В.О. Куценко // Техногенна безпека та цивільний захист. – 2016. – № 10. – С. 56–64.
3. *Алымов В.Т.* Техногенный риск: Анализ и оценка : [учебное пособие для вузов] / В.Т. Алымов, Н.П. Тарасова. – М. : ИКЦ «Академкнига», 2004. – 118 с.
4. *Берлянд М.Е.* Современные проблемы атмосферной диффузии и загрязнения атмосферы / М.Е. Берлянд. – Л. : Гидрометеоиздат, 1975. – 448 с.
5. *Степаненко С.Н.* Динамика турбулентно-циркуляционных и диффузионных процессов в нижнем слое атмосферы / С.Н. Степаненко. – Одесса : Маяк, 1998. – 288 с.
6. *Прусов В.А.* Моделювання природних і техногенних процесів в атмосфері / В.А. Прусов, А.Ю. Дорошенко. – К. : Наукова думка, 2006. – 542 с.
7. *Попов А.А.* Применение математического моделирования для определения зон влияния выбросов предприятий топливно-энергетического комплекса в атмосферу / А.А. Попов // Інформаційна безпека. – 2014. – № 4(16). – С. 187–193.
8. *Попов О.О.* Математичні моделі оцінки техногенного ризику / О.О. Попов // Электронное моделирование. – 2015. – Т. 37. – № 5. – С. 49–60.
9. *Марчук Г.И.* Математическое моделирование в проблеме окружающей среды / Г.И. Марчук. – М. : Наука, 1982. – 320 с.
10. *Попов О.О.* Розробка стохастичної математико-картографічної моделі забруднення атмосфери викидами від техногенно-небезпечних об'єктів / О.О. Попов // Техногенна безпека та цивільний захист. – 2016. – № 10. – С. 44–55.
11. *Попов А.А.* Использование картографического метода для решения задач комплексного экологического мониторинга техногенно-нагруженных территорий / А.А. Попов // Інформаційна безпека. – 2014. – № 2(14). – С. 195–198.
12. *Яцишин А.В.* Використання інформаційних технологій в задачах управління екологічною безпекою / А.В. Яцишин, О.О. Попов, В.О. Артемчук // Праці Одеського політехнічного університету. – 2013. – Вип. 2(41). – С. 289–294.
13. *Попов О.О.* Математичне та комп'ютерне моделювання техногенних навантажень на атмосферу міста від стаціонарних точкових джерел забруднення : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 01.05.02 "Математичне моделювання та обчислювальні методи" / О.О. Попов. – К., 2010. – 20 с.

Поступила 22.03.2017р.

УДК 004.056.52

О. А.Суліма, Київ

АНАЛІЗ ОСНОВНИХ СИСТЕМ НАДАННЯ ПОВНОВАЖЕНЬ КОРИСТУВАЧАМ

Abstract.Analysis of the method famous authorizing user to use data located in information system. One of widespread methods authorizing based on the use matrix models.

Актуальність

В роботах [1 – 3] обґрунтовано актуальність, поставлено та розв'язано задачу розширення функціональних можливостей технології адаптивного захисту систем доступу до мережевих інформаційних ресурсів за рахунок побудови додаткових критеріїв враховуючих міри таємності, значимості та обґрунтованості використання даних.

Актуальною є задача розширення функціональних можливостей даної технології за рахунок аналізу основних систем надання повноважень користувачам.

Постановка задачі

Сучасні державні інформаційні системи (DIS), які орієнтовані на розв'язування різних задач, що відповідають функціональній орієнтації установ, які їх використовують та наповнюють відповідними даними, в основному орієнтовані на накопичення та збереження інформації з ціллю подальшого надання відповідних даних, в першу чергу, користувачам, які є працівниками цієї установи. Дані що зберігаються в DIS характеризуються різними параметрами один з яких представляє собою параметр важливості цих даних по відношенню до деяких встановлених критеріїв, або параметр міри таємності цих даних.

Наступним параметром, який характеризує дані, представляє собою параметр міри зв'язності окремих даних між собою.

Приведені параметри та особливості, до яких призводять відповідні параметри, обумовлюють необхідність у використанні досить складних механізмів надання повноважень користувачам на використання тих чи інших даних. Такі повноваження характеризуються особливостями, які, в певній мірі, обумовлюють можливість класифікації відповідних систем надання повноважень та визначають критерії, або умови надання чи не надання відповідних повноважень.

Проаналізуємо основні системи надання повноважень користувачам.

Вирішення задачі

Системи надання повноважень в DIS, можуть розділятися на наступні класи:

- системи надання повноважень на основі аналізу параметрів, чи характеристик користувача, який звертається за отриманням тих чи інших повноважень (SPK);
- системи надання повноважень, що ґрунтуються на аналізі параметрів даних, стосовно яких користувач звертається до системи (SPZ);
- система надання повноважень, яка використовує різні аспекти приведених вище систем повноважень.

В рамках відповідних підходів функції надання повноважень та функцій захисту доступу до даних в багатьох випадках розглядаються як єдине ціле [1,2]. Оскільки бази даних переважно орієнтовані, на збереження,

накопичення та надання даних, то система доступу до даних, розглядається як система безпеки відповідної бази даних [3,4]. Тому, в літературі досить часто, по визначенню, відповідні системи розглядаються , як системи безпеки.

Найбільш поширеною моделлю доступу є матрична модель доступу, в якій в першому стовпці матриці розміщаються користувачі, яких прийнято називати суб'єктами, а в першому рядку матриці розміщаються ідентифікатори, даних чи їх груп, які називаються об'єктами. На перетині рядків, кожен за яких відповідає окремому суб'єкту, та стовпців, кожний з яких відповідає певному об'єкту, розміщуються ідентифікатори повноважень відповідного суб'єкта по відношенню до відповідного об'єкта. В загальному випадку, матрична модель записується у вигляді наступного співвідношення: $M = A(S_i, O_j, P_{ij})$, де A матриця, S_i суб'єкт з і-того рядка, O_j об'єкт j -того стовпця, P_{ij} повноваження суб'єкта S_i по відношенню до об'єкта O_j. Прикладом такого повноваження може служити читання даних, запис даних, модифікація даних, зміна повноважень та інші. Якщо $P_{ij} = 0$, то S_i не має повноважень до будь яких дій з O_j.

Очевидно, що матриця $A(S_i, O_j, P_{ij})$ в процесі функціонування DIS , може змінюватися, що витікає з приведених описів параметрів, що характеризують дані, які розміщаються в DIS . Це призводить до того, що модель $M = A(S_i, O_j, P_{ij})$ може мінятися. В першу чергу, розглядаються зміни, що стосуються повноважень S_i по відношенню до O_j. Це означає, що в процесі функціонування DIS можуть змінитися повноваження користувача S_i, що є досить природним. В процесі функціонування DIS , можуть мінятися об'єкти або суб'єкти. Такі зміни описуються додаванням або відніманням окремих рядків та стовпчиків, відповідно. Для зміни повноважень в рамках існуючих множин $\{S_i\}$ та $\{O_j\}$, процеси цих зміни вимагають введення сукупності правил, які можна було би активізувати в процесі функціонування DIS . Така система правил була виведена в роботі [5], яка називається системою «прийми-перекажи» в цій системі використовуються суб'єкти, об'єкти та повноваження.

Ця система привал описує наступні операції:

- операцію «перекажи»;
- операцію «прийми»
- операцію «створи»
- операцію «усунь»

Операція «прийми» описується співвідношенням:

$$[(y(\sigma) \to z)\&(x(t) \to y)] \to [x(h) \to z]$$

Це означає, що суб'єкт x приймає уповноваження h до об'єкту z при умові, що x має уповноваження t приймання повноважень.

Операція «створи» формально описується співвідношенням:

$(x\&\rho) \rightarrow (x(\rho) \rightarrow y)$

Це означає, що коли x має повноваження ρ, то x може утворити зв'язок $x(\rho)$ з суб'єктом або об'єктом y.

Операція «усунь» формально описується співвідношенням :

$[x(\rho) \rightarrow y] \rightarrow [x(\rho \backslash \sigma) \rightarrow y]$

Якщо x має множину повноважень ρ по відношенню до y, то операція «усунь» дозволяє від повноважень ρ відняти повноваження σ і тоді x буде мати по відношенню до y повноваження $(\rho \backslash \sigma)$.

Очевидно, що використання цієї системи правил дозволяє модифікувати матричну модель $M = A(S_i, O_j, P_{ij})$ довільним чином. Така модифікація визначається додатковими умовами, що можуть виникати в процесі функціонування бази даних.

Інший тип моделі доступу ґрунтується на використанні оцінок даних, до яких користувачі подають запит на використання. Очевидно, що для реалізації цього підходу повинна існувати певна оцінка потенціальних користувачів. Тоді надання, чи не надання доступу ґрунтується на співставленні такої оцінки. Прикладом такого типу моделі є модель Белла-Лападули [6].

В цій моделі кожний об'єкт має рівень захисту. Кожний рівень захисту описується класифікацією і множиною категорій. Класифікація представляє собою множину класів безпеки і представляє собою наступні класи:

- явні (I),
- з обмеженим доступом або «для службового використання» (P),
- таємні (T),
- надзвичайно таємні (S).

Множина класу $K = \{I \prec P \prec T \prec S\}$ є впорядкована. Множина категорій встановлюється на основі аналізу середовища, в якому відповідні дані можуть використовуватися. Фрагменти середовища визначають множину користувачів, які відповідні класи даних можуть використовувати. Таким чином, в даному підході не класифікуються безпосередньо користувачі а останні відносяться до згаданих категорій, які характеризуються, як певні елементи середовища. Прикладом можуть служити такі категорії як військовий штаб армії, штаб полку, і т.д. В цьому випадку, рівень безпеки буде позначатися L_i і можна записати, що $L_i = (K_i, C_i)$ є вищий, або рівний рівню безпеки $L_j = (K_j, C_j)$, якщо виконується співвідношення $K_1 \succ K_2, C_{(1} \supseteq C_2$,

що формально можна записати у вигляді наступного співвідношення:

$[(K_i \geq K_j)\&(C_i \supseteq C_j)] \rightarrow (L_i \geq L_j)$.

Досить важливими поняттями, які використовуються, при побудові моделей безпеки, є поняття про стан безпеки системи. Для того, щоб можна було формально описувати відповідне поняття, вводять наступне позначення:

O - множина об'єктів P - множина суб'єктів, L - множина рівнів безпеки. Стан системи описується співвідношенням: $Q = (D, A, \lambda, H)$, де D - множина активних повноважень суб'єктів до об'єктів, A - матриця повноважень, λ - функція рівня безпеки, H - поточна ієрархія об'єктів. Множина D складається з трійок (ρ, o, t), де ρ - суб'єкт o - об'єкт, t - повноваження. Тоді $(\rho, o, t) \in D$. Функція рівня λ описує перетворення: $\lambda: O \cup P \to L$. В теорії захисту інформації використовуються, на ряду з іншими, наступні аксіоми безпеки інформаційної системи:

- аксіома простої безпеки,
- аксіома признаної безпеки,
- аксіома сталості,
- аксіома зірки,
- аксіома не доступності об'єкту не активного,
- аксіома незалежності початкового стану;

Розглянемо для прикладу деякі з цих аксіом. Аксіома простої безпеки формується наступним чином. Суб'єкт може мати повноваження R до об'єкту тільки тоді, коли рівень авторизації суб'єкту є рівнем безпеки, який є вищим, або рівним рівню безпеки об'єкту. Стан системи $Q = (D, A, \lambda, H)$ виконує вимоги аксіоми простої безпеки тоді, коли для кожного елементу $A(\rho, o)$, який має повноваження R, виконується залежність $\lambda_a(\rho) \geq \lambda_a(o)$. Ця аксіома гарантує, що суб'єкт не буде мати повноважень доступу до інформації, яка знаходиться на більш високому рівні безпеки ніж рівень безпеки авторизації суб'єкту.

Аксіома признаної безпеки означає, що для кожного суб'єкта ρ, кожного об'єкту o і кожного повноваження t виконується наступне співвідношення:

$$[(\rho, o, t) \in D] \rightarrow [t \in A(\rho, o)].$$

Це означає, що суб'єкт може використовувати тільки ті повноваження, які є авторизовані в матриці доступу A. Аксіома зірки полягає в наступному. Стан безпеки $Q = (D, A, \lambda, H)$ виконує аксіому зірки тоді, коли для кожного суб'єкта $\rho \in \frac{\rho^{\square}}{\square}$, при $\frac{\rho^{\square}}{\subset P}$, останній входить в множину суб'єктів, які не являються довіреними і, для кожного об'єкту $o_i \in O$ виконується співвідношення:

$$A\rho \in A(\rho, o) \rightarrow \lambda_o(o) \geq \lambda_b(\rho)$$
$$R \in A(\rho, o) \rightarrow \lambda_o(o) \leq \lambda_b(\rho)$$

$$W \in A(\rho, o) \Rightarrow \lambda_o(o) = \lambda_b(\rho).$$

Ці співвідношення означають наступне. Суб'єкт який не є довіреним (під відсутністю довіреності розуміється, що суб'єкт є авторизованим, але рівень безпеки авторизації є нижчий від рівня безпеки об'єкта) може мати повноваження $A\rho$ до об'єкту o якщо рівень безпеки об'єкту G не нижчий ніж текучий рівень безпеки. Друге рівняння означає наступне. Суб'єкт, який не є довіреним може мати повноваження R (повноваження на читання даних) до об'єкту, якщо текучий рівень безпеки суб'єкту є не нижчий ніж рівень безпеки об'єкту. Третє рівняння означає наступне. Суб'єкт, який не є довіреним, може мати повноваження W (повноваження на запис даних) до об'єкту, якщо рівень безпеки об'єкту є рівнем текучому рівню безпеки суб'єкту.

Ці аксіоми описують ситуації, коли текучі рівні безпеки суб'єкту незалежних від рівня безпеки, його авторизації, знаходяться в рамках значень безпеки, які є відповідними текучим значенням рівня безпеки даних, з якими суб'єкт хоче працювати і цей факт описується в матриці доступу, то такий суб'єкт може здійснювати відповідні дії в системі. Ці аксіоми ілюструють той факт, що відповідна система є безпечна.

В довільній інформаційній системі, в процесі її функціонування, здійснюються процедури запису, зчитування, переносу даних, з одного місця в інше, витирання даних, їх модифікація та інші перетворення. В кожній системі існує структура, що відображає класифікацію даних, наприклад, по відношенню до міри їх важливості. Тому, важливою є задача відслідковування процесів, що відбуваються з даними для того, щоб окремі компоненти даних, наприклад, «таємних» не попадали в області пам'яті, в яких знаходяться данні, що відповідають рівню «для службового використання» і навпаки. Крім цього, існує задача, яка полягає у забезпеченні інтегральності даних. Параметр безпеки означає, що данні в процесі функціонування системи, не повинні модифікуватися. В рамках процесу функціонування DIS повинні аналізуватися процеси, що повязані з читанням та записом. Очевидно, що в даному випадку, мова іде про надання, чи не надання тих, чи інших повноважень. Для розв'язку цих задач була розроблена модель Діона, яка представляє собою сукупність визначень та аксіом, що в рамках приведених визначень дозволяють відслідковувати можливості зміни рівнів безпеки даних в інформаційних системах [7].

Важливим методом розв'язку задач контролю доступу є метод, що ґрунтується на використанні уявлень про ролі. Поняття ролі ґрунтується на приписуванні можливостей доступу до об'єктів і в подальшому приписуванні відповідних ролей суб'єктам. Використання ролей пов'язано з тим, що в багатьох організаціях повноваження користувача в значній мірі визначаються його посадою, яку той чи інший користувач займає. У відповідності з

прийнятими поняттями модель доступу, що ґрунтується на використанні уявлень про ролі позначається скороченням $RBAC$[8].

Роль представляє собою суб'єкти, які є не відомими до того часу, поки відповідну роль не стане використовувати конкретна особа. Завдяки цій моделі є можливим, встановлювати залежності між ролями та користувачами. Наприклад, дві різні ролі не можуть реалізовуватися однією особою. Ролі можуть створювати структури ієрархічні, що призводить до того, що ролі вищого рівня ієрархії, можуть управляти повноваженнями ролей, що знаходяться на нижчих рівнях ієрархії.

В рамках моделі $RBAC$ реалізуються наступні повноваження безпеки:

- мінімальні повноваження представляють собою опис об'єктів та повноважень, які є необхідні для розв'язання відповідної задачі,
- розподіл обов'язків полягає в тому, коли розв'язок задачі потребує співпраці двох користувачів, то це призводить до створення двох незалежних ролей, необхідних для виконання відповідної задачі,
- абстракція даних полягає у реалізації прав доступу низького рівня (читання, запис і т.д), які можуть бути об'єднанні в правах доступу високого рівня (передача рахунку, чи його прийом).

Формально, така модель описується наступним чином:

- U - множина користувачів
- P - множина повноважень
- R - множина ролей
- S - множина сесій
- $u \in U$ - окрема ідентифікована особа
- $r \in R$ - опис посади та обов'язків особи і її повноваження
- $s \in S$ - приписи різних ролей вибраному користувачу.

Користувач може починати сесію встановлюючи свою приналежність до певної ролі. Один користувач може відкривати цілий ряд сесій. Модель $RBAC$ перевіряє повноваження користувача до певної ролі, приписує $PA \subseteq PR$ та приписує користвача до ролі або $UA \subseteq UR$.

В рамках моделі реалізується наступні функції. Користувачеві приписується одна сесія, або $S \to U$ та кожній сесії приписується підмножина ролей, або $S \to 2^R$, це означає, що $rola(S) \subseteq \left\{\left(\frac{r}{kopictyba(S)}, r\right) \in UA\right\}$.

В результаті сесія S має повноваження, яке описується наступним чином: $U_{r \in rale(S)} \left\{\frac{P}{P, r} \in PA\right\}$.

На відміну від моделей матричних, в яких задаються користувачі S_i і об'єкти, яким приписуються повноваження $P(S_i, O_j)$, в моделі $RBAC$ визначаються ролі, до яких можна приписувати ті чи інші повноваження, а конкретні користувачі дістають ті чи інші повноваження у випадку, коли вони займають ті, або інші ролі, кожна з яких має певні повноваження. В рамках моделі $RBAC$ задається ієрархічна структура для ролей, яка по суті, є відображенням ієрархічних структур взаємозалежностей між працівниками деякої установи, чи організації, яка встановлює відповідні повноваження для працівників.

Проблеми захисту баз даних досить широко досліджуються, що приводить до створення різних механізмів реалізації доступу до даних, що є досить близьким до уявлень про надання повноважень.

Виходячи з приведеного аналізу, можна стверджувати, що надання повноважень та надання доступу представляють собою споріднені задачі.

В рамках даної роботи уявлення про надання доступу та надання повноважень розділяються наступним чином.

Система захисту доступу і, відповідно, надання користувачеві доступу до системи обов'язково проводить аналіз ідентифікаційних даних користувача і на основі цих даних надає, чи не надає доступ до системи, але ще й розв'язує задачу надання повноважень до реалізації в рамках бази даних певних функцій, які для баз даних є порівняно простими, наприклад, функції читання, запису, модифікації, перестановки, стирання даних, та інші.

Такий підхід приводить до того, що всі фактори, які обумовлюють безпеку системи, пов'язані з персональними даними користувача. Це, в свою чергу, приводить до того, що для реалізації несанкціонованого втручання до бази даних, достатньо в необхідній мірі повноти отримати доступ до ідентифікаційних даних користувача, які є персональними і доступ до них може бути мало зв'язаний з самою базою даних. Більше того, персональні дані, як правило, в тому чи іншому наближенні можуть використовуватися не тільки в рамках співпраці з окремою базою даних.

Це обумовлює більш широкі можливості несанкціонованого заволодіння частиною персональних даних, чи всіма персональними даними. Несанкціонований доступ в більшості випадків є результатом проведення цільових досліджень відповідних систем доступу не уповноваженими користувачами. Для проведення таких досліджень, використовується неповна інформація про персональні дані уповноваженого користувача.

Висновки

Проводиться аналіз відомих методів надання повноважень користувачу на використання даних, що знаходяться в інформаційній системі. Один з поширених методів надання повноважень ґрунтується на використанні матричних моделей. В рамках такої матриці існує можливість зіставити кожному з користувачів певні об'єкти, якими є дані, програми чи процеси до яких окремий користувач може мати певну сукупність повноважень.

Прикладом таких повноважень можуть служити повноваження на виконання операцій читання, запису, заміни інформації та інші. Відомими є моделі надання повноважень, які використовують уявлення про класи безпеки та уявлення про категорії об'єктів.

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* // ЗбірникнауковихпрацьІнститут проблем моделювання в енергетиці НАН України :Зб. наук. працьвип. 45 – К., 2008,– С. 112-115.
3. *Давыденко А.Н.* Анализ основных информационных компонент систем доступа / *А.Н. Давыденко* // Моделювання та інформаційнітехнології: Зб. наук. працьвип. 59. – К., 2011, – С.11-20
4. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты / *А.А. Петров* . – М. :ДМК, 2001 – 448 с.
5. *Гладков Л. А.* Генетические алгоритмы / *Л. А. Гладков, В. В. Курейчик, В. М. Курейчик*. – 2-е изд., испр. и доп . – М. :Физматлит, 2006 . – 320 с
6. *Акимов О. Е.* Дискретная математика: логика, группы, графы, фракталы / *О. Е. Акимов* . – М. : Акимова, 2005 . – 656 с.
7. *УотшемТ.Дж.* Количественные методы в финансах / *Т.ДжУотшем, К. Паррамоу*– М.: Юнити, 1999
8. *Хованов Н. В.* Анализ и синтез показателей при информационном дефиците / *Н. В. Хованов* – СПб.: Издательство Санкт-Петербургского университета, 2011

Поступила 20.03.2017р.

УДК 004.056:004.75

М. Р. Шабан, Київ

ПРОГРАМНА РЕАЛІЗАЦІЯ ПЕРЕВІРКИ ПОВНОТИ ТА НЕСУПЕРЕЧНОСТІ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИСТУ

Abstract. Information security is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Information security responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.

