ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ БЕЗПЕКИ ІНФОРМАЦІЇ / ORGANIZATIONAL & LAW INFORMATION SECURITY

DOI: 10.18372/2225-5036.23.11817

МОДЕЛЬ БАГАТОРІВНЕВОЇ СИСТЕМИ ДОСТУПУ

Олександр Суліма

Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова, Україна

СУЛІМА Олександр Андрійович

Рік та місце народження: 1991 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2014 рік.
Посада: аспірант Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова з 2014 року.
Наукові інтереси: інформаційна безпека.
Публікації: 10 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях.
E-mail: rfitfo@gmail.com

Анотація. *У цій статті детально розглядається розроблена модель багаторівневої системи доступу до інформації та даних, яка може забезпечити реальну реалізацію адекватних та прийнятних процедур доступу. Функціонування моделі реалізується в кілька етапів: перший етап реалізації методу надання повноважень на використання таємних даних задачею, який полягає в аналізі параметрів задач на основі якого вибирається алгоритм їх обробки с подальшою передачею результатів обробки відповідною задачею; другий етап реалізації методу надання повноважень на використання таємних даних задачею, полягає в обробці даних алгоритмами системи надання повноважень, а результат формується у вигляді рекомендацій у подальшому функціонуванні процесу розв'язку прикладної задачі, третій етап реалізації методу надання повноважень на використання таємних даних задачею, полягає у визначенні умов використання можливих результатів, отриманих прикладною задачею в предметній області. Модель базується на використанні засобів, пов'язаних із захистом даних: підготовка запиту на доступ, автентифікація користувача, надання повноважень, використання рівня таємності, визначений рівень безпеки. Розроблена модель використовує два рівні доступу: нульовий, коли користувач не потребує таємних даних, та перший, коли такі дані необхідні для розв'язання задачі.*

Ключові слова: *захист інформації, система доступу, рівень таємності, рівень безпеки, відкриті дані, величина впливу, модель доступу, багаторівневий доступ.*

Вступ

Проблема підвищення безпеки доступу до інформаційних засобів є актуальною, оскільки така система протидіє несанкціонованому доступу до даних. В роботі описується новий підхід до побудови системи доступу, який полягає в реалізації багаторівневого доступу з розділенням повноважень користувача і задачі.

Багаторівневі системи доступу до інформаційних засобів забезпечують можливість реалізації оптимальних процедур здійснення доступу до даних та інших засобів інформаційної системи. При побудові систем надання повноважень *(SNP)*, розв'язується задача надання повноважень не користувачеві, який отримав статус санкціонованого користувача SK системи захисту доступу до інформаційної системи (DIS), а надається повноваження задачі, що представляється SK і потребує тих, чи інших даних, включаючи дані, що відносяться до категорії таємних. У зв'язку з цим, приводяться визначення мір таємності, яким відповідають відповідні рівні захисту.

Таким чином основною *метою дослідження* є розв'язання задачі, яка полягає в розробці методу побудови багаторівневої системи надання повноважень різним суб'єктам, що звертаються до системи.

Основна частина дослідження

Кількість рівнів, що реалізуються в системі SNP, може визначатися наступними способами, що пов'язані з захистом даних.

На початковій стадії підготовки до запиту на доступ до даних користувач, який ініціює відповідний запит, має власні ідентифікаційні дані та інші дані, які потрібні для того, щоб користувач h_i отримав доступ. Відповідний користувач h_i повинен сформувати дані про задачу, яку йому необхідно розв'язати, використовуючи дані з системи DIS. Якщо користувач, для розв'язку задачі не потребує таємних даних певного рівня, то він може звертатися до системи DIS за отриманням цих даних. При цьому, сама задача може розв'язуватися засобами, що не належать DIS. Такий рівень доступу називається нульовим рівнем.

Дослідження задачі побудови багаторівневої системи доступу, реалізується в кілька етапів. Кількість етапів побудови багаторівневої системи доступу залежить від вибраної кількості рівнів, які будуть використовуватися в системі надання повноважень на використання таємних даних. Кількість визначених рівнів таємності даних та міри їх таємності встановлюється на основі аналізу предметної області до якої відносяться ці дані. В даній роботі розглядається метод побудови системи надання повноважень, що складається з трьох рівнів. Рівні повноважень, про які йде мова в роботі, будуть реалізовуватися в рамках двох блокової системи.

Перший етап реалізації методу надання повноважень на використання таємних даних задачею, яка звернулася за ними.

Перший рівень доступу полягає у наступному. Користувач h_i, що представляє задачу Za_i, яка потребує для розв'язку дані, що характеризуються таємністю, наприклад, першого рівня $r_i^{1t}(x_i)$, реєструється в системі доступу, а задача реєструється в системі наданням повноважень. Якщо система доступу автентифікувала користувача, то у випадку, коли задача, для розв'язку якої потрібні дані, що мають перший рівень таємності $r_i^{1t}(x_i)$, повинна системі SNP надати певні дані про задачу Za_i. Користувач вводить в систему задачу Za_i і може не знати, який рівень таємності мають дані, що потрібні для задачі. Тому інформація про задачу може вводитися в повному обсязі. Після надання задачі повноважень, фрагменти алгоритмів SNP, що визначають допустимі способи використання $r_i^{1t}(x_i)$, реалізують відповідні перетворення і тільки результат цих перетворень, який уже не має рівня таємності $r_i^{1t}(x_i^*)$ передається задачі і задача активізується з місця, для якого дані з SNP є вхідними [1]. У зв'язку з цим виникають наступні задачі:

– введення алгоритмів, які можуть використовуватися для допустимих перетворень $r_i^{1t}(x_i)$ і включення їх в склад системи SNP, які позначаються Az_i;

– перевірка чи є множина алгоритмів Az_i повна з точки зору потреб, які можуть виникнути у окремих задач, що звернулися за даними $r_i^{1t}(x_i)$ до SNP.

Перша задача розв'язується на основі використання наступних положень.

Положення 1. Необхідність введення параметру таємності для x_i^* обумовлюється тим, що є можливим варіант використання цих даних, який може привести до виникнення критичних ситуацій $\mathcal{K}r_i$ в середовищі використання результатів розв'язку задачі, яким є W_i.

Це означає, що не можна допускати можливість використання x_i^*, в результаті якого виникає $\mathcal{K}r_i$, що має негативну інтерпретацію в W_i. У зв'язку з цим, необхідно довести, що всі можливі негативні ситуації $\mathcal{K}r_i(W_i)$, які на даному етапі будемо співставляти з аномаліями An_i, складають обмежену множину і можуть бути визначеними в рамках W_i. Крім того необхідно довести, що множина $\{An_i\}$ є обмежена і кожний елемент цієї множини на початковому етапі формування DIS та W_i може бути визначеним.

Положення 2. Системи DIS орієнтовані на обслуговування соціальних об'єктів або соціальних складових інших об'єктів, якщо такі об'єкти потребують використання DIS.

Розглянемо наступне твердження.

Твердження 1. Множина $\mathcal{K}r_i$ та, відповідно, множина An_i є обмеженими.

Будь-яка область інтерпретації W_i може бути представлена як деяка сукупність простих об'єктів $\{x_1,\ldots,x_n\}$ та сукупність окремих процесів, що позначаються $\{Pr_i(x_{i1},\ldots,x_{im}),\ldots,Pr_i(x_{j1},\ldots,x_{jn})\}$, які можуть взаємодіяти між собою. Така взаємодія реалізується в рамках загальних алгоритмів $\{Al_i,\ldots,Al_n\}$. Для W_i характерно, що одні і ті ж $Pr_i(x_{i1},\ldots,x_u)$ не можуть одночасно використовуватися в різних $Al_i(Pr_i,\ldots,Pr_m)$.

Приймемо, що для Al_i кожне Al_j відрізняється від Al_i кількістю різних процесів, що використовуються у відповідних алгоритмах. З іншого боку, кількість критичних ситуацій, що можуть виникнути в W_i в результаті Al_i не більша кількості різних класів даних, що характеризуються параметрами таємності r_i^{et}. Кількість даних типу $r_i^{et} \geq \mathcal{K}r_i(W_i)$. На протязі одного циклу функціонування DIS, який рівний T, кількість $\mathcal{K}r_i$, буде визначатися співвідношенням $[(\mathcal{K}r_i, < r_i^{et}) \& (\mathcal{K}r_i, \leq (Al_i(T))]$. З цього виникає, що на інтервалі T кількість $\mathcal{K}r_i$ і, відповідно, An_i, які можуть виникати, є обмежена.

Спосіб модифікації даних в DIS, який передбачається в досліджуваному методі.

Оскільки наявність в DIS даних $r_i^z(x_i)$ з часом може зменшуватися, то і кількість $\mathcal{K}r_i$ з часом також буде зменшуватись. Введення нових даних типу $r_i(x_i)$ може реалізовуватися лише при розширенні W_i додатковими елементами $w_{ij} \in W_i$ або за рахунок ускладнення структури W_i, що записується у вигляді $S_i(W_i) \to S_{i+1}(W_i)$.

Будь-які дані можна представляти з певною мірою адекватності їх інтерпретації. Це означає, що дані, які характеризуються параметром таємності також можна представляти або описувати з різною мірою їх точності. Одна з характеристик даних $d_i(x_{i1},\ldots,x_{ik})$ представляє собою точність цих даних по відношенню до факторів, які вони відображають. Формально це можна описати наступним способом в вигляді співвідношення:

$$r_i^{et}(x_i) \to \left[j(x_i) = \left[j(\xi_{i1}) * \ldots * j(o_{ik}) \right] \right] \to$$
$$\to \left[j(\xi_{i1}) \right] * \ldots * j\left(x_{ig}\right) \& (g < k) \} \to$$
$$\to \{ [r_i^{mt}(x_i^*) < r_i^{et}(x_i)] \& [x_i^* = [j(\xi_{i1}) * \ldots * j(x_{ig})]] \}.$$

Це означає, що існує таке перетворення $r_i^{et}(x_i)$, яке може привести до $x_i \to x_i^*$, де $r_i(x_i) > r_i(x_i^*)$. Таким перетворенням може служити алгоритм типу $Al_i(DIS)$, який не є доступний користувачу h_i.

Якщо приведений вище процес модифікації інтерпретаційного опису величини x_i з ціллю зменшення рівня адекватності цього опису, що може відображатися зменшенням рівня точності x_i, продовжити, то можна перейти до такого рівня адекватності опису при якому x_i^* не зможе бути використаним для формування An_i в W_{ij}, а це означає, що x_i^* втрачає параметр таємності $r_i(x_i)$.

В рамках цієї роботи, використання $r_i^{et}(x_i)$, для розв'язування задачі Za_i з цілю $C_i(Za_i)$, є можливим, якщо виконуються наступні умови:

$$[C_i(Za_i) \neq An_i(W_i)] V [C_i(Za_i) \to \neg An_i(W_i)], \quad (1)$$

$$Za_i(x_{i1},\ldots,r_{ij}^t(x_{ij}),\ldots,x_n) \to [(Za_i) \neq An_i(W_i)]. \quad (2)$$

В першій умові мова йде про те, що $C_i(Za_i)$ не представляє собою аномалію, або з $C_i(Za_i)$ не може бути виведена аномалія. Друга умова відповідає випадку, коли розв'язок задачі Za_i, яка використовує $r_i(x_i)$ приводить до цілі $C_i(Za_i)$, яка не представляє собою аномалій $An_i(W_i)$.

Способи забезпечення можливості виконання умов надання необхідних даних поточній задачі.

Для забезпечення приведених вище умов, необхідно таким чином організувати роботу Al_i з даними, що мають рівні таємності $r_i^{et}(x_i)$, щоб процеси перетворення цих даних були не можливим для довільних $Al_i \in Za_i$. Оскільки DIS володіє не тільки даними типу $r_i^{et}(x_i)$, а і їх інтерпретаціями $j(r_i^{et}(x_i))$, а також даними про всі можливі $\mathcal{K}r_i(W_i)$, то в рамках DIS можуть реалізовуватися фрагменти $Az_i \in Al_i$, які безпосередньо реалізують такі перетворення даних типу $r_i^{et}(x_i)$, які не приведуть до виникнення $\mathcal{K}r_i(W_i)$.

Твердження 2. Система $\left[r_i(x_i) \right] \ldots Az_m \left[r_i(x_m) \right] \}$ є повною по відношенню до задач Za_i.

Для того щоб довести твердження необхідно показати, що для довільної Za_i існує Az_i, яка забезпечує коректне використання будь-яких $r_i^{et}(x_i)$. Система SNP перевіряє умову, чи $C_i(Za) \to \mathcal{K}r_i(W_i)$, що реалізується на основі відомих описів $\mathcal{K}r_i(W_i)$ і представлених в Za цілей $C_i(Za_i)$. Крім того, SNP перевіряє, чи $C_i(Za) \neq \mathcal{K}r_i(W_i)$, що також можливе, оскільки всі $\mathcal{K}r_i(W_i)$ є відомими системі DIS. Якщо $C_i(Za_i) \to An_i(W_i)$, то Za отримує модифіковані дані $r_i^{et}(x_i) \to r_i^{gt}(x_i)$, де $g < e$ і проводить перевірку умови:

$$Za_i \left[x_{is},\ldots,x_{in},\ldots,r_i^{gt}(x_i) \right] \to \left\{ \left[C_i(Za_i) \right] \to \left[An_i(W_i) \right] \right\},$$

якщо умова не виконується, то реалізується перетворення $r_i^{gt}(x_i) \to [r_i^{ht}(x_i^*) \& (h < g)]$. Якщо ця умова не виконується, то відповідне перетворення повторюється з елементом $r_i^{ht}(x_i^*)$ до того часу поки умова не стане виконуватися, або поки $r_i^{kt}(x_i^*) \to r_i^{ht}(x_i^{n+1})$, де x_i^{n+1} перестає відноситися до таємних даних [2].

Оскільки алгоритми $Az_i \left[r_i^{it}(x_i) \right]$ є алгоритмами, що реалізують фрагмент перетворення Al_i з Za_i, то перетворення типу (2) виконується, а система $\{ Az_i \left[r_i(x_i) \right], \ldots, Az_i \left[r_m(x_m) \right] \}$ є повна.

З приведеного твердження виходить, що система DIS в цілому і SNP не відмовляє задачі Za_i у наданні необхідних даних, а тільки не допускає можливості окремій задачі Za_i, використовуючи таємні дані, створювати в предметній області W_i, що інтерпретує DIS не допустимі або критичні ситуації. Слід відмітити, що в приведеному випадку мова йде про вибраний діапазон міри таємності, який має певну кількість внутрішніх рівнів, що визначаються на основі аналізу $W_i \to DIS$ і позначаються символом $r_i^{1t}(x_i)$.

Діапазон міри рівнів таємності, який будемо позначати $r_i^{2t}(x_i)$ і в якому кількість рівнів визначається на основі аналізу $An_i(W_i)$, є діапазон, що хара-

ктеризується наступним. Система алгоритмів, що використовується в цьому діапазоні, представляє собою алгоритми Ad_i, які формують результат свого функціонування у дискретній формі. Результат, при використанні Ad_i, визначається на дискретній множині.

Другий етап реалізації методу надання повноважень на використання таємних даних задачею, яка звернулася за ними.

На основі представлених Za_i даних про $C_i(Za_i)$, вхідних даних $\lambda_i(x_i)$ та обґрунтування необхідності використання даних типу $r_i^{2t}(x_i)$, система SNP проводить ряд перевірок, які є спільними для всіх рівнів $r_i^{2t}(x_i)$ та реалізує ряд процесів, що відображають специфіку рівня r_i^{2t}. Як і на попередньому рівні, необхідні дані розпізнаються по їх інтерпретаційних описах, які формуються в задачі та які присутні в DIS. В цьому випадку, для перевірки допустимості використання $r_i^{2t}(x_i)$, в процесі розв'язку задачі, використовуються алгоритми, які є аналогічними до алгоритмів Az_i, але результат проведеного аналізу такі алгоритми формують в дискретній формі [3]. Це означає, що алгоритм Ad_i надає задачі інформацію про те, чи можна використовувати відповідні дані, чи, ні на відміну від рівня $r_i^{1t}(x_i)$, в якому алгоритм Az_i надав задачі можливість використання x_i, але при цьому, надане значення x_i було замінене на менш таємне значення. Алгоритм Ad_i, про який йде мова, аналогічно до алгоритму Az_i реалізує своє функціонування на основі аналізу $An_i(W_i)$, які мають більш високий рівень небезпеки, для функціонування W_i. Алгоритм Ad_i використовує дані типу $r_i^{2t}(x_i)$ таким чином, щоб результат його роботи допускав дискретну інтерпретацію і був узгоджений з Za_i. В більшості випадків, Ad_i дозволяє використовувати задачі Za_i дані типу $r_i^{2t}(x_i)$ у тому випадку, коли задача орієнтована на протидію $An_i(W_i)$, або Za_i орієнтована на елімінацію відповідної $\mathcal{K}r_i(W_i)$. Другою відмінністю роботи Ad_i по відношенню до Az_i є те, що система SNP вимагає, щоб розв'язок задачі Za_i активізувався в середовищі DIS, або у спеціально виділеному окремому обчислювальному середовищі.

Третій етап реалізації методу надання повноважень на використання таємних даних задачею, яка звернулася за ними.

Наступним діапазоном міри таємності, який позначається $r_i^{3t}(x_i)$ і який може мати певну кількість рівнів таємності, функціонує наступним чином. Так само як і в попередніх випадках, алгоритми Ar_i, які є аналогічні до Az_i і Zd_i, проводять аналіз характеристик задачі Za_i. Основними компонентами цих характеристик, є ціль задачі $C_i(Za_i)$, вхідні дані задачі Dw та схеми перетворень, що реалізуються в алгоритмі розв'язку Za_i, що відносяться до перетворень з даними $r_i^{3t}(x_i)$. В результаті такого аналізу алгоритм Ar_i формує ряд умов, про допустимість використання в Za_i даних $r_i^{3t}(x_i)$. На відміну від перших двох діапазонів міри таємності, при виявленні запиту на таємні дані третього діапазону, які відповідають найбільш важливим даним, що стосуються предметної області (W_i), система SNP перевіряє обґрунтованість використання таких даних. Їх не обґрунтоване використання, чи, тим більше, не санкціоноване використання, може привести до значних втрат в середовищі W_i. Тому, безпосереднє використання таких даних тією, чи іншою задачею Za_i повинно не тільки перевірятися на допустимість, а і перевірятися на обґрунтованість розв'язку такої задачі.

Перевірка параметру обґрунтованості представленої задачі в рамках надання повноважень системою SNP.

Обґрунтованість розв'язку задачі перевіряється наступним чином:

– перевіряється чи у відповідності з параметрами Za_i в результаті розв'язування задачі Za_i, не формуються передумови виникнення негативних ситуацій в результаті розв'язування інших санкціонованих задач в області W_i;

– перевіряється чи безпосереднє використання відповідних даних в Za_i, при не суперечній цілі, не приведе до опосередненого розкриття інформації про відповідні таємні дані.

Оскільки міра таємності пов'язується з мірою можливої небезпеки, до якої може привести використання даних, то SNP повинна провести аналіз зовнішніх, по відношенню до DIS і W_i, факторів, що можуть взаємодіяти з $DIS \cup W_i$, або мають відношення до цього комплексу. Перевірка зовнішніх факторів полягає у виявленні зв'язків між зовнішніми факторами та результатами розв'язку задачі, що описуються ціллю [4].

Передумова виникнення негативних факторів означає, що в W_i і DIS сформувалась на логічному рівні структура, яка може виступити активізатором виникнення критичних ситуацій. В загальному випадку це означає наступне: нехай відомо, що $An_i(W_i)$ виникає у випадку, коли в системі можливий наступний вивід або послідовність дій та відповідних подій:

$$\forall Za_i \exists Za_j \left[\left(Za_j \,\&\, Pp_i(W_i) \right) \rightarrow An_i(W_i) \right],$$

де Za_i одна з задач, яка при використанні Pp_i може привести до виникнення $An_i(W_i)$, яка має найвищий рівень аномалії з точки зору її критичності, Pp_i - передумова, яка описується логічною формулою, що виникає в W_i.

Оскільки всі $\mathcal{K}r_i(W_i)$ або $An_i(W_i)$ задаються при формуванні DIS і відповідної системи W_i, то існує можливість провести обернений вивід з ціллю виявлення деякої Pp_i. Якщо Pp_i буде виведено на основі параметрів задачі та $An_i(W_i)$, то SNP відмовить у наданні $r_i^{3t}(x_i)$ задачі Za_i, що буде відповідати першій перевірці.

Спосіб використання текстових описів інтерпретації даних в методі реалізацій процесу надання повноважень системою SNP.

Відомо, що процес розв'язку задачі Za_i, який потребує вхідні дані Dw, використовує не тільки значення цих даних, а і їх інтерпретацію. В більшості випадків інтерпретація вхідних даних відображається або використовується, при проектуванні алгоритму Al, який передбачає використання цих даних. В рамках системи DIS і, відповідно, W_i, крім самих величин значень даних, використовуються текстові описи їх інтерпретації, що є необхідними компонентами бази DIS [4]. Інтерпретаційні описи таємних даних, що описуються у вигляді $j\left[r_i^{3t}(x_i)\right]$ і використовуються для запиту цих даних, представляють собою опис певного їх наближення. Цей наближений опис є відомим для $h_i(Za_i)$. Доповнення такого опису реалізується фрагментом алгоритму Al_{ji}, що знаходиться в SNP. Відповідні перетворення, необов'язково приводять до виявлення повної інформації про $r_i^{3t}(x_i)$. Тому виникає задача перевірки, чи $j(r_i^{3t}(x_i))\,\&\,j(al_i(r_i^{3t}(x_i)))$ не приведе до повного виявлення інформації про $r_i^{3t}(x_i)$, або $J\left[r_i^{3t}(x_i)\right]$ у випадку, коли на основі описів $j\left[r_i^{3t}(x_i)\right]$ та $\left[al_i(x_i)\right]$ можна було б отримати вивід, що описується співвідношенням:

$$\left\{j\left[r_i^{3t}(x_i)\right]\&\,j\left[al_i(x_i)\right]\right\}\rightarrow J\left[r_i^{3t}(x_i)\right],$$

де $J\left[r_i^{3t}(x_i)\right]$ – є повним інтерпретаційним описом таємних даних $r_i^{3t}(x_i)$ з DIS. Якщо такий вивід є можливий, то відповідні дані переходять в статус відкритих даних. Такий перехід може бути не допустимим, якщо в рамках W_i не реалізувалися перетворення, які унеможливили б виникнення відповідної аномалії в W_i. Очевидно, що будь-яке використання таємних даних $r_i^{3t}(x_i)$, для реалізації деякого процесу Pr_i, що породжується алгоритмом Al_i, приводить до пониження таємності відповідних даних на певну величину $\delta\left[r_i^{3t}(x_i)\right]$. Щоб уникнути таких наслідків використання $r_i^{3t}(x_i)$ необхідно відповідні процеси $\mathrm{Pr}_i(Al_i)$ реалізовувати в умовах, які забезпечують відповідний рівень таємності. Цей метод реалізується в рамках даного підходу за рахунок використання внутрішніх алгоритмів Az_i, які використовуються в якості фрагментів $Al_i \in Za_i$. Але це не може в повній мірі гарантувати не розкриття даних $r_i^{3t}(x_i)$, оскільки в рамках реалізації процесів $\mathrm{Pr}_i(Al_i)$ можуть існувати процеси міграції інформації про вхідні дані і, в тому числі, про таємні дані. Дослідження процесів міграції інформації про таємні дані, чи про дані взагалі, які будемо позначати $Im\left[r_i^{3t}(x_i)\right]$ потребують окремого розгляду. Тому приймемо, що використання таємних даних, для розв'язування задач, приводить до певної міри пониження їх таємності. Визначення величини пониження міри таємності за рахунок міграції $Im\left[r_i^{3t}(x_i)\right]$ в рамках даної роботи визначається на основі використання системи прийняття рішення (SPR). В SPR формуються умови та правила, що застосовуються для реалізації процедур виводу певних рекомендацій у випадку, коли величини пониження рівня таємності за рахунок міграції $Im(x_i)$ є не допустимими.

В рамках даного підходу існує можливість компенсувати пониження рівня таємності, що в багатьох випадках уникнути не можливо. Згідно з прийнятим положення про те, що міра таємності визначається мірою загрози, чи небезпеки, до якої може допровадити несанкціоноване використання таємних даних в W_i, пониження рівня таємності даних можна допустити, якщо відповідну небезпеку у необхідній мірі понизити шляхом її часткової елімінації. Цей підхід пов'язаний з необхідністю аналізу предметної області інтерпретації W_i. Тому, цю задачу більш детально розглядати не будемо. Приймемо наступне положення.

Положення 3. Кожне використання таємної інформації приводить до пониження рівня її таємності, як мінімум, за рахунок міграції інформації про ці дані в процесі, що реалізує розв'язок відповідної задачі.

В більшості випадків, в середовищі W_i критичні ситуації приводять до негативних наслідків, коли вони активізуються тими, чи іншими подіями. Серед таких подій можуть бути:

– події, що обумовлюються зовнішніми факторами, які не зв'язані безпосередньо з процесом $\mathrm{Pr}_i[Za_i]$;

– події, що обумовлені процесом розв'язання окремої задачі, яка використовує таємні дані;

– події, що обумовлюються само активізацією аномалій An_i, чи $\mathcal{K}r_i$ в W_i.

Приведені особливості в більшій мірі відносяться до системи прийняття рішень і пов'язані з аналізом області W_i і тому, більш детально розглядатися не будуть.

Спосіб оцінки таємності даних, що реалізується в рамках досліджуваного методу формування багаторівневого доступу.

Розглянемо метод оцінки рівня таємності даних. На загальному рівні відмітимо відповідні положення, що стосуються оцінки таємних даних. Така оцінка потрібна в основному для того, щоб можна було говорити про той чи інших рівень безпеки даних без використання кожного разу опису інтерпретацій величини міри таємності [5]. Оцінка міри таємності $r_i(x_i)$ передбачає необхідність впровадження певної шкали вимірювань. Така шкала повинна бути відносною, оскільки таємність, як деяке поняття, є поняттям відносним. Оскільки уявлення про таємність можна розглядати по відношення до уявлень про величини втрат, при несанкціонованому використанні таємних даних для розв'язку деякої задачі Za_i, то величину рівня таємності доцільно визначати у зв'язку з величиною можливих втрат. Для цього необхідно ввести наступні положення та визначення, що стосуються цих питань.

Положення 4. Оскільки будь-які дані і, у тому числі, таємні дані мають свою предметну область інтерпретації W_i, то параметри, що використовуються для опису цих даних також повинні мати інтерпретацію в цій же предметній області.

Визначення 1. Довільна предметна область W_i, яка розглядається в даному випадку, представляє собою сукупність окремих об'єктів $\{x_i\}$, які об'єднані в деяку структуру $S(X)$, яка може представлятися на графовому та логічному рівнях $G(X)$ і $L(X)$, відповідно, сукупність процесів $Pr_i(X)$, які реалізуються у відповідних структурах, що формально записується у вигляді:

$$W_i = \{G(X), L(X), Pr_i(X)\}.$$

Втрати, які можуть мати місце в W_i обумовлюються виникненням аномалій $An_i(W_i)$, або виникненням критичних ситуацій $Kr_i(W_i)$.

Визначення 2. Кожна W_i функціонує у відповідності з деякою стратегією, або сукупністю стратегій $Sr(W_i)$, які реалізуються на основі використання процесів Pr_i: $St(W_i) = F(Pr_i, \ldots, Pr_m)$, де F – функція взаємозв'язків між Pr_i та Pr_m.

Визначення 3. Аномалією $An(W_i)$ є така зміна в середовищі W_i, яка приводить до неможливості реалізації окремих процесів:

$$An(W_i) \to St(Pr_1, \ldots, \neg Pr_i, \ldots Pr_m).$$

Визначення 4. Критичною ситуацією $Kr_i(W_i)$ є така зміна в середовищі W_i, яка приводить до неможливості реалізації однієї із стратегій:

$$Kr_i(W_i) \to \{St_1 * \ldots * \neg St_i * \ldots * St_m\}.$$

Для використання приведених визначень, при формуванні оцінки величини таємності необхідно ввести наступні умови та обмеження.

Умова 1. Діапазон вимірювання величини таємності окремих даних буде представляти собою шкалу від нуля до 100, а одиницею вимірювання величини таємності приймемо величину процентів.

Введемо наступні положення.

Положення 5. Приймемо, що можуть існувати алгоритми розв'язку задач, або відповідні задачі Za_i, які орієнтовані на досягнення цілі, яка полягає у впровадженні втрат в об'єкті, або предметної області, в якій задача має інтерпретацію.

Положення 6. Можуть існувати задачі, які орієнтовані на цілі, що полягають в розвитку предметної області W_i та на протидії можливим негативним фактором, дія яких на W_i має в рамках предметної області власну інтерпретацію.

Визначення 5. Рівень таємності даних $r_i^t(x_i)$ визначається величиною втрат, до яких може привести реалізація задачі, ціллю якої є безпосередня або опосереднена дія на W_i, яка приведе до втрат, розмір яких можна визначити.

Визначення розміру втрат полягає у аналізі наступних факторів, що можуть мати місце в середовищі W_i:

– неможливість реалізації окремого процесу, або групи процесів $\{Pr_{is}, \ldots Pr_k\}$;

– неможливість реалізації однієї із стратегій $St_i(W_i)$;

– елімінація компоненти x_i з X та інші зміни в W_i, які можуть мати негативну інтерпретацію в довільній із стратегій St_i, які визначаються в W_i.

Очевидно, що одні і ті ж дані можуть використовуватися для реалізації задач позитивного впливу і негативного впливу на W_i [6]. Міра позитивного впливу, яку здійснює реалізація задачі Za_i, може визначати величину таємності даних, з використанням яких такий вплив здійснюється. Незалежно від цього, в першу чергу, величина рівня таємності визначається по величині можливості реалізації негативного впливу на W_i. Величина негативного впливу суттєво залежить від конкретної предметної області та її особливостей. На загальному рівні, величина негативного впливу на W_i визначається наступним чином:

– в діапазоні таємності r_i^{1t} - визначається кількістю елементів $\{x_i\}$ до елімінації яких приводить негативний вплив;

– в діапазоні таємності $r_i^{2t}(x_i)$ визначається кількістю аномалій, до виникнення яких приводить негативний вплив;

– в діапазоні таємності r_i^{3t} визначається кількістю критичних ситуацій до яких приводить негативний вплив.

Всі приведені величини вимірюються в процентах від всього об'єму відповідних факторів, що мають місце у W_i в цілому. Весь діапазон значень в процентах ділиться на три діапазони, які виділяють-

ся для трьох діапазонів таємності даних з W_i. Такий поділ є наступним:

– від 0 % до 50% використовується, для визначення підрівнів таємності в діапазоні r_i^{1t};

– від 50 % до 80% використовується, для визначення підрівнів таємності в діапазоні r_i^{2t};

– від 80 % до 100% використовується, для визначення підрівнів таємності в діапазоні r_i^{3t}.

Такий розподіл шкали рівня таємності ґрунтується на тому, що унеможливлення окремих стратегій приносить максимальні втрати і, коли унеможливлено виконання всіх стратегій, то втрати приймають величину 100%. Втрати окремих процесів визначаються в діапазоні від 50 % до 80%. При цьому, якщо кількість втрачених процесів відповідає втраті однієї St_r, то процент стає рівний величині, яка відповідає втраті одного St_i в діапазоні від 80 % до 100%. Аналогічно існує зв'язок втрат елементів $x_i \in r_i^{3t}(x_i)$ з втратами окремих процесів. З цього виходить, що шкала визначення r_i^t не лінійна і є різною для різних W_i.

Висновки

Запропоновано модель багаторівневої системи доступу для визначення параметрів прикладних задач та методи їх оцінок, які за рахунок використання таємних даних з державної інформаційної системи не залежно від користувача, який представив відповідну задачу, дозволяють здійснювати прийняття рішень системою надання повноважень уникаючи небезпек, які можуть з'явиться під впливом дій користувача.

У відповідності з приведеними в роботі даними досліджено і розв'язано наступні задачі:

– визначено основні етапи реалізації методу побудови багаторівневої системи надання повноважень;

– спосіб модифікації даних в DIS, який передбачається в досліджуваному методі;

– способи забезпечення можливості виконання умов надання необхідних даних текучій задачі;

– розроблено спосіб використання текстових описів інтерпретації даних в методі реалізацій процесу надання повноважень системою SNP.

Література

[1] Y. Zhou, L. Ma, M. Wen, «Task-Constrained RBAC Model and Its Privilege Redundancy Analysis», *2nd International Conference on Information Science and Control Engineering*, pp. 489–492, 2015.

[2] C. Pengrui, W. LingDa, Ya. Chao, Yu Ronghuan, «A hierarchical Access Control model of software repository based on RBAC», *7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pp. 761–765, 2016,

[3] P.-C. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, A. Reninger, «Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control», *IEEE Symposium on Security and Privacy (SP '07)*, pp. 222–230, 2007.

[4] M. VenkataSwamy, S. Ramaswamy, N. Agarwal, «CBPM: Context Based Privacy Model», *IEEE Second International Conference on Social Computing*, pp. 1050–1055, 2010.

[5] P. E. Engelstad, «On the Usability of Clustering for Topic-Oriented Multi-level Security Models», *IEEE European Modelling Symposium (EMS)*, p. 14–20, 2015.

[6] D. Thorleuchter, D. Van den Poel, «High granular multi-level-security model for improved usability», *International Conference on System science, Engineering design and Manufacturing informatization*, pp. 191–194, 2011.

УДК 004.056.52 (045)

Сулима А.А. Модель многоуровневой системы доступа

Аннотация. *В данной статье подробно рассматривается разработанная модель многоуровневой системы доступа к информации и данных, которая может обеспечить реальную реализацию адекватных и приемлемых процедур доступа. Функционирование модели организуется в несколько этапов, к которым относятся: первый этап реализации метода предоставления полномочий на использование секретных тайных данных задачей, который заключается в анализе параметров задач, на основе которого выбирается алгоритм их обработки с последующей передачей результатов обработки соответствующей задачей, второй этап реализации метода предоставлении полномочий на использование тайных данных задачей, заключается в обработке данных алгоритмами системы предоставления полномочий, а результат формируется в виде рекомендаций в дальнейшем функционировании процесса решения прикладной задачи, третий этап реализации метода предоставления полномочий на использование тайных данных задачей, заключается в определении условий использования возможных результатов, полученных прикладной задачей в предметной области. Модель базируется на использовании средств, связанных с защитой данных: подготовка запроса на доступ, аутентификация пользователя, предоставление полномочий, использование уровня секретности, определенный уровень безопасности. Разработанная модель использует два уровня доступа: нулевой, когда пользователь не нуждается тайных данных, и первый, когда такие данные необходимы для решения задачи.*

Ключевые слова: *защита информации, система доступа, уровень секретности, уровень безопасности, открытые данные, величина воздействия, модель доступа, многоуровневый доступ.*

Sulima O. Model of multilevel access system

Abstract. *This paper highlights the model of multilevel access system to information and data that can provide a real implementation of adequate and affordable access procedures.*

The functioning of the model is organized in several stages, which include: the first stage of the implementation of the method for authorizing the use of secret data by the task, which consists in analyzing the parameters of tasks, on the basis of which the algorithm for processing them is selected, followed by the transfer of the results of processing to the corresponding task, authorization to use secret data task is to process data by algorithms of the authorization system, and the result of the form In the form of recommendations in the future functioning of the process of solving an applied problem, the third stage of the implementation of the method for authorizing the use of secret data by the task, the results obtained by the applied problem in the subject area. The model based on the use of funds related to data protection: preparation of a request for access, authentication user empowerment, the use of secrecy, a certain level of security. The model uses two levels of access: zero when the user does not need secret data and the first where such data are necessary for solving the problem.
***Key words**: data protection, system access level of privacy, security level, public data, exposure value, a model of access, multi-access.*

Отримано *10 червня 2017 року*, затверджено редколегією *25 липня 2017 року*