УДК 004.9:519.716

М. Л. Тюльпін
А. А. Шиян

УДОСКОНАЛЕННЯ МЕТОДІВ ІДЕНТИФІКАЦІЇ КОНФЛІКТІВ В МАНДАТНИХ МОДЕЛЯХ РОЗМЕЖУВАННЯ ДОСТУПУ

Вінницький національний технічний університет;

Анотація
Проаналізовано мандатні моделі розмежування доступу та запропоновано варіанти їх удосконалення.
Ключові слова: метод, розмежування доступу, ідентифікація конфлікту, удосконалення.

Abstract
Mandate model access control were analyzed and options for their improvement were proposed.
Keywords: method, access control, conflict identification, improvement.

Вступ

Відповідно до стандартів серії ISO 27000 створення системи менеджменту інформаційної безпеки є обов'язковим елементом захисту інформаційних процесів в кожній організації чи підприємстві [1]. Необхідність захисту інформації викликана тим, що наявність інформаційної асиметрії притаманна всім інноваційних процесам, які є потужними драйверами економічного та соціального розвитку країни.

Практична реалізація захисту інформації часто базується на формальних моделях захисту інформації [2]. При цьому переважно розглядаються технічні системи, в яких здійснюються інформаційні процеси. Однак процес переходу від моделей захисту інформації до їх практичної реалізації вимагає наявності додаткових організаційних заходів [3].

Метою роботи є удосконалення методів ідентифікації конфліктів в мандатних моделях розмежування доступу.

Результати дослідження

Основним джерелом для створення інцидентів інформаційної безпеки є людина. Саме завдяки цьому все ще залишається велика потреба в розробці нових та удосконаленні існуючих методів для опису та прогнозування діяльності окремих людей та соціальних груп (як структурованих, так і неструктурованих). Тільки на базі таких моделей можна буде розробити моделі та методи для захисту суб'єктів інформаційної безпеки від негативного впливу.

Модель контролю доступу (MAC) - це метод розподілу доступу за допомогою фіксованого набору дозволів. Модель MAC, по суті, є електронною реалізацією паперового управління конфіденційними документами. У MAC є такі дієві елементи:

- Об'єкти з рівнем конфіденційності. Будь-який файл чи каталог у файловій системі. Такому об'єкту присвоюється будь-яке значення в «дереві» рівнів доступу. Дозволяє об'єкту підвищити рівень конфіденційності (змінити рівень на вищий, а ніж існуючий). Категорично не допускається зниження рівня конфіденційності.
- Суб'єкт з рівнями доступу. Процес будь-якої програми або сесії. Усі об'єкти успадковують, від суб'єкта мітку рівня доступу.
- Ієрархія рівнів доступу, які обробляються в системі (зазвичай зареєстровані в операційній системі). Зазвичай вказується як число без знаку (від нуля до обмеженого реалізацією значення) для зручності. У цьому випадку рівні доступу (вищий/нижчий/рівний) порівнюються за допомогою найпростіших арифметичних дій (більше, менше або дорівнює).

Для Суб'єктів або Рівнів конфіденційності об'єктів визначення рівнів доступу називають зазвичай термінами «мітка прав», «рівень прав», або просто «права».

Повноваження перевіряються кожного разу, коли суб'єкт звертається до об'єкта, котрий захищений MAC.

При перевірці права доступу суб’єкта до об’єкта за мандатною моделлю можливі такі варіанти:

- Права суб'єкта вищі, ніж права об'єкта. Суб'єкту дозволено лише читати об'єкт: він бачить його, але не може змінити.
- Права суб’єкта знаходяться нижче прав об'єкта. Суб’єкту умовно дозволено створювати об’єкт із вищими правами. На практиці суб'єкт немає технічної можливості виконати цю операцію (він просто «не бачить» об'єкт, що змінюється, наприклад, файл або каталог з файлами).
- Права суб’єкта дорівнюють правам об’єкта. У цьому випадку суб’єкту дозволяється читати та змінювати об’єкт.

Можливі варіанти удосконалення методів ідентифікації конфліктів в мандатних моделях розмежування доступу представлено в Таблиці нижче.

Керування доступом на рівні операційної системи (ОС)		**Спеціалізоване програмне забезпечення (ПЗ) з базою даних**		**Спеціалізоване ПЗ з базою даних та власною структурою документів**	
Переваги	**Недоліки**	**Переваги**	**Недоліки**	**Переваги**	**Недоліки**
Будь який файл-документ, каталог	Тип розробки залежить від ОС	Незалежність від ОС	Застосувати до каталогів не можна	Незалежність від ОС	Застосувати до каталогів не можна
	Може бути проблема одночасному доступі (розподіл доступу між ПЗ та ОС)	Будь який файл-документ (завантаживши в базу)	Тривалість розробки	Надання доступу до окремих розділів документу	Тривалість розробки
Рекомендований доступ до ПЗ з локальної мережі.	Рекомендований доступ до ПЗ з локальної мережі.	Доступ до ПЗ звідусіль (інтернет, локальна мережа)		Доступ до ПЗ звідусіль (інтернет, локальна мережа)	Складність розробки (власна структура документа)

Висновки

Проаналізовано мандатні моделі розмежування доступу та запропоновано варіанти удосконалення методів ідентифікації конфліктів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Андреєв В. І., Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки. К. : Вид. ДУІКТ, 2009. 292 с.

2. Богуш В. М., Довидьков О. А., Кривуца В. Г. Теоретичні основи захищених інформаційних технологій. К. : ДУІКТ, 2010. 454 с.

3. US Department of Defense. Department of Defense Trusted Computer System Evaluation Criteria. In: The ‘Orange Book’ Series. Palgrave Macmillan, London : 1985. 116 p.

Тюльпін Михайло Леонідович — студент групи 1КІТС-22М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: mtyulpin@gmail.com

Шиян Анатолій Антонович — канд. фіз.-мат. наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця

Tiulpin Myhailo – Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: mtyulpin@gmail.com

Shyian Anatolii — PhD (Phys. and Math.), Associate Professor, Associate Professor of the Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia