УДК 004.056

Касянчук Н.В.

ДОСЛІДЖЕННЯ МОДЕЛЕЙ ДИСКРЕЦІЙНОГО РОЗМЕЖУВАННЯ ДОСТУПУ

Вінницький національний технічний університет

Анотація

В ході дослідження було проведено аналіз моделей дискреційного розмежування доступом до інформаційних систем. Виявлено низку характерних особливостей, переваг і недоліків існуючих дискреційних моделей управління доступом.

Ключові слова: захист інформації, розмежування доступу, дискреційна модель.

Abstract

In the course of the study, we analyzed the models of discretionary discrimination of access to information systems. A number of characteristic features, advantages and disadvantages of existing discretionary access control models are revealed.

Key words: protection of information, access differentiation, discretionary model.

Вступ

За умови стрімких темпів розвитку інформаційних технологій, збільшення кількості загроз інформації, ступеня невизначеності їх виникнення і реалізації, а також складності систем захисту інформації та їх спеціалізованої спрямованості, набуває актуальності завдання побудови системи захисту інформації.

Захист інформації – це сукупність організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації. Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виключне право тієї або іншої держави. Проте в останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів із різноманітних країн. Слідством цього процесу значно зросла потреба у захисті конфіденційної інформації.

Один із методів захисту інформації є система розмежування прав доступу до неї. Системи розмежування прав доступу здійснюють контроль за доступом суб'єктів інформаційної системи до об'єктів цієї системи. В основі будь-якої такої системи лежить модель розмежування прав доступу.

Результати досліджень

Дискреційна модель розмежування доступу передбачає, що права доступу суб'єктів до кожного окремого об'єкта системи можуть бути довільним чином обмежені на основі деякого зовнішнього по відношенню до системи правила. Також дискреційна модель вимагає ідентифікованості всіх суб'єктів та об'єктів системи. [1]

Основним елементом дискреційного розмежування доступу є матриця доступу. Матриця доступу – це матриця D розміром |S|x|O|, рядки якої відповідають суб'єктам, а стовпчики – об'єктам. Кожний елемент матриці доступу D [s,o] ⊆ R визначає права доступу суб'єкта s до об'єкта o, де R – множина можливих прав доступу. [2]

Суб'єкти s - є активними сутностями, здебільшого це користувачі або процеси. Об'єкти o - є пасивними сутностями, що потребують захисту. Це можуть бути, наприклад, файли, записи баз даних, сегменти оперативної пам'яті. У деяких операціях доступу суб'єкти можуть виступати як пасивні сутності, до яких здійснюють доступ інші суб'єкти, тому множини S та O знаходяться у відповідності S ⊆ O.

У матриці доступу D кожен рядок відповідає певному суб'єктові s, а кожен стовпчик – об'єктові o. Елементом матриці D[s,o] є множина прав доступу, або повноважень суб'єкта s стосовно об'єкта o. Ці права, власне, і визначають, що може робити суб'єкт з об'єктом.

Проведений аналіз систем дискреційного розмежування доступу показав пріоритетність двох напрямів цього виду моделювання, а саме: матричного (модель Харрісона – Руззо – Ульмана) і потокового (класична модель Take – Grant, розширена модель Take – Grant).

Модель Харрісона – Руззо – Ульмана передбачає представлення системи розмежування прав доступу скінченним автоматом, який функціонує згідно з визначеними правилами переходу.[4-5]

Модель Take – Grant застосовується для аналізу систем дискреційного розмежування доступу. За допомогою чого підтверджується або спростовується ступінь захищеності даної інформаційної системи, яка повинна задовольняти регламентованим вимогам. Модель представляє всю систему як спрямований граф, де вузли графа – це, або об'єкти, або суб'єкти. Дуги між ними марковані, і їх значення вказують права, які має об'єкт чи суб'єкт.[6]

Вирішення задачі розмежування доступу в даних моделях зводиться до розв'язання оптимізаційної задачі на матриці або графі.

Дискреційна система є однією з найбільш гнучких систем розмежування доступу. Це є однією з головних причин її широкого розповсюдження. Також дана система розмежування доступу є простою в реалізації. Але порівняльні дослідження цього напряму математичного моделювання дозволили виявити низку недоліків, що істотно знижують сферу застосування моделей.

Наприклад, модель Харрісона – Руззо – Ульмана може виражати велику різноманітність політик дискреційного розмежування доступу, але при цьому не надавати алгоритмів перевірки їх безпеки. Також стає неможливим обмеження суб'єктів-власників об'єктів у наданні ними доступу іншим суб'єктам.

У той же час класична і розширена моделі Take – Grant при розширенні спектра політик безпеки стають занадто громіздкими, через що значно ускладняється їх практичне використання.

Висновки

Отже, в ході дослідження було розглянуто моделі дискреційного розмежування доступу в інформаційних системах, а саме моделі Харрісона – Руззо – Ульмана та Take – Grant. Виявлено їхні переваги та недоліки.

Основною перевагою дискреційної системи розмежування доступу є її проста реалізація і, як наслідок, її широка розповсюдженість на практиці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Девянин П. Н. Модели безопасности компьютерных систем / П. Н. Девянин. – М. : Издательский центр "Академия", 2005. – 144 с.

2. Семенов С.Г. Методика настройки параметров распределения доступа и защиты информации в компьютерных системах критического применения / С.Г. Семенов // Системи озброєння і військова техніка. – Х.: ХУ ПС. – 2012. – Вип. 4(32). – С. 153-158.

3. Семенов С.Г. Методы и средства распределения доступа и защиты данных в компьютеризированных информационных управляющих системах критического применения / С.Г. Семенов. – Х.:НТУ «ХПИ», 2013. – 360 с.

4. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. — Феникс, 2008. — С. 34—40. — 173 с. — ISBN 978-5-222-13164-0.

5. Harrison M., Ruzzo W., Ullman J. ESIGN: Protection in operating systems (англ.). — 1976. — Август (т. 19, № 8). — С. 461–471. — ISSN 0001-0782

6. Миронова В. Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В. Г. Миронова, А. А. Шелупанов, Н. Т. Югов // Доклады ТУСУРа. – 2011. – № 2 (24). – С. 206 – 210.

Наталія Володимирівна Касянчук – студентка групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: natali109788@gmail.com

Nataliia Kasianchuk - student of UB-14b group, faculty of management and information security, Vinnitsa technical university, Vinnitsa, e-mail: natali109788@gmail.com