УДК 004.056

ПЕРЕВАГИ ТА НЕДОЛІКИ КОНЦЕПТУАЛЬНИХ МОДЕЛЕЙ БЕЗПЕКИ УПРАВЛІННЯ ДОСТУПОМ

Дьогтєва Ірина Оксентіївна
асистент
Вінницький національний технічний університет
м. Вінниця, Україна

Анотація: Долідження моделей безпеки управління доступом дозволяють створити передумови не лише для розвитку інформаційної безпеки загалом, а й для розробки методів аналізу захищеності інформаційних систем. Також класичні моделі слугують матеріалом для розробки моделей, які дозволяють точніше та детальніше описувати особливості функціонування систем захисту на практиці.

Ключові слова: інформаційна система, метод контролю доступу, модель безпеки, управління доступом, політика інформаційної безпеки

Відповідно до основної аксіоми теорії захисту інформації питання безпеки інформації описуються доступами суб’єктів до об’єктів [1, с. 6]. Тому для більшості формальних моделей базовим є подання інформаційної системи як сукупності взаємодіючих сутностей – суб'єктів і об'єктів [2, с. 3]. Застосування безпосередньої моделі будується на присвоєнні сутностям ідентифікаторів і формалізації набору правил, що дозволяють визначити, чи має даний суб'єкт доступ до даного об'єкта, причому оскільки суб'єкт також потребує захисту, то особливостями моделей є те, що суб'єкт є окремим випадком об'єкта.

Даний формальний підхід може бути представлений у вигляді графу доступу об'єкта до об'єктів, де безліч графів доступу формують фазовий простір. В такому разі функціонування конкретної системи визначається траєкторією в фазовому просторі, а захист інформації може полягати в тому,

щоб уникати "несприятливих" траєкторій.

Серед основних концептуальних моделей виділяють (табл. 1) [1, с. 10]:

дискреційна або вибіркове керування доступом (Discretionary access control, DAC) – доступ визначається власником об’єкту, тобто власники даних вирішують, хто має доступ до певних ресурсів;

мандатна або примусовий контроль доступу (Mandatory access control, MAC) – реалізується системою за допомогою міток безпеки;

на основі ролей (Role-Based Access Control, RBAC) – визначається функціями користувача, де рішення про надання доступу приймаються системою на підставі ролей і / або посад суб'єктів.

Таблиця 1

Характеристики компонентів основних концептуальних моделей управління доступом

Модель	DAC	MAC	RBAC
сутності (суб’єкти, об’єкти)	ідентифіковані (наявність унікального ідентифікатора)	ідентифіковані	ідентифіковані
суб’єкти (S), користувачі (U)	виступають власниками	рівень доступу	множина ролей (R)
об’єкти (O)	права доступу (P)	решітка рівнів конфіденційності (L, <=) (наявність рівня конфіденційності)	множина прав доступу (P)
реалізація доступу	матриця доступів M [s, o] (s володіє p щодо o в разі наявності даного p в M [s, o])	співвідношення рівня доступу s з заданим L для o	u володіє p, які відповідають r

Деякі сучасні джерела до класичного списку додають ще моделі [2, с. 83]:

на основі атрибутів (Attribute-Based Access Control, ABAC) – доступ забезпечується функцією характеристик суб'єкта; модель заснована на аналізі правил для атрибутів об'єктів або суб'єктів, можливих операцій з ними та середовища, яке відповідає запиту; на основі правил (Rule Based Access Control, RuBAC) – доступ визначається набором правил, детермінованих системним адміністратором; адаптована до ризиків (Risk-Adaptable Access Control, RAdAC) – політика, яка динамічно змінюється відповідно до актуального середовища ризиків.

По суті DAC є основною реалізацією розмежувальної політики при

обробці конфіденційних відомостей, відповідно до вимог системи захисту інформації, яка реалізується за допомогою списку контролю доступу (Access Control List, ACL) чи матриці доступу, в умовах централізованого зберігання.

Крім типового підходу до побудови DAC, при якому кожен об'єкт системи прив'язаний до суб'єкта (власника), який встановлює права доступу до об'єкта (наприклад, керівники підрозділів є власниками даних в рамках своїх підрозділів), існують і системи з єдиним виділеним суб'єктом – суперкористувачем (наприклад, мережевий адміністратор може дозволити власникам ресурсів управляти доступом користувачів до своїх ресурсів), системи з можливістю суб'єкта передавати права доступу іншому суб'єкту та змішані варіанти побудови, коли одночасно в системі присутні як власники, які встановлюють права доступу до своїх об'єктів, так і привілейований користувач, який має можливість зміни прав для будь-якого об'єкта та / або зміни його власника.

Основною перевагою DAC є простота реалізації, яка обумовлюється фактом поширення, недоліками – статичність, яка не враховує динаміку змін станів системи; питання визначеності правил поширення прав доступу і аналіз їх впливу на систему безпеки для класичного варіанту використання.

MAC передбачає використання мітки конфіденційності (аналоги: мітка безпеки (security label), мітка критичності, мітка чутливості (sensitivity labels)) для інформації, що міститься в об'єктах, і видачу офіційних дозволів (допусків) суб'єктів на звернення до інформації відповідного рівня конфіденційності. Варто зауважити, що за сертифікацією CISSP (Certified Information Security Systems Professional) [3, с. 800]: мітка критичності складається з класифікації і категорій, де класифікація використовує ієрархічну структуру, категорії представляють собою окремі види інформації в рамках системи, тобто класифікація вказує на рівень критичності, а за допомогою категорій реалізується принцип «необхідно знати» (need-to-know). При цьому категорії можуть відповідати структурі підрозділів компанії, проектам або рівнями посад, класифікація проводиться за ступенем конфіденційності інформації, і

залежить від середовища, в якому здійснює свою діяльність певна компанія.

В порівнянні з DAC реалізація систем з політикою безпеки MAC досить складна та ресурсоємна, яка практично не використовується «в чистому вигляді» і на практиці доповнюється елементами інших моделей доступу, однак правила в подібних системах досить зрозумілі та спостерігається вища якість надійності таких систем безпеки.

При RBAC права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх використання, утворюючи ролі. В моделі користувачі сортуються за групами або категоріями на основі посадових функцій або відділів, категорії, які в свою чергу, визначають дані, до яких вони мають доступ.

До складу референтної моделі входять [4]: ядро (Core RBAC), ієрархічність (Hierarchical RBAC) та поділ обов'язків (separation of duties). Виділяють два типи ієрархій: обмежені (доступний тільки один рівень ієрархії), звичайні (доступна певна кількість рівнів ієрархії). Модель також дозволяє організувати кілька видів поділу обов'язків, зокрема, статичний (Static Separation of Duty, SSD) та динамічний (Dynamic Separation of Duties, DSD).

До переваг насамперед відносять гнучкість та динамічність змін в процесі функціонування системи правил розмежування доступу, що максимально підходить для компаній з великою «плинністю» кадрів, до недоліків при використанні «в чистому вигляді» – відсутність врахування поточної ситуації. Перспективним в рамках даної моделі є її використання з метою сприяння децентралізованого управління.

Згідно NIST [5, с. 6], ABAC визначається як метод контролю доступу, де запити суб’єкта на виконання операцій над об’єктами надаються або відхиляються на основі призначених атрибутів суб’єкта, об’єкта, умов середовища та набору політик, які визначаються на основі даних атрибутів та умов. Атрибути дозволяють спростити структуру управління за рахунок використання фізичних аспектів бізнесу (дозволи можуть бути засновані на типі користувача, розміщенні, відділі тощо).

Серед переваг виділяють: інтуїтивно зрозумілий характер ABAC, який приховує набори технічних дозволів за простими для розуміння профілями користувачів; гнучкість. Зазвичай ABAC використовують в поєднанні RBAC, з метою поєднання простоти адміністрування RBAC з гнучкими специфікаціями політики та можливістю динамічного прийняття рішень ABAC [6, с. 3-15]. Гібридне рішення ABAC/RBAC (ARBAC) дозволяє системі поєднувати IT і бізнес-структури.

RuBAC по суті дозволяє певним людям отримувати доступ до пристроїв, баз даних або інших обмежених мережевих областей на основі попередньо встановлених критеріїв [2, с. 84].

До переваг RuBAC належать: стандартизація й контроль контексту доступу до ресурсів; покращення безпеки через встановлення необхідних обмежень на використання ресурсів; оптимальний дизайн системи RuBAC з автоматизацією. Серед обмежень виділяють: налаштування детальних правил на кількох рівнях займає багато часу і вимагає попередньої роботи від IT-персоналу, що спричинює необхідність у певній формі постійного моніторингу; громіздкість; потреба в регулярних змінах. Зазвичай RuBAC розглядають в якості додаткової безпеки.

Великомасштабні обчислювальні середовища (зокрема, глобальна інформаційна мережа Міністерства оборони США (GIG)) спричинили появу контролю доступу, адаптованого до ризику (RAdAC).

У RAdAC привілеї доступу надаються на основі комбінації особи користувача, потреби місії та рівня ризику безпеки, який існує між системою, до якої здійснюється доступ, і користувачем [6, с.3-17]. RAdAC для визначення ризиків використовує показники безпеки: вагомість методу аутентифікації, рівень гарантії сеансового з’єднання між системою та користувачем і фізичне місцезнаходження користувача.

Загалом, вибір оптимальної моделі управління доступом залежить від безпосередньо цілей самого бізнесу, стилю управління і безпеки компанії в цілому. В переважній більшості компанії комбінують моделі для отримання

необхідного рівня захисту.

СПИСОК ЛІТЕРАТУРИ

1. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Издательский центр «Академия», 2005. 144 с.

2. Mike Chapple. Access Control, Authentication, and Public Key Infrastructure. Third edition. Burlington, MA : Jones & Bartlett Learning, 2020. 375 p.

3. Shon Harris, Fernando Maymi. CISSP All-in-One Exam Guide, Eighth Edition. McGraw Hill Professional, 2018, 1376 p.

4. INCITS 359-2012[R2017]: Information technology – Role Based Access Control.URL:https://standards.incits.org/apps/group_public/project/details.php?project_id=1906 (дата звернення: 30.01.2022)

5. NIST SPECIAL PUBLICATION 1800-3 Attribute Based Access Control / Bill Fisher, Norm Brickman, Prescott Burden, Santos Jha, Brian Johnson, Andrew Keller, Ted Kolovos, Sudhi Umarji, Sarah Weeks/. SECOND DRAFT. National Institute of Standards and Technology Special Publication 1800-3b, Natl. Inst. Stand. Technol. Spec. Publ. 1800-3b, 2017. 48 p.

6. NIST SPECIAL PUBLICATION 800-95 Guide to Secure Web Services. Recommendations of the National Institute of Standards and Technology / Anoop Singhal, Theodore Winograd, Karen Scarfone. Natl. Inst. Stand. Technol. Spec. Publ. 800-95, 2007. 128 p.