напівжорсткою організацією, Комп'ютерні науки та інженерія, матеріали 3-ї Міжнародної конференції молодих науковців CSE-2009. – Львів: Вид-во Нац. ун-ту "Львівська політехніка", 2009. – С.42–44. 4. Брунець І. Основні показники вибору колаборативного мультимедійного середовища, Комп'ютерні науки та інженерія, матеріали IV Міжнародної науково-технічної конференції CSIT-2009. – Львів: Вид-во Нац. ун-ту "Львівська політехніка", 2009. – С.263–266. 5. Про електронне урядування: (Урядовий портал) [Електронний ресурс] – http://www.kmu.gov.ua. 6. Клименко І.В. Технології електронного урядування / І.В. Клименко, К.О. Ліньова. – К.: Центр сприяння інституційному розвитку державної служби, 2006.– 191 с. 7. Е-урядування – мешканцям Львова: (Офіційний портал Львівської міської ради) [Електронний ресурс] – http://www.city-adm.lviv.ua. 8. Singel R.. Analysis: New Law Gives Government Six Months to Turn Internet and Phone Systems into Permanent Spying Architecture. 9. Електронне урядування: проблеми і перспективи: (Персонал № 10) [Електронний ресурс] – http://www.personal.in.ua/article.php?ida=595. 10. Про електронне урядування: (Регіональний центр розвитку електронного урядування в Автономній Республіці Крим) [Електронний ресурс] – http://crimea.e-gov.org.ua/node/13. 11. Facilitating effective online participation in e-government : (E-government in New Zealand) [Електронний ресурс] / Thorpe S. – http://www.e.govt.nz/resources/research/progress/transformation/chapter13.html.

УДК 004.89

Є.В. Буров, А.В. Гульова
Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж

ВИКОРИСТАННЯ МОДЕЛЕЙ ДЛЯ КЕРУВАННЯ ДОСТУПОМ ДО РЕСУРСІВ ІНТЕЛЕКТУАЛЬНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Запропоновано підхід до використання активних концептуальних моделей для надання та позбавлення прав доступу до ресурсів інформаційної системи. Порівняно з відомим механізмом керування доступом RBAC запропонований метод створює можливість динамічного, документованого надання та вилучення прав доступу до ресурсів у контексті бізнес-процесів, які виконуються у системі.

Ключові слова: контроль доступу, концептуальна модель, інтелектуальна система.

Paper describes an approach of using active conceptual models for access control in information systems. Compared to well known RBAC approach this method provides dynamic, documented and automatic access rights provision and removal within context of currently executed business process.

Keywords: access control, conceptual model, intellectual system.

Постановка проблеми у загальному вигляді

Зростання складності інформаційних систем, підвищення ступеня інтеграції бізнес-процесів (БП) підприємств, подальша глобалізація світової економіки, зростання темпів змін бізнесового середовища вимагає створення інформаційних систем, які здатні аналізувати поточну ситуацію та швидко адаптуватися до змін. Актуальними напрямами досліджень для розв'язання цих задач є застосування рішень наукової галузі штучного інтелекту для видобування знань та моделювання БП [1], розроблення систем бізнес-аналітики (Business Intelligence) для підтримки прийняття рішень. Зокрема, одним з головних завдань другої генерації бізнес-аналітики (BI 2.0) є швидке реагування на події, що виникають у бізнесовому середовищі [2]. Вузьким місцем у створенні таких

систем є підсистема керування доступом до ресурсів, операції якої значною мірою здійснюються вручну, людиною – системним адміністратором.

Аналіз останніх досліджень та публікацій

Наявні сьогодні механізми керування доступом до ресурсів охоплюють такі підходи, як вибірковий (DAC – Discretionary Access Control), мандатний (MAC – Mandatory Access Control), та такий, що використовує ролі (RBAC – Role-based access control).

У DAC політику доступу визначає користувач–власник об'єкта. Власник надає права іншим користувачам. Тому кожен керований ресурс за такого підходу має власника. На практиці у багатьох підприємствах користувачі не володіють інформаційними ресурсами, а єдиним власником є саме підприємство. Крім того, не завжди доцільно, щоб звичайні користувачі мали право надавати доступ для інших користувачів. Отже, DAC не завжди адекватно відображає залежності між суб'єктами та об'єктами доступу. З використанням DAC складно адмініструвати велику кількість ресурсів, неможливо визначати та підтримувати складні політики доступу.

У методі MAC політику доступу визначає система, а не власник. MAC використовується у багаторівневих системах керування доступом, де кожен комп'ютер може опрацьовувати багато рівнів міток секретності, асоційованих з ресурсами. Для отримання дозволу доступу до ресурсу суб'єкт доступу мусить мати рівень доступу не менший, ніж мітка, асоційована з визначеним об'єктом безпеки (керованим ресурсом). Головною проблемою, яку вирішує MAC, є контроль доступу до конфіденційної інформації. MAC широко застосовується у військових системах, де необхідно контролювати доступ до секретних документів і кількість рівнів секретності є порівняно невеликою. Для використання у промислових системах абстракція з мітками доступу не є достатньо гнучкою і не відображає реалій промислових бізнес-процесів [3].

У методі керування доступом, що використовує ролі (RBAC), права доступу також визначає система, а не користувач-власник ресурсу, як в DAC. Ролі в RBAC відповідає множина прав доступу до ресурсів. Механізм RBAC дає змогу визначати доступ до складних бізнес-операцій, наприклад, транзакцій. Користувачі отримують відповідні права через асоціацію з певними ролями. Ролі об'єднуються в ієрархії, у яких дозволи ролей вищих рівнів наслідуються на нижчих рівнях. Керування доступом з використанням ролей має найбільший ефект, коли на підприємстві є багато користувачів з однаковими наборами прав доступу, які і зводяться до визначених ролей. Зміна прав доступу для ролі відразу діє для усіх асоційованих з цією роллю користувачів. [3]. Керування доступом на базі ролей сьогодні є найдосконалішим підходом до керування доступом. Для RBAC розроблено проекти стандартів [4]. Водночас в RBAC права доступу призначаються адміністратором вручну та є статичними.

У роботі [5] визначено головні недоліки механізму керування доступом RBAC:

- у великих організаціях є багато користувачів, набори прав доступу яких змінюються та залежать від поточних завдань, які виконуються. Керування доступом з використанням RBAC у цих умовах призводить до створення великої кількості ролей, якими важко адмініструвати у сукупності;
- у разі додавання до наявної системи нових підсистем кількість ролей зростає в арифметичній прогресії, що на певному етапі унеможливлює ефективне адміністрування;
- зміна змісту ролей вимагає корекції їх визначення. Ці функції, природно, мали б виконувати бізнес-працівники, що приймають рішення, видають завдання для виконання. Але корекція дозволів доступу до ресурсів потребує значних технічних знань, якими бізнес-працівники не володіють. Тому для підтримки RBAC потрібен штат технічних працівників – системних адміністраторів, кількість яких збільшується зі зростанням складності системи;
- з часом права доступу для працівників розширюються, адже під час виконання нових завдань додаються нові права. Зворотний процес (вилучення прав) на практиці не виконується або виконується із значним запізненням. В результаті працівники отримують необгрунтовано великі права доступу, що знижує загальний ступінь захищеності системи та суперечить принципу мінімальних прав доступу.

У [5] для вирішення останньої проблеми пропонують періодично здійснювати аудит системи та вилучати неактуальні права. Водночас, така операція вимагає значних витрат часу і є доволі складною.

Принцип найменших прав [3] є загальноприйнятим у практиці адміністрування. Він полягає у тому, що користувачу надається прав доступу не більше ніж вимагають завдання, які цей користувач виконує. Дотримання цього принципу унеможливлює виконання користувачем зайвих, а також потенційно небезпечних дій. На практиці дотримання принципу найменших прав вимагає детальної специфікації потрібних прав доступу в умовах постійної зміни завдань, які виконує користувач, що є складною задачею.

Еволюція методів керування доступом до ресурсів інформаційної системи значною мірою відбувалася у двох напрямах:

- розв'язання задачі єдиної реєстрації та аутентифікації користувача у межах наявної інформаційної системи. Користувач аутентифікується не для роботи на конкретному сервері, а в усій інформаційній системі або її частині – домені. Для розв'язання цієї задачі були розроблені служби каталогів з відповідною інфраструктурою аутентифікації та загальносистемні політики;
- урахування бізнес-абстракцій з метою створення відповідностей між бізнес-процесами та правами доступу користувачів. Такими бізнес-абстракціями є користувачі, групи, посади, організації, організаційні підрозділи, ролі. Детальніше такі абстракції та пов'язані з ними механізми призначення прав доступу описані у [6]

На нашу думку, підходи до керування доступом мають такі істотні недоліки:

- відсутність документованого обгрунтування рішення з присвоєння або позбавлення прав доступу;
- рішення з керування доступом не пов'язані явно з наявними на підприємстві бізнес-процесами та правилами. Водночас, власне бізнес- процеси та правила є джерелом та підставою для призначень прав доступу;
- рішення про присвоєння прав доступу приймає системний адміністратор, який є технічним працівником, а не менеджер проекту або інша особа, яка уповноважена приймати управлінські рішення та безпосередньо керує виконанням бізнес-процесів;
- ручний характер призначення прав доступу – часто реактивний, а не проактивний процес призначення – призводить до затримок у виконанні процесів;
- відсутність шаблонів, типових конфігурацій прав доступу, які можна застосовувати повторно для різних користувачів, призводить до непродуктивного використання людських ресурсів;
- не враховується наявність різнотипних керованих ресурсів інформаційної системи, таких як файлові системи різних комп'ютерів, таблиці СУБД, доступ до приміщень (електронні замки), різноманітні інформаційні сервіси. Відсутність планування доступу до різнотипних ресурсів в контексті виконання певного виробничого завдання або ролі призводить до відсутності координації доступу, помилок і затримок у виконанні завдань;
- наявність різнотипних керованих ресурсів, що зберігають окремі варіанти облікових записів однієї і тієї самої людини, призводить до того, що користувачу необхідно запам'ятовувати велику кількість паролів. Складність пароля обмежена здатністю людини його запам'ятати. Якщо відмовитися від запам'ятовування пароля, то можна створювати довші та складніші паролі і, отже, краще захистити систему.

В результаті призначені права доступу є часто неадекватними до завдань, які виконує працівник – прав доступу забагато або замало. Недостатність прав доступу призводить до неможливості або істотних затримок у виконанні завдання, що негативно впливає на бізнес-процес загалом. Надлишок прав доступу, хоч і створює додаткові можливості для працівника щодо вибору різних способів вирішення завдання, загалом зменшує захищеність інформаційної системи і не відповідає принципу найменших прав доступу.

У роботі [7] описано підхід до використання активних, семантично-орієнтованих концептуальних моделей для розв'язання задач в інтелектуальній інформаційній системі.

Цілі статті

Метою цієї статті є розроблення методу керування доступом до ресурсів з використанням моделей доступу, який враховує структуру бізнес-процесів та великою мірою вирішує зазначені вище проблеми.

Архітектура та основні принципи керування доступом в інтелектуальній інформаційній системі

Керування доступом до ресурсів з використанням моделей відбувається в інтелектуальній системі моделювання та підтримки виконання бізнес-процесів, описаній у [7, 8]. Складовими частинами цієї системи моделювання (рис. 1) є база фактів, онтологія, репозиторій моделей. Онтологія займає центральне місце у системі, тому що всі інші складові формулюються на її основі. Так, факти з бази фактів є об'єктами, визначеними в онтології. Кожна модель з репозиторію моделей формулюється з використанням понять, також визначених в онтології. В онтології формулюються загальні обмеження та залежності між типами об'єктів, які враховуються під час створення та використання моделей.

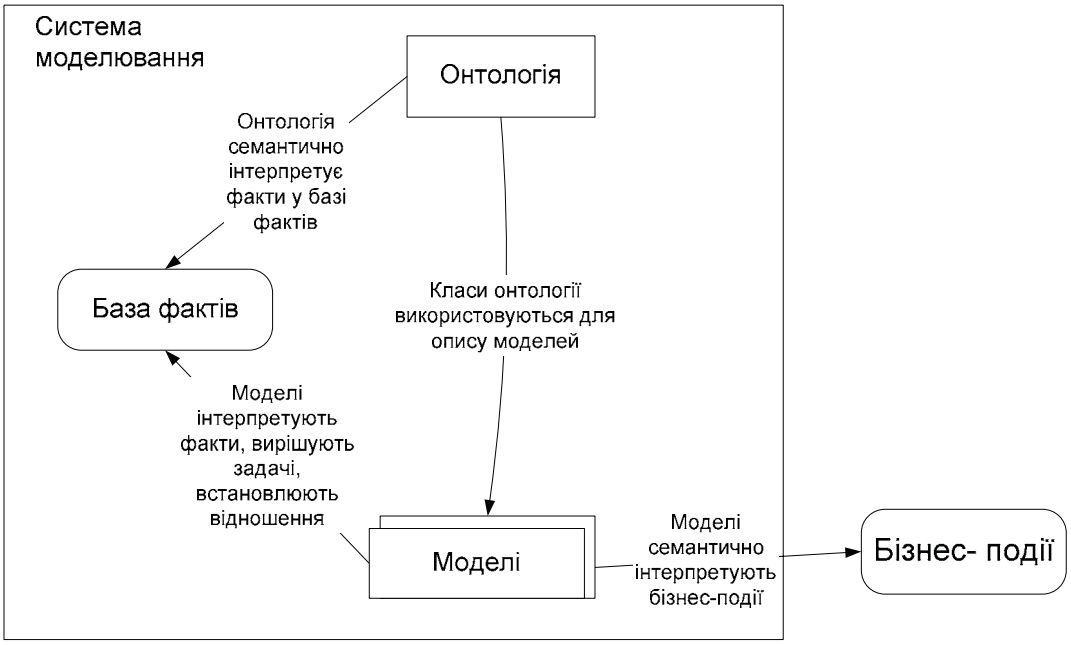

Рис. 1. Складові частини системи моделювання

Моделі застосовуються для виконання операцій у системі. Кожна модель призначена для розв'язання однієї конкретної задачі і є порівняно простою. Водночас, модель у процесі виконання може активізувати інші моделі. Так формуються складні конгломерати моделей, які у сукупності вирішують складні завдання. Моделі створюються людиною-експертом, та відображають її знання про спосіб розв'язання конкретної задачі.

У роботі [8] визначено два типи бізнес-моделей, що використовуються у системі – нормативні моделі та робочі моделі. Робочі моделі відображають реальні події, документи, бізнес-операції як об'єкти (факти) онтології. Робочі моделі застосовують та створюють у процесі виконання бізнес-процесів. Для забезпечення відповідності між реаліями та фактами бази фактів, необхідно, щоб інформаційна система не дозволяла інших способів проведення бізнес-операцій, ніж за посередництвом системи моделювання.

Нормативні моделі відображають бізнес-правила, стандартні процедури, шаблони документів та накладають додаткові обмеження на робочі моделі, мета яких – досягти відповідності корпоративним та державним стандартам.

Моделі керування доступом до ресурсів (надалі – ресурсні моделі), по суті, є нормативними моделями, що обмежують доступ до визначених ресурсів та асоціюються з окремими операціями робочої моделі бізнес-процесу, керованими ресурсами, та з певною множиною працівників.

На рис. 2 наведено загальну схему ресурсної моделі. Ресурсна модель загалом специфікує функціональні ролі працівників та ресурси необхідні для виконання конкретного (часто типового) бізнес-завдання. У моделі визначено множину ролей та множину ресурсів. Як ресурси використовуються бізнес-абстракції, зрозумілі бізнес-працівнику (наприклад, документ, сервіс електронної пошти, Інтернет). Між ролями та ресурсами визначено відношення, зважені (параметризовані) такими характеристиками, як обмеження доступу (наприклад, тільки для читання) кількісні обмеження (наприклад, максимальний трафік).

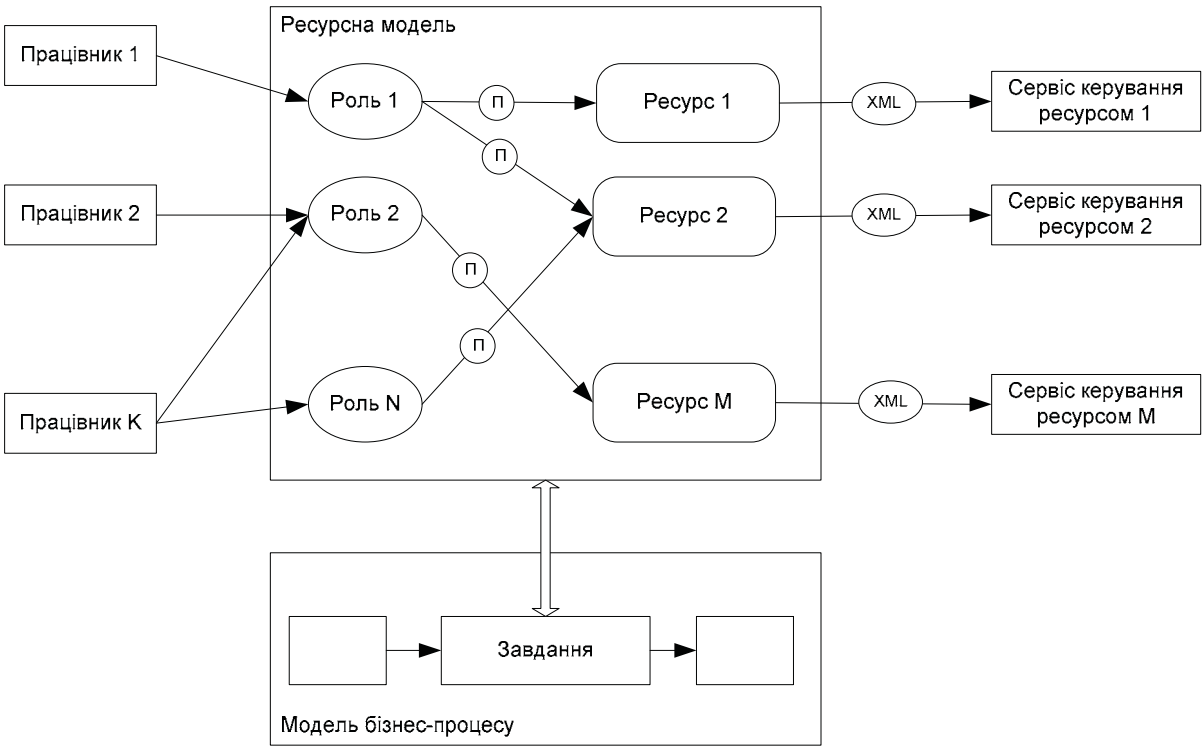

Рис. 2. Загальна схема використання ресурсної моделі

Перед початком виконання завдання ролі моделі асоціюються з конкретними працівниками, які виконують ці ролі. Цю операцію реалізує менеджер, а не системний адміністратор. Після проведення такої асоціації і за умови, що відповідна бізнес-модель є активною, асоційовані працівники набувають визначені ресурсною моделлю права доступу. Після закінчення виконання завдання надані права доступу автоматично вилучаються. Надання прав доступу відбувається через формування моделлю XML-файлів, які містять всю необхідну інформацію, та відсилання цих файлів відповідним сервісам керування ресурсами.

Ресурсні моделі працюють з семантичною абстракцією людини – працівника фірми, а не користувача комп'ютера, як це зроблено, наприклад, в операційних системах. Це дає змогу відстежувати права доступу до різноманітних ресурсів і в контексті виконання виробничих завдань працівником. Відповідно у базі фактів для кожного працівника зберігаються відомості про бюджети, назви користувачів та паролі, з якими цей працівник працює з різними сервісами та комп'ютерами інформаційної системи. Цю інформацію використовують для надання доступу до конкретних ресурсів. Працівник може і не володіти інформацією про свої облікові записи та паролі. При цьому необхідно забезпечити його аутентифікацію на початку роботи з системою із застосуванням, наприклад, біометричних методів або смарт-карток.

Моделі асоціюються не тільки з окремими операціями моделі бізнес-процесу, але й із певними фактами бази фактів. Це забезпечує надання прав працівнику залежно від його посади, віку, статі, підтримує виконання загальнокорпоративних політик доступу, незалежно від завдань, які виконує працівник. Наприклад, так реалізуються такі правила, як "Кожен працівник фірми має доступ до сервісу електронної пошти" або "Кожен працівник фірми має доступ до корпоративного інтранет-порталу", "Керівнику проекту дозволено ініціювати міжнародні дзвінки".

Розглянемо використання ресурсної моделі на прикладі бізнес-процесу створення технічної пропозиції (Technical Proposal) для проекту з розроблення програмного забезпечення (рис. 3). Процес розроблення технічної пропозиції розпочинається після отримання від потенційного замовника запиту на технічну пропозицію (RFP – request for proposal). У запиті сформульовані вимоги замовника щодо кінцевого продукту, технологій та процесу розроблення, бізнесові очікування щодо термінів розроблення та якості продукту.

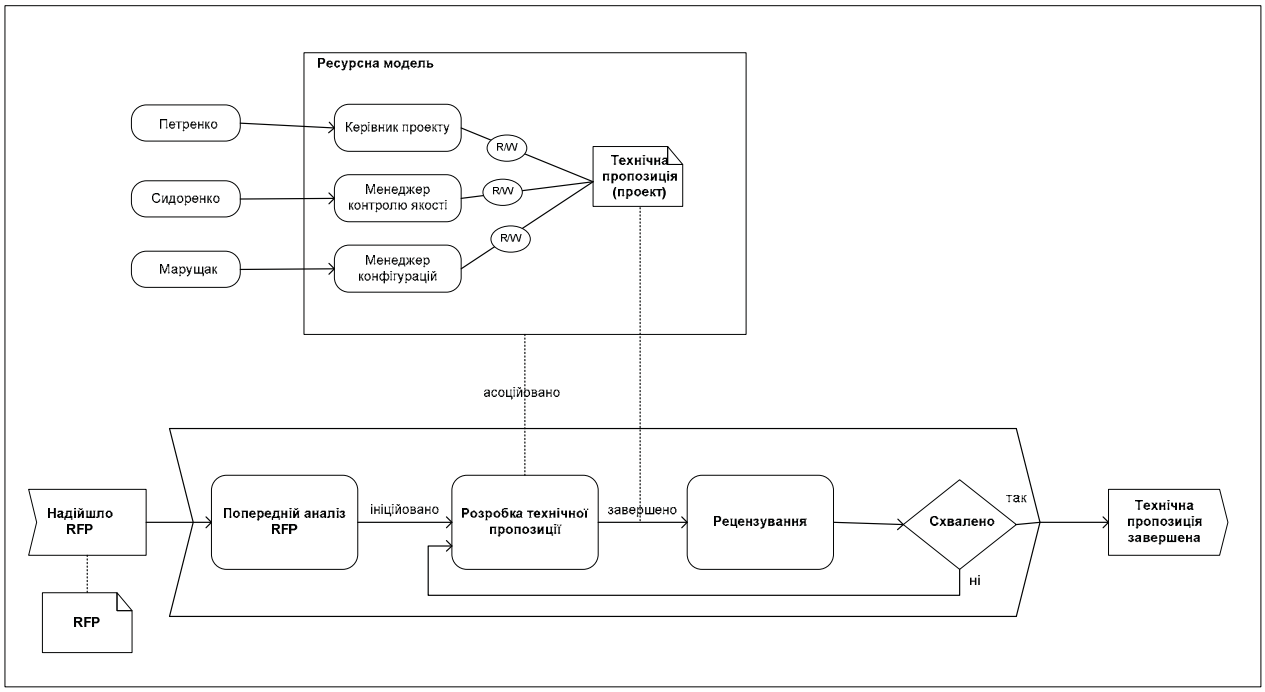

Рис. 3. Використання ресурсної моделі у процесі розроблення технічної пропозиції

В процесі розроблення технічної пропозиції створюється документ – "Технічна пропозиція", в якому визначаються складові частини, технології та спосіб розроблення, визначаються терміни, етапи та проміжні етапи розроблення, уточнюються функціональні можливості кінцевого продукту, визначаються додаткові обмеження та вартість розроблення.

Технічну пропозицію розробляє вузьке коло досвідчених фахівців під керівництвом керівника проекту. Як правило, у розробленні технічної пропозиції, крім керівник проекту, який відповідає за планування та технічну реалізацію, беруть участь керівник відділу контролю якості (QA), що відповідає за розроблення процесу контролю якості продукту на усіх етапах його розроблення. За необхідності, якщо продукт є достатньо складним технічно або вимагає тестування на багатьох апаратних та програмних платформах, до розроблення пропозиції також залучається експерт з керування конфігураціями (Configuration manager). Цей експерт планує процеси придбання додаткового обладнання, його встановлення та налаштування.

Порядок розроблення технічної пропозиції визначається корпоративними стандартами. Нехай розроблення пропозиції починається після схвалення RFP менеджером вищого рівня і формування проектної групи. Менеджер також асоціює працівників з ролями моделі. Початковий документ технічної пропозиції формується на основі шаблону та зберігається у репозиторії документів з керованим доступом, наприклад, VSS.

Під час формування документа учасники проектного колективу мають доступ до документа як щодо читання, так і щодо запису. Вони створюють окремі розділи документа, читають та висловлюють зауваження щодо інформації, доданої до документа іншими. Остаточну відповідальність за зміст та якість документа загалом несе керівник проекту. Коли документ сформовано, він надходить до рецензента. Одночасно з цим модель створення пропозиції перестає бути активною і усі учасники проектної групи позбавляються прав доступу. Рецензентом є менеджер вищого рівня. Він читає, але не змінює пропозицію, висловлює свої зауваження. Якщо проект

технічної пропозиції схвалив рецензент, то його відправляють замовнику. Якщо у документ потрібно внести зміни, його передають проектній групі на доопрацювання. При цьому модель етапу створення прозиції знову стає активною та усі учасники колективу знов отримують повний доступ до документа. Після цього процес повторюється доти, доки документ не буде схвалено або остаточно відхилено рецензентом.

Порівняно з методом керування доступом до ресурсів RBAC, запропонований метод має такі переваги:

- надані права доступу відповідають завданням, які виконує працівник у цей момент часу, та загалом – комплексу бізнес-процесів, які виконуються в організації;
- динамічний характер призначення та вилучення прав доступу;
- відсутність розширення прав доступу з часом;
- детальніший контроль доступу з використанням семантичних астракцій. Можливість побудови складних правил керуванням доступом з використанням властивостей бізнес-об'єктів, часових параметрів, усіх релевантних фактів бази знань;
- надає права доступу бізнес-працівник, уповноважений приймати управлінські рішення, а не системний адміністратор. Це спрощує процес виділення прав та вивільняє системних адміністраторів від рутинної роботи;
- надання прав доступу документується та зберігається навіть після того, як модель стає неактивною. Документом стає сама ресурсна модель. Це спрощує аудит системи;
- можливість повторного використання ресурсних моделей зменшує працемісткість присвоєння прав;
- створюється можливість стандартизації бізнес-процесів і окремих бізнес-операцій, а також відповідних ресурсних моделей та забезпечення дотримання стандартів працівниками;
- завдання виділення прав доступу вирішується одночасно і в комплексі із завданнями планування процесу виконання завдання, оцінки необхідної кількості та параметрів ресурсів;
- автоматичне присвоєння та вилучення прав щодо сформованої ресурсної моделі.

Недоліком є більша складність системи, необхідність попередньої реалізації системи моделювання бізнес-процесів з використанням бази знань.

Формальна специфікація ресурсної моделі

Формально ресурсна модель подається як кортеж

$$MdRes=(M(Rol),M(Res),M(LnRolRes))$$

де M(Rol) – це множина, всі елементи якої є об'єктами визначеного в онтології On класу Role:

$$M(Rol) = (Rol \mid Type(Rol) = Role)$$

аналогічно,

$$M(Res)=(Res|Type(Res)=Resource)$$

$$M(LnRolRes)=(LnRolRes|Type(LnRolRes)=LinkResourceRole)$$

Класи онтології, що відповідають ролям, в загальному випадку утворюють ієрархію класів. Для кожного класу ієрархії визначають правила та обмеження, що відповідають цьому класу та повинні бути дотримані для усіх похідних класів. Так, наприклад, можна визначити загальний клас Role та детальніший клас PMRole для опису ролі взагалі та ролі керівника проекту. В класі PMRole будуть відображені обмеження, дійсні для керівників проектів і незалежні від конкретної ресурсної моделі.

Своєю чергою, об'єкт Rol сам є класом, але визначеним і дійсним тільки у межах ресурсної моделі MdRes. В цьому сенсі можуть існувати різні екземпляри цих об'єктів у різних екземплярах MdRes. Як клас, Rol містить додаткові обмеження, сформульовані на рівні моделі MdRes

$$Rol=(M(SlRol),M(CsRol)),$$

де M(SlRol) = властивості (слоти) ролі; M(CsRol) – обмеження, визначені для ролі.

До найважливішої категорії обмежень CsRol належать обмеження на характеристики людей, яким дозволено виконувати роль Rol. Такими обмеженнями, наприклад, можуть бути вимоги щодо досвіду, стажу роботи, посади тощо.

Серед властивостей SlRol ролі визначають як властивості, успадковані від батьківських класів $M(SlRol)_{inh}$, так і властивості, визначені на рівні моделі $M(SlRol)_{md}$

$$M(SlRol)=M(SlRol)_{inh} \bigcup M(SlRol)_{md} .$$

Аналогічно, і обмеження ролі поділяються на успадковані обмеження та обмеження, визначені додатково, в межах моделі:

$$M(CsRol)=M(CsRol)_{inh} \bigcup M(CsRol)_{md} .$$

Класи онтології, що відповідають ресурсам, також утворюють ієрархію, та успадковують свої властивості від загального класу Бізнес-Ресурс. В онтологію керованих бізнес-ресурсів входять, наприклад, такі важливі типи ресурсів, як Документи та Сервіси.

Специфікація ресурсу містить множину властивостей M(SlRes), множину обмежень M(CsRes) та множину посилань на сервіси системи, які реалізують та обслуговують визначений у моделі тип ресурсу – M(SvRes).

$$Res=(M(SlRes), M(CsRes),M(SvRes)) .$$

Аналогічно до ролей, властивості, обмеження та множина посилань на сервіси успадковуються від батьківських класів онтології On.

Зв'зок між роллю та ресурсом LnRolRes задано на парі (Rol,Res).

$$LnRolRes=((Rol,Res), M(SlLnRolRes), M(CsLnRolRes)) ,$$

де M(SlLnRolRes) – множина параметрів зв'язку, M(CsLnRolRes) – множина обмежень.

Створення та використання ресурсних моделей

Опрацювання ресурсних моделей виконується на декількох стадіях – створення, ініціалізації, використання. Передумовою використання ресурсних моделей у системі є розроблення та впровадження системи моделювання бізнес-процесів та розроблення онтологій бізнес-об'єктів.

Створення ресурсних моделей

Ресурсні моделі створює бізнес-працівник або менеджер з конфігурацій, який глибоко розуміє як бізнес-процеси підприємства, так і ресурси, необхідні для виконання цих процесів.

Ресурсна модель багаторазового використання створюється у графічному редакторі – середовищі моделювання. Автор моделі визначає ролі, ресурси, та описує їх зв'язки. У визначену модель він вводить обмеження, які диктуються бізнес-правилами, або технічними причинами. Для основних компонент моделі визначаються діапазони допустимих типів значень. Спеціальна компонента середовища моделювання – валідатор – перевіряє обмеження, що існують в онтології, та вимагає їх дотримання. Закінчена модель валідується на відсутність двозначностей, невизначеностей. Закінчена та валідована модель зберігається у репозиторії моделей у вигляді xml- файла.

Ініціалізація ресурсної моделі

В процесі ініціалізації ресурсної моделі відбувається налаштування моделі-шаблона з репозиторію моделей, асоційованого з конкретною операцією бізнес-процесу.

Операцію ініціалізації виконує бізнес-працівник. В процесі цієї операції на основі готового шаблону моделі створюється екземпляр моделі, який асоціюється з визначеною бізнес-операцією. До екземпляру моделі додаються обмеження та параметри, важливі для реалізації цієї моделі у контексті бізнес-операції. Важливим завданням є конкретизація значень, заданих у шаблоні як діапазон (набір) можливих значень. Ініціалізована модель валідується і у разі позитивного результату є готовою для виконання.

Виконання ресурсної моделі

Ініціалізована ресурсна модель виконується автоматично. Сигналом для активізації ресурсної моделі є активізація асоційованої моделі бізнес-операції. Після активізації моделі компонент системи моделювання – інтерпретатор моделей-інтерпретує xml-файл опису ініціалізованої моделі і генерує команди керування сервісами керованих ресурсів, які і додають відповідні ACE до списку ACL ресурсу.

Сигналом для деактивізації ресурсної моделі є подія закінчення та деактивізації асоційованої бізнес-операції. У такому разі інтерпретатор моделей генерує команди, які вилучають права доступу, надані моделлю.

Мова подання ресурсної моделі

Для опису ресурсної моделі було розроблено формат подання даних на основі стандарту мови опису доступу до ресурсів XACML (Extensible access control language) [9]. Приклад частини XML-файлу ресурсної моделі для процесу розроблення технічної пропозиції наведено нижче.

```
<Model>
  <ModelMetadata>
        <ModelId> id </ModelId>
        <ModelType> ResourceAccessModel </ModelType>
        <OntologyURI> www.acme.org/ResourceOntology</OntologyURI>
        <ModelRepositoryURI>www.acme.org/ModelRepository</ModelRepositoryURI>
        <BusinessOperation Datatype="&xml;string" Name="BusinessOp"
OntologyType="business_operation">ProposalCreationURI</BusinessOperation>
  </ModelMetadata>
  <PolicySet PolicySetId= "PPS:projectmanager:role">
        <Role OntologyType="ProjectManagerRole">
              <AttributeValue Datatype="&xml;string"
Name="RoleName">ProjectManager</AttributeValue>
              <AttributeValue Datatype="&xml;string" Name="Instance"
OntologyType="person">Marushak</AttributeValue>
              <AttributeValue Datatype="&xml;string" Name="Constraint"
OntologyType="constraint">Constraint</AttributeValue>
        </Role>
        <Rule RuleId="Permission:to:write:and:read:proposal">
              <Target>
                    <Resources>
                          <Resource>
                                <AttributeValue Datatype="&xml;string"
Name="ResourceName" OntologyType="document">Proposal</AttributeValue>
                                <AttributeValue Datatype="&xml;string"
Name="Instance">DocumentURI</AttributeValue>
                                <AttributeValue Datatype="&xml;string" Name="Constraint"
OntologyType="constraint">Constraint</AttributeValue>
                          </Resource>
                    </Resources>
                    <Actions>
                          <Action>
                                <AttributeValue Datatype="&xml;string" Name="ActionName"
OntologyType="action">Write</AttributeValue>
                                <AttributeValue Datatype="&xml;string" Name="ActionName"
OntologyType="action">Read</AttributeValue>
                                <AttributeValue Datatype="&xml;string" Name="ServiceURI"
OntologyType="AccessControlService">ServiceURI</AttributeValue>
                                <AttributeValue Datatype="&xml;string" Name="Constraint"
OntologyType="constraint">Constraint</AttributeValue>
                          </Action>
                    </Actions>
              </Target>
        </Rule>
  </PolicySet>
  <PolicySet PolicySetId= "PPS:qamanager:role">
        .....
  </PolicySet>
</Model>
```

Опис моделі містить секції метаданих та секції опису політик доступу. В секції метаданих вказано загальні відомості про модель: ідентифікатор, посилання на онтологію, репозиторій моделей, бізнес-операцію, асоційовану з цією моделлю. У секціях політик доступу для кожної ролі встановлено ресурси, допустимі операції. Важливою частиною опису є посилання на відповідний тип онтології та визначення додаткових обмежень, що діють на рівні моделі.

Висновок

Розроблений метод доступу до ресурсів з використанням моделей дає змогу побудувати інформаційну систему, в якій права доступу присвоюються динамічно, в контексті виконання бізнес-завдань. При цьому задача адміструванння правами доступу істотно спрощується у разі підвищення рівня захисту системи.

1. The Need for a Process Mining Evaluation Framework in Research and Practice / Rozinat A., Karla Alves de Medeiros, Gunther C, and all.//Business Process Management Workshops. Hofstede A, Boualem Benatallah H Eds.-Springer-Verlag Berlin Heidelberg, 2008. – 502 p. 2. Александров А. BI 2.0: прообраз новой архитектуры бизнес-аналитики [Electronic resource] – Режим доступу: http:/www.osp.ru/os/2007/05/426080. – Назва з екрана. 3. Ferraiolo D. Role-Based Access Control / Ferraiolo D, Kuhn R, Chandramouli R. – Artech house inc, 2007. – 405 p. 4. Ferraiolo D. Proposed NIST Standard for Role-Based Access Control. /Ferraiolo D, Sandhu R, Gavrila S, and all // ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001. – P.24–274 5. Beyond Roles: A Practical Approach to Enterprise User Provisioning. [Electronic resource]. – Режим доступу: http://www.idsynch.com/docs/beyond-roles.html. – Назва з екрана. 6. Буров Є.В. Автоматизація проектування систем керування доступом у розподіленій інформаційній системі / Буров Є.В. // Вісник Нац. ун-ту "Львівська політехніка" "Інформаційні системи та мережі". – 2003. – № 489. – С.12–26. 7. Буров Є.В. Опрацювання знань у когнітивній інформаційній системі керованій моделями / Буров Є.В. // Східно-Європейський журнал передових технологій. – 2009. – № 6/7(42). – С. 40–49. 8. Буров Є.В. Інтелектуальна сиситема підтримки прийняття рішень у договірному процесі / Буров Є.В., Калінчук Ю.О., Ломтєв А.В. // Вісник Нац. ун-ту "Львівська політехніка" "Інформаційні системи та мережі". – 2009. – № 653. – С.24–31 9. Core and hierarchical role based access.control (RBAC) profile of XACML v2.0. OASIS Standard,1 February 2005. [Electronic resource]. – Режим доступу: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf. – Назва з екрана.