Використання моделі багаторівневої системи доступу

УДК 004.274:004.056

Олександр Суліма[1], Антон Маметов

ІПМЕ ім. Г.Є. Пухова НАН України, [1]rfitfo@gmail.com

Мета дослідження полягає у вирішенні науково-прикладної задачі побудови інформаційних засобів захисту даних в інформаційних системах [1] на основі використання багаторівневої системи надання повноважень користувачам [2].

Дворівнева модель надання повноважень на використання даних різних рівнів конфіденційності функціонує наступним чином. На першому рівні надання повноважень відповідна система аналізує повноваження користувача, який звертається до системи для отримання даних. Перевіряються ідентифікаційні дані користувача та дані, що визначають його право на доступ до даних певних рівнів конфіденційності. Користувач, який звертається до системи, крім власних даних, повинен надати системі відомості про задачу, для розв’язання якої потрібні відповідні дані. У випадку, коли дані, за якими звернувся користувач, відносяться до вищих рівнів конфіденційності і не повинні надаватися користувачу, то система надання повноважень переходить на другий рівень. На цьому рівні функції користувача виконує прикладна задача, що була представлена користувачем – фізичною особою, і в цьому випадку така задача називається користувачем – задачею. На цьому рівні система надання повноважень проводить аналіз параметрів інформаційних запитів задачі і на його основі приймає рішення про можливість надання даних задачі або ж приймає рішення щодо забезпечення умов, які гарантують можливість вирішення зазначеної задачі. Важливим аспектом функціонування системи надання повноважень на другому рівні є те, що користувач – фізична особа не має можливості впливати на прийняття системою рішення щодо надання повноважень на отримання даних задачею або сприяти забезпеченню можливості розв'язання цієї задачі. Це означає, що під час роботи з даними високого рівня конфіденційності у користувача відсутня можливість вплинути на розв'язання задачі, виходячи з певних суб'єктивних факторів чи інших причин, які можуть мати відношення до нього.

На другому рівні надання доступу відповідна система може виконувати цілий ряд функцій із забезпечення процесу розв'язання прикладної задачі. Для реалізації таких функцій система надання повноважень аналізує дані про предметну область інтерпретації, яку вона обслуговує. Прикладом однієї з можливостей із забезпечення розв’язання прикладної задачі може слугувати наступна можливість системи. Для обраного рівня конфіденційності даних система містить алгоритми, якими можуть перетворюватися відповідні дані. Система надання повноважень обирає алгоритм перетворення даних, який найбільшою мірою відповідає фрагменту алгоритму, що реалізується в задачі і призначений для перетворень цих даних, за якими звертається задача, та за результатами чого здійснює відповідні перетворення даних. Завдяки цьому система не передає дані задачі, а передає їй результат перетворення відповідних даних, який має рівень конфіденційності нижчий, ніж рівень

конфіденційності даних, які перетворювалися. Цей підхід ґрунтується на тому, що дані відповідного рівня конфіденційності можна перетворювати тільки обмеженою кількістю алгоритмів. Це обмеження встановлюється на основі аналізу інтерпретації відповідних даних у предметній області інтерпретації, яку обслуговує відповідна інформаційна система.

Для реалізації процесу побудови багаторівневої моделі надання повноважень водиться ряд положень, які визначають умови використання відповідної системи. Прикладом такого положення є вимога, яка стосується необхідності інтерпретації даних, які використовуються прикладними задачами, які узгоджуються з інтерпретаціями компонентів, що входять до складу предметної області інтерпретації, та обслуговуються інформаційною системою. Доводяться твердження про обмеженість множини критичних ситуацій та аномалій, які можуть виникати в предметній області інтерпретації інформаційної системи. Доводяться також твердження про те, що система засобів, які використовуються системою надання повноважень на використання відповідних даних, є повною відносно задач. У роботі приймається, що необхідність тих чи інших рівнів конфіденційності даних визначається можливим рівнем втрат. До цих втрат може призвести використання результатів розв'язання, які отримані несанкціонованими прикладними задачами. Використання цих результатів може відбуватися лише в предметній області інтерпретації інформаційної системи.

Важливим компонентом системи надання повноважень є система прийняття рішень, використання якої дозволяє співпрацювати з прикладною задачею, яка потребує даних, що мають найвищі рівні конфіденційності. Оскільки необхідний рівень конфіденційності даних визначається рівнем втрат, до яких може призвести використання результатів, отриманих несанкціонованими задачами у відповідній предметній області інтерпретації, що використовує відповідні дані, то можливість пониження рівня конфіденційності даних, при використанні результатів розв’язання санкціонованих задач, може призвести до підвищення рівня безпеки інформаційної системи, що безпосередньо пов'язана з безпекою процесів, які відбуваються в предметній області інтерпретації цієї інформаційної системи.

Список використаних джерел:

1. Давиденко А.М. Використання формальних засобів опису процесів надання повноважень / А.М. Давиденко, О.А. Суліма // Захист інформації – Київ, 2016. - Том 18. - №2. - С.143-149

2. Суліма О.А. Модель багаторівневої системи доступу / О.А. Суліма // Безпека інформації – Київ, 2017. –Том 23. – с. 123-130.