіх даних типу r_i^t вибрано дані, що задовольняють вимогам вибору, то встановлюються базові параметри даних.

До таких параметрів відносяться наступні параметри даних:

- міра таємності даних $r_i^{kt}(x_i)$;
- міра значимості даних $\aleph_i(x_i)$;
- міра обґрунтованості використання даних $\lambda_i(x_i)$;

Здійснимо розробку алгоритму надання повноважень задачам на

використання даних.

Вирішення задачі

При розробці алгоритму надання повноважень, необхідно реалізовувати процеси аналізу на основі використання числових даних параметрів, які при цьому використовуються. Це означає, що необхідно для всіх параметрів ввести способи визначення їх значень, ввести метрики вимірювання таких значень та узгодити шкали вимірювань різних параметрів. В системі надання повноважень SNP використовуються три групи параметрів, до яких відносяться:

- параметри таємних даних:
- параметри задач, що потребують таємні дані;
- загальні інформаційні параметри.

Крім аналізу методів визначення числових значень параметрів, необхідно визначити методи взаємного аналізу параметрів, що відносяться до DIS з відповідними параметрами, що відносяться до задач, які звертаються до DIS за отриманням даних.

Розглянемо параметри даних, якими є:

- міра таємності $r_i(x_i)$;
- міра важливості $\aleph_i(x_i)$;
- міра обґрунтованості їх використання $\lambda_i(x_i)$.

Міра таємності є величина, що визначається різними інтервалами значень, кожний з яких є певним рівнем таємності. Інтервал між двома рівнями таємності визначає міру таємності, величини яких є меншими від більшої границі інтервалу. Величина інтервалів та кількість мір таємності в них вибираються на основі інтерпретації втрат, в предметній області інтерпретації, до яких приводить несанкціоноване використання відповідних даних. Для визначення таких мір, можуть використовуватися різні масштаби, а кожний інтервал рівня таємності може мати різну кількість відліку мір таємності. Це означає, що в цілому шкала величини параметру таємності є не лінійна і для кожного інтервалу може бути різною. Різні дані, що відносяться до різних елементів W_i, можуть відноситися до різних мір таємності в рамках одного рівня. Деякі величини можуть мати однакову міру таємності і т.д. Зміна міри таємності, яка визначається величиною втрат, реалізується зміною величини таємності, що відповідає величині зміни відповідних втрат. Величина втрат може виявитися більшою ніж міра таємності в деякому інтервалі рівнів таємності. Тому, відповідні втрати приймаються більшими на стільки, щоб така втрата відповідала найближчій більшій мірі таємності. Зменшення міри таємності, що відноситься до даних, які характеризують елемент в W_i, реалізується з дискретністю, яка передбачена встановленими величинами міри таємності в кожному з прийнятих рівнів таємності.

Міра важливості $\aleph_i(x_i)$ є параметром, який на початковому етапі встановлюється у відповідності з проектними, або прийнятими величинами, якщо W_i є технічним об'єктом, чи об'єктом соціального типу, відповідно. На

протязі процесу роботи DIS відслідковується в рамках SNP частота використання відповідного x_i і, в залежності від цього, величина $\aleph(x_i)$ змінюється. При аналізі $\aleph(x_i)$, система SNP визначає, чи величина $\aleph(x_i) \geq \delta_i\aleph$, де $\delta_i\aleph$ - величина порогу, меншим від якого $\aleph_i(x_i)$ не повинен бути.

Міра обґрунтованості визначається на основі аналізу цілі та значимістю x_i, для досягнення цілі $C_i(Za_i)$. В цьому випадку, також використовується порогове значення, яке визначає різницю між $C_i(Za_i)$ та ціллю, яка досягається без використання x_i. В кінцевому випадку $\delta_i\aleph$ і $\delta_i\lambda$ приймаються, як величини без розмірності [4].

В DIS всі дані характеризуються параметрами r_i, $\aleph_i$ і λ_i. Кожен з цих параметрів в процесі роботи SNP аналізується окремо. Якщо аналізовані параметри, значення яких представлені задачею Za_i, або $r_i(x_i^z)$, $\aleph_i(x_i^z)$ та $\lambda_i(x_i^z)$ відповідають приведеним обмеженням, що задаються порогами, то задача отримує доступ до значень відповідних даних, що приведені в рамках задач. Оскільки параметри, які потребує задача описуються у вигляді $j(x_i^z)$, а не адресами їх розміщення, то дані розміщаються в DIS у відповідності з їх текстовими описами. Це означає, що точність тих, чи інших даних визначається повнотою інтерпретаційного опису у відповідному запиті, що надає задача Za_i системі SNP.

Крім характеристик даних, для отримання доступу до тих, чи інших параметрів, задача повинна системі SNP надати характеристики задачі Za_i. Першою з таких характеристик є суперечність задачі: $\sigma^s\{C_i(Za_i)\&[\,Al_i(Za_i)]\&Dw_i(Za)\}$.

В цьому випадку, ціль $C_i(Za_i)$ описується у вигляді деякої структури, а вхідні дані Dw_i описуються областями визначення відповідних вхідних параметрів, що використовується в $C_i(Za)$ та $Al(Za_i)$. Очевидно, що Dw_iтакожпредставляють собою текстові описи їх інтерпретації, на основі яких відповідні Dw_i вибираються з DIS, якщо доступ до даних, система SNP надає. Якщо $\sigma^s\{C_i\&(Al)\&Dw_i\}$ є суперечна, то SNP відмовляє задач Za_i у доступі до даних.

Кожна задача, що використовує таємні дані має свій власний параметр таємності $P(Za_i) = P[M(Za_i), r(Za_i)]$. В цьому випадку, система SNP перевіряє, чи $r_i^{et}(x_i) \geq maxp^r(Za_i) \pm \delta p_i(Za_i)$.

Оскільки r_i^{et} визначає інтервал таємності, або її рівень, то перевіряється приведена нерівність. Аналогічно здійснюється перевірка в частині, що стосується міри таємності задачі, яка повинна також відповідати $\mu(x_i)$.

Значимість задачі $\aleph_i(Za_i)$ представляє собою параметр аналогічний параметру $\aleph_i(x_i)$, тому, він також перевіряється шляхом реалізації порогового контрою різниці між $\aleph_i(x_i \in Za_i)$ та $\aleph_i(Za_i)$.

Актуальність задачі $Ak(Za_i)$ визначається певними критеріями, що відображають еволюційність змін в W_i в результаті розв'язку задачі Za_i. [6]. Такі критерії формуються на основі аналізу W_i і описуються як критерії змін, що можуть відбуватися в W_i в наслідок дії на W_i результатів розв'язку

окремих задач. Оскільки, перед розв'язкам задачі система SNP має можливість аналізувати лише опис цілі задачі $C_i(Za)$, то визначення величини міри актуальності $Ak(Za_i)$ може здійснюватися лише з точністю, яку може забезпечити опис $C_i(Za_i)$. Тому, міра $Ak(Za_i)$, визначена на початковому етапі може виявитися дещо відмінною від реального ефекту впливу розв'язку Za_i на W_i. У зв'язку з цим, система DIS аналізує дані про реальний вплив результатів розв'язку задачі на Za_i і зберігає відповідні дані в наступній формі. Для кожної задачі Za_i, що звертається в DIS за таємними даними, система SNP формує профіль задачі, який вміщає всі параметри, які мають до задачі відношення, включаючи параметри даних та інформаційні параметри, який позначається $Prf(Za_i)$. Якщо окремі параметри, для цієї задачі, змінилися після розв'язку останньої, то відповідні параметри корегуються в профілі задачі $Prf(Za_i)$. Прикладом таких параметрів, що можуть змінюватися, може служити не тільки параметр $Ak(Za_i)$, а і параметр, що змінюється обов'язково – $\aleph(Za_i)$, що виникає з його визначення. Навіть параметр таємності може змінюватися у відповідності з положенням, згідно з яким міра таємності може зменшуватися з ростом параметра $\aleph_i(x_i)$.

До інформаційних параметрів, що характеризують задачу, відносяться: параметр доповнення P_c, параметр повторення P_p, параметр дублювання P_d [7]. Приведенні параметри встановлюються в процесі аналізу задачі, який проводить SNP у випадку, коли Za_i звернулася до SNP за обслуговуванням. Параметр P_c визначає розбіжність між $C_i(Za_i)$ та компонентами задачі $Al(Za)$ та $Dw(Za_i)$. Цей параметр визначається у випадку, коли між $C_i(Za_i)$ і іншими компонентами Za_i виникає суперечність. Ця суперечність, для даного випадку, є дещо специфічна на відміну від класичного уявлення про суперечність. Відрізняються вони тим, що суперечність виникає у випадку, коли $Dw_i(Za_i)$, чи $Al(Za_i)$ ілюструють факт існування недостатньої визначеності $C_i(Za_i)$ по відношенню до $Dw_i(Za_i)$ та $Al(Za_i)$. Наприклад, в Dw_i існують дані, що використовуються в $Al(Za_i)$, а в $C_i(Za_i)$ відсутня будь-яка інформація про результати розв'язку Za_i, які були б пов'язані з відповідними фрагментами Dw_i і Al_i. Параметр P_p означає повторення задачі, яка уже розв'язувалась. Параметр P_d означає дублювання задачі, яка уже розв'язувалась для W_i. На рисунку 1 приведена блок-схема процесу аналізу, який реалізує SNP.

На рисунку 1 використовуються наступні позначення:

- OD - перевірка, чи присутній текстовий опис даних;
- WD - визначення адреси даних;
- DT - визначення, чи дані є таємними;
- VTZ - визначення міри таємності задачі;
- ZP - визначення, чи міра таємності задачі є більша, або рівна мірі таємності даних;

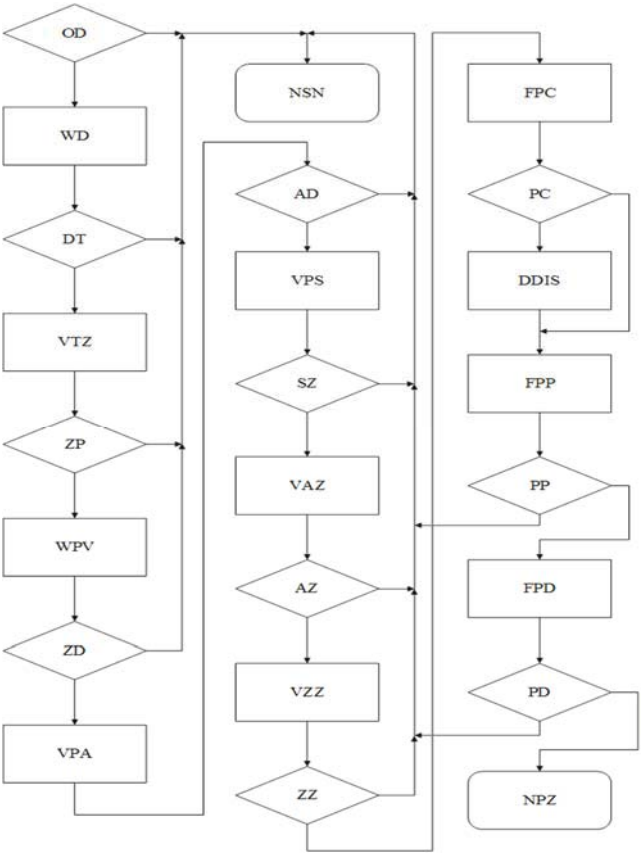

Рис. 1 Блок-схема процесу надання повноважень

- NSN - негативний вихід з системи надання повноважень;
- WPV - визначення параметра значимості даних;
- ZD- перевірка, чи величина значимості даних є допустимою;
- VPA - визначення параметра актуальності даних;
- AD - перевірка, чи значення параметра актуальності даних є допустимим;
- VPS - визначення суперечності задачі;
- SZ - перевірка, чи величина суперечності задачі є допустимою;
- VAZ - визначення актуальності задачі;
- AZ - перевірка, чи величина актуальності задачі є допустимою;
- VZZ - визначення значимості задачі;
- ZZ - перевірка, чи величина значимості задачі є допустимою;
- FPC - формування параметру доповнення даними системи DIS;
- PC - перевірка, чи повинна задача доповнити DISновими значеннями параметрів;
- FPP - формування параметру повторення задачі;
- $DDIS$ - доповнення державної інформаційної системи новими параметрами;

-PP - перевірка , чи задача не повторюється;

-FPD - формування параметру дублювання задачі;

-PD- перевірка, чи має місце дублювання задачі;

-NPZ -надання повноважень задачі на використання даних, за якими задача звернулася до системи DIS.

Після співпраці системи DIS з задачами та наданню задачам таємних даних, виникає необхідність визначення, чине змінився суттєво рівень безпеки системи DIS, в цілому. Для цього, необхідно визначити період співпраці з задачами та умови, при яких така перевірка повинна реалізовуватися. Передача даних, які є таємними, для їх використання задачами, є тим фактором, який може суттєво впливати на рівень безпеки системи DIS. Оскільки рівень безпеки системи DIS є оцінкою інтегральною, яка залежить від цілого ряду факторів, то перш за все, необхідно визначити текучі значення оцінок цих факторів. Першим з таких факторів є рівень таємності та частота використання таємних даних. Наступним фактором є міра прогресивності змін, до яких привело використання результатів розв'язку задач. Третім фактором є кількість задач, яким система відмовила в наданні повноважень на використання таємних даних та ряд інших факторів, які носять більш детальний характер.

Розглянемо параметр таємності і розглянемо функцію, яка пов'язує параметр r_i^{it} з $\beta(DIS)$. Кількісне співвідношення на деякому загальному рівні буде виглядати наступним способом. Приймемо, що небезпека β деякої системи DIS визначається кількістю рівнів таємності даних, які в DIS знаходяться. Безпека, чи небезпека по відношенню до самої DIS, як деякої інформаційної системи не має сенсу. Небезпека, чи необхідний рівень безпеки DIS повинен оцінюватися тими втратами в середовищі W_i, до яких може приводити використання даних з DIS, для розв'язку задач Za_i, які є несанкціонованими. Такі задачі будемо позначати Za_i^n. Система захисту, яка реалізується в DIS, повинна розпізнавати серед всіх можливих задач Za_i несанкціоновані задачі Za_i^n. Несанкціоновані задачі, з точки зору використання результатів їх розв'язку в W_i, є такі задачі, використання яких приводить до зменшення функціональних можливостей W_i, по відношенню до встановленої їх кількості, при формуванні, або проектуванні об'єкту, який становить предметну область інтерпретації даних з DIS. Допустимі різні варіанти визначення негативних змін в W_i, але приведений спосіб визначення негативних змін будемо вважати достатньо універсальним. Тому, міру негативних змін в W_i, які відбуваються в результаті реалізації Za_i^n будемо вимірювати в процентах. Виходячи з того, що використання таємних даних з DIS може приводити до суттєвих негативних змін в W_i приймаємо, що $r_i^{et}(x_i)$ визначається деякою безрозмірною величиною, яка відповідає проценту ушкоджень, до яких може привести Za_i^n, що використовує $r_i^{et}(x_i)$. Таким способом визначення необхідної міри таємності $x_i \in DIS$ дозволяє виключити можливість використання суб'єктивних факторів, при визначенні міри

таємності даних в деякій DIS. При такій інтерпретації необхідної міри таємності даних $x_i \in DIS$, можна прийняти, що зниження міри таємності x_i, приводить до зниження рівня безпеки $\beta(DIS)$ в цілому [5].

Виходячи з викладеного вище, можна співставляти рівень безпеки $\beta(DIS)$ із здатністю засобів захисту DIS, в даному випадку системи SNP, розпізнавати серед всіх можливих задач Za_i, задачі, що є несанкціонованими, або задачі Za_i^n. Система SNP реалізує перевірку параметрів даних, за якими звертається задача, та перевірку значень параметрів самої задачі, що звернулася за отриманням даних до DIS і відповідно SNP. В даному випадку не розглядається ситуація, коли несанкціонована задача звертається за даними, які не є таємними. В цьому випадку приймається, що несанкціоновану задачу може пропонувати тільки несанкціонований користувач. Кожний користувач, що звертається до системи аутентифікується системою захисту доступу.

Висновки

В роботі реалізовано алгоритм надання повноважень задачам на використання даних. Для цього проаналізовані процеси аналізу на основі використання числових даних параметрів. Для всіх параметрів введені способи визначення їх значень, введені метрики вимірювання таких значень та узгоджені шкали вимірювань різних параметрів. Розроблена блок-схема процесу управління функціонування системи надання доступу та досліджуються його можливості.

1. Davydenko A. Formalization level of abstraction of state information resourses access systems / A. Davydenko // Scientific letters of academic society of Michel Baludansky, ISSN 1338-9432. Volume 4, 1 2016, p.35-38.

2. Давыденко А.Н. Расширение теоретических возможностей математических моделей нейронных сетей обуславливаемых их использованием для решения задач защиты систем доступа / А.Н. Давыденко // Збірник наукових праць Інститут проблем моделювання в енергетиці НАН України : Зб. наук. праць вип. 45.. – К., 2008,– С. 112-115.

3. *Давыденко А.Н.* Анализ основных информационных компонент систем доступа / А.Н. Давыденко // Моделювання та інформаційні технології: Зб. наук. праць вип. 59. – К., 2011, – С.11-20

4. *Стахов А.П.* Введение в алгоритмическую теорию измерения / А.П Стахов. – М.: Советскоерадио, 1977.

5. *Ершов Ю.Л.* Математическая логика / Ю.Л. Ершов, Е.А. Палютин. – М.: Наука, 1979.

6. *Морозов А.Д.* Введение в теорию фракталов / А.Д. Морозов. – М.: Ижевск, 2002.

7. *Лейбин В.М.* Информатизация и системне исследования / В.М. Лейбин. – М.: Книжный дом «ЛИБРОКОМ», 2009.

8. *Балакирский В.Б.* Безопасность электронных платежей / В.Б. Балакирский. – СПб.: Конфидент, №5, 1996.

Поступила 1.11.2016р.