УДК 004.056:061.68

МОДЕЛІ РОЗМЕЖУВАННЯ ДОСТУПУ ДО РЕСУРСІВ ОПЕРАЦІЙНОЇ СИСТЕМИ

Кузьо Д.Б.
Тернопільський національний економічний університет, магістрант

I. Вступ

Ефективність функціонування сучасних операційних систем безпосередньо залежить від того, наскільки відповідають повноваження користувача системи його посадовим функціям. Перевищення повноважень призводить до збільшення ненавмисних помилок користувача, зростання ризиків, пов'язаних з несанкціонованим доступом до даних. При недостатніх повноваженнях виникають складнощі у виконанні співробітником своєї роботи. Захист циркулюючої в операційних системах інформації здійснюється на основі моделей та засобів керування доступом.

Незважаючи на досить високий рівень теоретичних досліджень в області формальних моделей доступу, їх практична реалізація наштовхується на істотні труднощі, пов'язані з формалізацією, тобто забезпеченням відповідності абстрактних сутностей і процесів моделі реальним об'єктам і правилам функціонування операційних систем.

II. Мета роботи

Метою роботи є аналіз переваг та недоліків моделей розмежування доступу до ресурсів операційної системи.

III. Аналіз моделей розмежування доступу

Найбільш відомими та поширеними на сьогодні є класичні моделі, такі як дискреційна та мандатна [1]. Дискреційний контроль доступу дозволяє суб'єктам незалежно визначати права доступу до об'єктів за умови наявності прав власності на дані об'єкти. Даний підхід забезпечує гнучкість і динамічність у зміні повноважень користувачів системи.

При всій наочності і гнучкості можливих налаштувань розмежувальної політики доступу до ресурсів, матричним моделям притаманні суттєві недоліки. Основний з них - це надто громіздкий та деталізований рівень опису відносин суб'єктів і об'єктів. Через це ускладнюється процедура адміністрування системи захисту. Як наслідок, ускладнення адміністрування може призводити до виникнення помилок, збільшення кількості вразливостей та можливостей доступу до інформації з боку порушників. Істотним недоліком дискреційних моделей є також динамічна зміна суб'єктів і об'єктів.

З метою усунення недоліків матричних моделей були розроблені багаторівневі моделі захисту, прикладами яких є модель кінцевих станів Белла і Ла-Падула, а також решітчаста модель Д. Деннінга. Багаторівневі моделі виконують формалізацію процедури встановлення прав доступу за допомогою використання так званих міток конфіденційності або мандатів, що призначаються суб'єктам та об'єктам доступу. Таким чином, багаторівневі моделі дозволяють попередити можливість навмисного або випадкового знищення рівня конфіденційності інформації за рахунок її витоку.

Висновок

У роботі проведено аналіз переваг та недоліків моделей розмежування доступу до ресурсів системи. Проведений аналіз показує, що багаторівневі моделі знаходяться ближче до реальних потреб, ніж матричні моделі, і представляють собою гарну основу для побудови автоматизованих систем розмежування доступу. Мандатні моделі доцільно застосовувати у випадках централізації систем управління доступом, при якій кожен користувач має рівно стільки інформації, скільки йому потрібно, і безпека або надійність даних є основним пріоритетом. Зазвичай це великі системи, де функції всіх членів чітко регламентуються.

Список використаних джерел

1. Девянин П. Н. Модели безопасности компьютерных систем. М.: Издательский центр «Академия», 2005. – 144 с.
2. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”.