УДК 004.056.53

Кудлик А. В.

ДОСЛІДЖЕННЯ МАНДАТНИХ МОДЕЛЕЙ КЕРУВАННЯ ДОСТУПОМ ДЛЯ РЕАЛІЗАЦІЇ ВІДПОВІДНОГО ЕЛЕМЕНТУ СТАНДАРТУ АУДИТУ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

Дана робота присвячена дослідженню мандатних моделей керування доступом, а також розглянуто модель розмежування прав доступом яка бере за основу призначення всім учасникам процесу оброблення інформації спеціальних міток.

Ключові слова: аудит, мандатна модель, інформаційна безпека, розмежування доступу, інформаційні технології.

Abstract

This paper is devoted to the study of mandated access control models, and also the model of access rights differentiation which considers the purpose of assigning all participants to the process of processing information of special labels is considered.

Keywords: audit, mandate model, information security, access differentiation, information technology.

Вступ

В сучасному світі розвинутих інформаційних технологій гостро постає проблема захисту інформації та обмеженню доступу до певної інформації. Особливо актуальним є проблема витоку інформації від об’єктів з високим рівнем доступу до об’єктів з низьким рівнем доступу, тобто протидія виникненню каналів зверху вниз.

У даній роботі розглядається розробка прототипу програми, що покликана класифікувати інформацію, шляхом присвоєння інформації певного рівня безпеки.

Основна частина

У роботі розглянуто проблему розмежування доступу, одну з мандатних моделей керування доступом. Поставлено задачу аналізу переваг та недоліків досліджуваних моделей.

Мандатна модель керування доступом ґрунтується на правилах секретного документообігу, прийнятих у державних і урядових закладках багатьох країн.

Основу мандатної (повноважної) політики безпеки (МПБ) становить мандатне управління доступом (Mandatory Access Control - MAC), яке передбачає, що:

1. всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;
2. у системі визначено лінійно упорядкований набір міток секретності;
3. кожному об'єкту системи надано мітку секретності, яка визначає цінність інформації, що міститься в ньому,- його рівень секрет ності в АС;
4. кожному суб'єкту системи надано мітку секретності, яка визначає рівень довіри до нього в АС,- максимальне значення мітки секретності об'єктів, до яких суб'єкт має доступ; мітка секретності суб'єкта називається його рівнем доступу.

МПБ у сучасних системах захисту на практиці реалізується мандатним контролем на найнижчому апаратно-програмному рівні, що дає змогу досить ефективно будувати захищене середовище для механізму мандатного контролю. Пристрій мандатного контролю називають монітором звернень. Мандатний контроль, який ще називають обов'язковим, оскільки його має проходити кожне звернення суб'єкта до об'єкта, організується так: монітор звернень порівнює мітки рівня секретності кожного об'єкта з мітками рівня доступу суб'єкта. За результатом порівняння міток приймається рішення про допуск.

Найчастіше МПБ описують у термінах, поняттях і визначеннях властивостей моделі Белла-Лападула. Основним положенням політики Белла-ЛаПадули, взятими з реального життя, є призначенням всім учасникам процесу оброблення інформації, що підлягає захисту, і документам, в яких вона міститься, спеціальних міток, наприклад, «таємно», «цілком таємно», що дістали назву рівня безпеки.

Усі рівні безпеки впорядковуються за допомогою встановлено відношення домінування. Наприклад, рівень «цілком таємно» вважається більш високим, ніж рівень «таємно», або домінує над ним.

Контроль доступу здійснюється з урахуванням рівнів безпеки сторін, що взаємодіють, на основі двох простих правил:

1. Уповноважена особа (суб'єкт) має право читати тільки ті документи, рівень яких не перевищує його властивості рівня безпеки;
2. Уповноважена особа (суб'єкт) має право зносити інформацію тільки в ті документи, рівень безпеки яких не є нижчим за його власний рівень безпеки.

Рівні безпеки суб'єктів і об'єктів задаються за допомогою функції рівня безпеки, яка ставить у відповідність у відповідність кожному об'єктові і суб'єктові рівень безпеки, що належить множині рівнів безпеки.

Белл та Ла Падула запропонували таке визначення безпечного стану:

1. Стан (F,M) називається безпечним щодо читання тоді і тільки тоді, коли для кожного суб'єкта, що здійснює в цьому стані доступ читання до об'єкта, рівень безпеки цього суб'єкта домінує над рівнем безпеки цього об'єкта: $\forall s \in S, \forall o \in O, read \in M\ [s,o] \rightarrow F(s) \geq F(o)$.
2. Стан (F,M) називається безпечним щодо запиту тоді і тільки доті, коли для кожного суб'єкта, що здійснює в цьому стані доступ запиту до об'єкта, рівень безпеки цього об'єкта домінує над рівнем безпеки цього суб'єкта: $\forall s \in S, \forall o \in O, write \in M\ [s,o] \rightarrow F(o) \geq F(s)$.
3. Стан є безпечним тоді і тільки тоді, коли він є безпечним і щодо читання, і щодо запису.

Белл і Ла Падула довели теорему, що формально доводить безпеку системи при дотриманні певних умов. Теорема дістала назву основної теореми безпеки.

Результати та висновки

Головне завдання мандатної політики безпеки полягає у запобіганні витоку інформації від об'єктів, що мають високий рівень доступу, до об'єктів із низьким рівнем доступу.

На сьогодні найпоширенішим описом мандатної політики безпеки є модель Белла-ЛаПадула.

Перевагами мандатної політики безпеки є те: що її правила прозорі і зрозумілі, а системи, що побудовані на цієї політиці безпеки надійні

Недоліками мандатної політики безпеки є значні вимоги до обчислювальних ресурсів та складність у практичної реалізації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Українські спеціальні системи [Електронний ресурс]. – Режим доступу: http://www.uss.gov.ua/audit-of-information-security. – Аудит інформаційної безпеки інформаційних систем та інформаційно-телекомунікаційних систем.
2. Огнева А.М. Аудит інформаційних систем і технологій [Текст] / А.М.Огнева // Вісник Хмельницького національного університету. Сер. Економічні науки. — 2009. — Т. 1, №6. — с. 229%232.
3. Ярочкин В. И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.
4. Антонюк А. О. Політика безпеки інформації в захищених автоматизованих системах: наукова стаття – М., 2003. – 5 с.
5. StudFiles. [Електронний ресурс]. – Режим доступу: https://studfiles.net/preview/1938199/page:36/. – Модель безопасности Белла – ЛаПадула
6. Учебные материалы. [Електронний ресурс]. – Режим доступу: https://works.doklad.ru/view/Gs62t9DAgvk.html. – Міжнародний аспект

Андрій Вадимович Кудлик – студент групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: andriy.kudlik123@gmail.com

Науковий керівник: ***Шиян Анатолій Антонович*** - кандидат фізико-математичних наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Andrii Vadimovich Kudlyk - student of UB-14b group, faculty of management and information security, Vinnytsia national technical university, Vinnytsia, e-mail: andriy.kudlik123@gmail.com

Supervisor: ***Shiyan Anatoliy Antonovich*** - candidate of physical and mathematical Sciences, associate Professor of management and security of information systems, Vinnytsia national technical University, Vinnytsia.