УДК 681.3.06

ПІДХІД ДО МОДЕЛЮВАННЯ РОЛЬОВОЇ ПОЛІТИКИ БЕЗПЕКИ

Віктор Жора
Фізико-технічний інститут НТУУ "КПІ"

Анотація: **Розглянуто принципи моделювання рольової політики безпеки. Сформульовано логіко-математичну модель рольової політики безпеки та запропоновано її структуру. Наведено аспекти практичного застосування рольової політики безпеки.**
Summary: **The report deals with the principles of modelling of Role-Based Access Control. The logical-mathematical model of Role-Based Access Control is formulated and its structure is offered. The aspects of practical application of Role-Based Access Control are also given.**
Ключові слова: **Політика безпеки, роль, користувач, повноваження, сеанс.**

I Вступ

Однією з найважливіших задач при побудові захищених інформаційно-телекомунікаційних систем (ІТС) є пошук необхідних та достатніх умов інформаційної безпеки (ІБ). Політика безпеки (ПБ) є інтегральною характеристикою, що дає змогу визначити умови захищеності системи. В [1] наголошується, що визначення ПБ як набору норм і правил, що регламентують обробку інформації в системі з метою протистояння певній множині загроз, є неповним і пропонується брати до уваги діяльніший аспект, тобто розглядати як складові ПБ концепцію забезпечення ІБ, менеджмент, інжиніринг та аудит безпеки. Тим не менш, в даній роботі пропонується модель ПБ, що більше відповідає визначенню в [2]. В такому сенсі можна ототожнити поняття політики безпеки і політики контролю доступу.

На даному етапі розвитку науково-практичної бази в галузі захисту інформації (ЗІ) прийнято розрізняти три типи ПБ: дискреційну (DAC – Discretionary Access Control), мандатну (MAC – Mandatory Access Control) та рольову (RBAC – Role Based Access Control). Підходи до моделювання перших двох наведені в [3] та [4]. Практична діяльність в сфері ЗІ довела, що дискреційна ПБ найкращим чином пристосована для вирішення проблем контролю доступу в ІТС цивільного призначення. Мандатна ПБ спрямована на ЗІ в ІТС організацій, що працюють з критичною інформацією, де є необхідним багаторівневе розмежування повноважень і прав доступу згідно з допусками до обробки інформації тієї чи іншої категорії.

Звичайно, при виборі ПБ необхідно враховувати види доступів до інформації, особливості її обробки, організаційну структуру ІТС, сферу її застосування, можливі канали витоку інформації та багато інших важливих факторів. Тим не менш, рольова ПБ дозволяє більш гнучко, ніж інші види політик, регламентувати доступ до інформації. Наявність рис дискреційної та мандатної ПБ дозволяє впроваджувати її в більшості типів ІТС.

II Постановка задачі

Розвиток інформаційних технологій разом із розширенням технічних можливостей для несанціонованого ознайомлення з інформацією ставлять нові умови для захищених систем її обробки. Серед багатьох з них – можливість виконання групами користувачів однакових обов'язків, можливість центрального адміністрування ІТС та наявність виділених для цього повноважень, можливість передачі прав доступу користувачам разом із збереженням чіткого розмежування доступу тощо. Потрібно зазначити, що ці послуги забезпечуються в різних програмних продуктах принаймні протягом останніх п'ятнадцяти років, проте лише в середині 90-х років минулого століття постала проблема формалізації альтернативної дискреційній і мандатній ПБ моделі рольової політики. В [5] наводяться вагомі аргументи щодо того, що рольова ПБ як найкраще забезпечує вимоги з ЗІ в цілому класі комп'ютерних систем (КС) цивільного призначення.

Останніми роками виробники почали запроваджувати риси рольової ПБ в системи керування базами даних, системи управління безпекою, мережеві операційні системи. Коренями рольової політики є використання груп в UNIX та інших операційних системах, групування привілеїв в системах керування базами даних та концепція розмежування доступу. Проте, незважаючи на те що рольова ПБ має багато переваг в порівнянні з іншими в питаннях управління безпекою, розробка формалізованої, несуперечливої та уніфікованої моделі триває. Тим не менш, американським Національним Інститутом стандартів і технологій (NIST) вже створено стандарт з рольової ПБ. Для розгляду моделі NIST [6] доцільно запровадити визначення певних понять, що використовуються для описання рольової ПБ, і які не повністю визначені в нормативних документах України в галузі ЗІ.

III Базові визначення

Основним поняттям рольової ПБ є роль – сукупність функцій щодо керування КС, комплексу засобів захисту та обробки інформації, доступних користувачеві. Також її можна визначити як багатозначне відношення між множинами користувачів і повноважень, що регламентується набором функціональних обов'язків фізичних користувачів. За базову пропонується взяти об'єктну модель КС. Згідно з цим під користувачами, процесами і об'єктами ми будемо розуміти відповідно об'єкти-користувачі, об'єкти-процеси та пасивні об'єкти, які, в свою чергу, визначені в [2]. Множину всіх ролей позначимо через **R**. Нехай **U** – множина користувачів системи, **P** – множина процесів, а **O** – множина пасивних об'єктів. Множину всіх можливих доступів в системі позначимо через **A**. Деякі міркування щодо можливої структуризації цієї множини наведено в [7]. Повноваження визначимо як елемент множини повноважень **T**, що будується як декартовий добуток множин процесів, об'єктів та доступів:

$$\mathbf{T} = \mathbf{P} \times \mathbf{O} \times \mathbf{A} . \tag{1}$$

Як часову характеристику КС можна розглядати поняття сеансу, що фактично відповідає часу роботи користувача в системі. Кожний сеанс $S \in \mathbf{S}$ – це відображення користувача на набір ролей, що йому привласнені.

Відношення призначення користувачів позначимо через $\mathbf{UA} \subseteq \mathbf{U} \times \mathbf{R}$. Вибірка з цієї множини для фіксованої ролі виводить список користувачів, яким присвоєна дана роль, тобто тих користувачів, які можуть виконувати функціональні обов'язки згідно з даною роллю в КС:

$$assigned\_users(R) = \{U \in \mathbf{U} \mid (U, R) \in \mathbf{UA}\}, \ R \in \mathbf{R} \tag{2}$$

Відношення призначення повноважень $\mathbf{TA} \subseteq \mathbf{R} \times \mathbf{T}$ дає змогу визначити набір всіх повноважень ролі в контексті її роботи в системі як вибірку з цієї множини для фіксованої ролі:

$$assigned\_privileges(R) = \{T \in \mathbf{T} \mid (T, R) \in \mathbf{TA}\}, \ R \in \mathbf{R} . \tag{3}$$

Цілком природним буде вимагати, щоб залежно від сеансу роботи в системі користувач міг мати різні повноваження. Це необхідно в тому разі, коли одна і та ж людина виконує функціональні обов'язки відповідно до різних посад. Під час одного сеансу цьому користувачеві може бути присвоєна одна роль, а протягом іншого – друга. Взагалі, на початку сеансу користувач може активізувати певну підмножину ролей:

$$session\_roles(S) \subseteq \{R \in \mathbf{R} \mid (U(S), R) \in \mathbf{UA}\}, \ S \in \mathbf{S} , \tag{4}$$

де $U(S)$ – користувач, що ініціював даний сеанс. Він є єдиним, тому кожний сеанс асоційований з одним користувачем, у той час як кожний користувач асоційований з одним або більше сеансами.

Отже, наведені вище поняття є елементами моделі рольової ПБ та формують її структуру.

IV Структура рольової політики безпеки

Згідно з [6] модель рольової ПБ містить в собі чотири компонента:

ядро;

модель ієрархії ролей;

модель бази даних авторизацій;

модель активації.

Ядро є необхідним компонентом при розробці рольової ПБ, позаяк інші є незалежними і можуть бути імплементовані окремо.

Ядро рольової ПБ фактично реалізує розмежування доступу і містить набори основних типів і відношень між ними. Базовими відношеннями є "користувач-роль" та "роль-повноваження", які полегшують розподіл повноважень між користувачами.

Суть даної ПБ полягає в тому, що не користувач або процес асоційований з об'єктами, як це спостерігалось в дискреційній та мандатній ПБ, а роль асоційована з набором повноважень. Отже, користувач може отримати певний доступ до об'єкта тільки тоді, коли він є членом ролі, якій призначено відповідні повноваження.

Таким чином, можна сформулювати умову надання доступу в КС, де реалізовано рольову ПБ. Для цього ми використаємо формалізм моделювання доступу, застосований в [8], а також врахуємо введені в попередньому розділі позначення.

Нехай мав місце ланцюжок доступів $U \xrightarrow{act} *P$, $U \in \mathbf{U}$, $P \in \mathbf{P}$, *act – доступ на активізацію процеса. Доступ* $P \xrightarrow{a} O$, $a \in \mathbf{A}$, $O \in \mathbf{O}$ *в* деякий *момент часу* $t \in \mathbf{N}$ *може відбутися лише за умови*

$$((U, R) \in \mathbf{UA}) \wedge ((R, T) \in \mathbf{TA}) \wedge (T = T(P, O, a)) \wedge (R \in session\_roles(S)),$$
$$R \in \mathbf{R}, S \in \mathbf{S} . \tag{5}$$

Дану умову проілюстровано на схемі ядра рольової ПБ (рис. 1). В разі, якщо під час даного сеансу користувач активізував роль, повноваження якої дозволяють доступ відповідного типу до необхідного об'єкта, цей доступ надається.

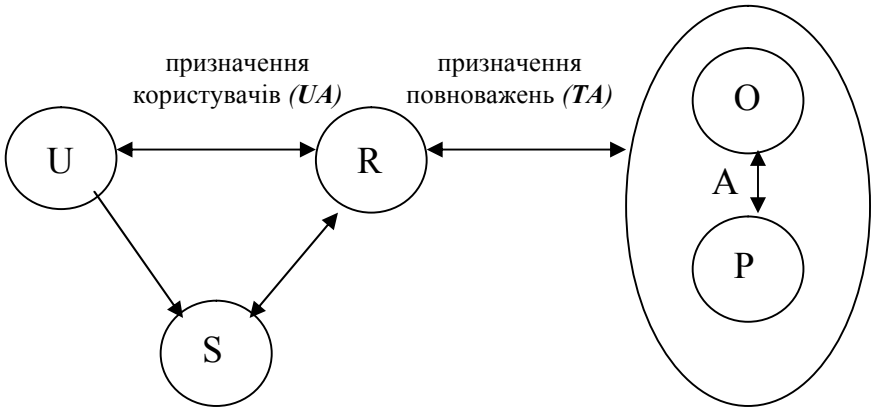

Рисунок 1 – Ядро рольової ПБ

Модель ієрархії ролей додає відношення для підтримки ієрархічної структури підприємства чи установи. Зазвичай ця структура має вигляд дерева або зверненого дерева. З математичної точки зору ієрархія – це частковий порядок, що визначає відношення старшинства між ролями. Старші ролі наслідують повноваження молодших, в той час як молодші – користувачів, асоційованих із старшими. Отже, модель ієрархії ролей визначає відношення включення між ролями, яке ми позначимо "ϕ". $R_1 \phi R_2$ тільки якщо повноваження R_2 є також повноваженнями R_1, а користувачі R_1 є також користувачами R_2. Формально запишемо це наступним чином:

$$\begin{aligned} R_1 \phi R_2 \Rightarrow \quad & (authorized\_privileges(R_2) \subseteq authorized\_privileges(R_1)) \wedge \\ & \wedge (authorized\_users(R_1) \subseteq authorized\_users(R_1)), R_1, R_2 \in \mathbf{R} \\ authorized\_users(R) = & \{U \in \mathbf{U} \mid R' \phi R, (U, R') \in \mathbf{UA}\}, \ R, R' \in \mathbf{R}, \\ authorized\_privileges(R) = & \{T \in \mathbf{T} \mid R' \phi R, (T, R') \in \mathbf{TA}\}, \ R, R' \in \mathbf{R}. \end{aligned} \quad (6)$$

Бачимо, що існує можливість надання повноважень ролі як сукупності повноважень молодших ролей згідно з ієрархією.

Запровадження ієрархії є досить зручним для гнучкого розподілу обов'язків між користувачами, оскільки логічним є розширення повноважень в КС з підвищенням посади працівника. Очевидно, найширші повноваження буде мати адміністратор безпеки – користувач, який відповідає за встановлення відношень між групами типів рольової ПБ, призначення повноважень, накладання обмежень, контроль за адекватністю виконання ПБ тощо.

Модель бази даних авторизацій додає відношення виключення між ролями, пов'язані з функціональними обов'язками користувачів. Статичне розмежування повноважень необхідне для уникнення конфлікту інтересів. Це трапляється, коли один і той самий користувач не може виконувати одну або більше ролей в системі. Наприклад, при обробці електронного платіжного документа його мають завізувати окремо один від одного операціоніст та бухгалтер. Очевидною помилкою буде можливість виконання одним користувачем обов'язків згідно з обома цими посадами. Статичне розмежування повноважень може накладатись як на відношення "користувач-роль", так і на модель ієрархії ролей. Для першого випадку:

$$\begin{gathered} \forall \left(\sum_{k=i}^{k=j} R_k, n \right) \in \mathbf{R^*}, \forall \mathbf{R'} \subseteq \sum_{k=i}^{k=j} R_k : |\mathbf{R'}| \geq n \Rightarrow \prod_{R \in \mathbf{R'}} assigned\_users(R) = \varnothing, \\ i, j, k, n \in \mathbf{N}, n \geq 2, \end{gathered} \quad (7)$$

де $\mathbf{R^*} \subseteq 2^{\mathbf{R}} \times \mathbf{N}$ – множина пар наборів ролей та чисел, що обмежують кількість користувачів, асоційованих з цими наборами.

Для моделі ієрархії ролей:

$$\forall\left(\bigsum_{k=i}^{k=j} R_k, n\right) \in \mathbf{R}^*, \forall \mathbf{R}' \subseteq \bigsum_{k=i}^{k=j} R_k : |\mathbf{R}'| \geq n \Rightarrow \bigcap_{R \in \mathbf{R}'} authorized\_users(R) = \varnothing, \quad (8)$$
$$i, j, k, n \in \mathbf{N}, n \geq 2$$

Модель активації реалізує обмеження повноважень під час сеансу користувача (принцип останньої привілеї), тобто додає відношення виключення, пов'язані з ролями як частинами сеансів, в той час як модель бази даних авторизацій передбачає апріорне обмеження повноважень. За цих умов кожен користувач може мати різні повноваження залежно від часу його роботи в системі. Отже, визначимо динамічне розмежування повноважень як обмеження ролей, що активуються під час сеансу користувача. Це потрібно в тих випадках, коли користувач згідно з статичним розмежуванням обов'язків не може бути членом деякої ролі, проте для робочих цілей має володіти деякими правами, що властиві цій ролі.

$$\forall\left(\bigsum_{k=i}^{k=j} R_k\right), n \in \mathbf{N}, \left(\bigsum_{k=i}^{k=j} R_k, n\right) \in \mathbf{R}^{**} \Rightarrow (n \geq 2) \wedge (j - i \geq n), i, j, k \in \mathbf{N},$$

$$\forall S \in \mathbf{S}, \forall\left(\bigsum_{k=i}^{k=j} R_k\right) \in 2^{\mathbf{R}}, \forall \mathbf{R}'' \in 2^{\mathbf{R}}, \forall n \in \mathbf{N}, \left(\bigsum_{k=i}^{k=j} R_k, n\right) \in \mathbf{R}^{**},$$

$$\mathbf{R}'' \subseteq \bigsum_{k=i}^{k=j} R_k, \mathbf{R}'' \subseteq session\_roles(S) \Rightarrow |\mathbf{R}''| < n,$$

де $R^{**} \subseteq 2^R \times N$ – множина пар наборів ролей та чисел, що обмежують кількість ролей, які можуть бути активізованими протягом сеансу.

Зв'язок моделей ієрархії ролей, бази даних авторизацій та активації з ядром рольової ПБ проілюстровано на рис. 2.

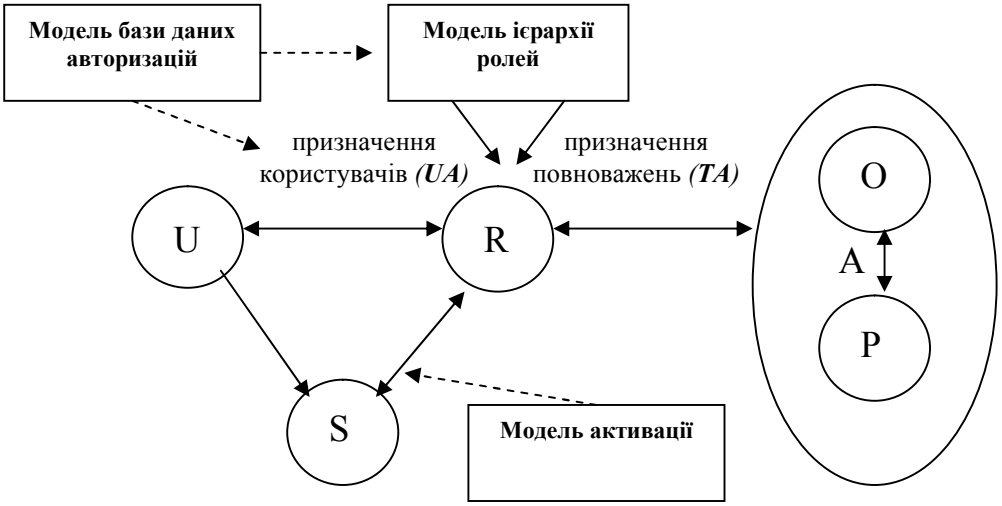

Рисунок 2 – Зв'язок компонентів рольової ПБ з ядром

V Висновки

Модель рольової ПБ, розглянута вище, має наступні переваги над дискреційною ПБ:

- зникає проблема автоматичного поширення прав доступу, оскільки ці права розподіляються переважно за ролями, а не за користувачами;
- вирішується питання контролю за поширенням прав доступу.

Основна перевага рольової ПБ над мандатною полягає в тому, що перша дозволяє реалізовувати захист як конфіденційності, так і цілісності інформації, в той час як мандатні моделі спрямовані на захист однієї з фундаментальних властивостей захищеної інформації.

Гнучкість рольової ПБ пояснюється інкапсуляцією певних рис як дискреційної, так і мандатної ПБ. Керування безпекою є зручним, оскільки атрибути доступу встановлюються не для кожного користувача

окремо, а для цілої групи. Це, в свою чергу, зменшує як часові, так і матеріальні витрати на адміністрування КС. Слабким місцем рольової ПБ є наявність надзвичайних повноважень адміністратора безпеки, що, відповідно, збільшує ймовірність реалізації загроз, спричинених людським фактором. Запобіжними заходами можуть слугувати запровадження протоколювання та аудиту, надання контролюючих функцій іншим користувачам, захист файлів протоколу тощо.

Література: ***1.*** *Бондаренко М, Потій О., Лавріненко В., Горбенко. Ю. Визначення політики безпеки інформаційно-телекомунікаційних систем. – Тези доповідей VI Міжнародної науково-практичної конференції "Безпека інформації в інформаційно-телекомунікаційних системах", 13-16 травня 2003.* ***2.*** *Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-98, ДСТСЗІ СБ України, Київ, 1998.* ***3.*** *Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М.: "Яхтсмен", 1996.* ***4.*** *Bell D. E., La Padula L. J. Secure Computer Systems: Mathematical foundations and model // Report ESD-TR-73-278, Mitre Corp., Bedford, MA, March 1976.* ***5.****Ferraiolo, D. and Kuhn, R. 1992. Role-based access control. In Proceedings of the NIST–NSA National (USA) Computer Security Conference, 554–563.* ***6.*** *David F. Ferraiolo, Ravi Sandhu, Serban Gavrila and D. Richard Kuhn and Ramaswamy Chandramouli. Proposed NIST Standard for Role-Based Access Control. - ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001.* ***7.*** *Антонюк А. О., Жора В. В. Моделювання доступу та каналів витоку в інформаційних системах. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 3 – К.: 2001, с. 156-160.* ***8.*** *Антонюк А О., Жора В. В. Загрози інформації і канали витоку. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 2 – К.: 2001, с. 42-46.*

УДК 681.3.067

РЕШЕНИЕ НЕКОТОРЫХ ПРОБЛЕМ ЗАЩИТЫ МУЛЬТИАГЕНТНЫХ СИСТЕМ

Александр Хошаба, Наталья Месюра
Винницкий национальный технический университет

Аннотация: **Проводится анализ категорий распределенных систем и характерных для них угроз. Основное внимание уделяется разработке методов защиты мультиагентных систем. Рассмотрена реализация платформенных методов защиты мультиагентных систем.**
Summary: **In article the analysis of categories of the distributed systems and characteristic threats for them is carried out. The basic attention is given development of methods of protection in multiagent systems. Realization of platform methods of protection in multiagent systems is considered.**
Ключевые слова: **Защита информационных ресурсов компьютерных сетей, интеллектуальные технологии, мультиагентные системы, распределенные системы.**

I Введение

Работа распределенных систем базируется на функционировании корпоративных и глобальных компьютерных сетей, которые, в свою очередь, требуют использования современных средств защиты информации. В период создания распределенных систем для решения этой задачи главным образом использовались методы, направленные на защиту информационных ресурсов и средств передачи данных. Однако в настоящее время все большую актуальность приобретает решение вопросов политики безопасности распределенных систем, которая должна быть гибкой и прогрессивной.

К одному из важных способов решения задач политики безопасности специалисты относят создание концепции агента для описания современных программных компонент [1 – 5]. Решение задач гибкости и универсальности функционирования программных компонент приводит к созданию мультиагентных систем (МАС).

Для изучения проблем защиты МАС необходимо провести анализ категорий распределенных систем, определить их отличительные характеристики функционирования в смысле использования системных компонент, рассмотреть реализацию платформенных методов защиты МАС.

II Классификация архитектурных стилей распределенных систем

Классификация архитектурных стилей распределенных систем позволяет определить взаимосвязь между