- сфера послуг Internet-страхування є сьогодні однією з перспективних і, водночас, недостатньо представленою на ринку не тільки України, а й багатьох розвинених країн;
- Internet-страхування забезпечує постійний, тісний та надійний зв'язок з клієнтом, а загалом – тривалу і взаємовигідну співпрацю;
- на відміну від інших Internet-послуг, Internet-страхування є специфічною галуззю, яка потребує застосування, поряд зі звичайними, інтелектуальних технологій опрацювання інформації та прийняття рішень;
- розв'язання багатьох задач та проблем взаємодії з клієнтами потребує не просто механічного підходу, а вирішень на рівні експертних та інтелектуальних систем [1];
- саме інтелектуальні технології, на думку авторів, гарантують ефективне просування систем Internet-страхування на ринку і забезпечать страховим компаніям стабільний прибуток за рахунок охоплення та утримання своєї частки клієнтів.

1. Берко А.Ю. Інформаційні моделі прийняття рішень в медичному страхуванні // Вісн. Нац. ун-ту "Львівська політехніка". – 2002. – № 464. – С. 3–11. 2. Базилевич В.Д., Базилевич К.С. Страхова справа. – К.: Т-во "Знання", КОО, 2002. 3. Пономаренко В.С. Інформаційні системи і технології в економіці. – К.: "Академія", 2002. 4. Информационные технологии в страховании http://www.rbc.ru/insurance/einsurance.html

УДК 681.3.06

Є.В. Буров
Національний університет "Львівська політехніка",
кафедра "Інформаційні системи та мережі"

АВТОМАТИЗАЦІЯ ПРОЕКТУВАННЯ СИСТЕМИ КЕРУВАННЯ ДОСТУПОМ У РОЗПОДІЛЕНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

This paper proposes formal specifications for correct and business-oriented access rights design in complex corporative information system.

Запропоновано формальні специфікації для проектування системи прав доступу в розподіленій інформаційній системі.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ

Інформаційна система (ІС) сьогодні стала однією з визначальних компонент в інфраструктурі будь-якого підприємства. Водночас ускладнення таких систем, швидкі та постійні зміни як в апаратній, так і в програмній, логічно-організаційній складовій значно утруднюють процеси керування та налаштування ІС. Наслідком цього є зростання вартості експлуатації ІС та негативні наслідки в роботі підприємства загалом.

ЗВ'ЯЗОК ВИСВІТЛЕНОЇ ПРОБЛЕМИ ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Визначальною тенденцією розвитку інформаційних систем сьогодення є поступовий перехід на новий рівень їх аналізу та проектування – рівень бізнес-процесів. Власне поняття бізнес-процесів покладено в основу головних стандартів, що визначають рівень якості роботи підприємства – ISO 9000, CMM та нового стандарту ISO/IEC 15504. Підхід до аналізу, проектування та керування інформаційною системою на рівні бізнес-процесів дозволяє оцінити якість функціювання такої системи безпосередньо у термінах бізнес-процесів, визначити вплив якості проектних, структурних, функціональних рішень та поточних налаштувань інформаційної системи як однієї з допоміжних підсистем підприємства на якість виконання головних бізнес-процесів.

Одним з шляхів вирішення вказаних проблем є побудова автоматизованих систем проектування та керування інформаційними системами. Такі системи, спираючись на комплекс формальних моделей ІС, широко застосовуючи засоби штучного інтелекту та експертні системи, дозволять покращити якість проектування ІС, гнучкіше та оперативніше реагувати на зміни.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ, В ЯКИХ ЗАПОЧАТКОВАНО РОЗВ'ЯЗАННЯ ДАНОЇ ПРОБЛЕМИ І НА ЯКІ СПИРАЄТЬСЯ АВТОР

У роботі [5] запропоновано систему формальних специфікацій для автоматизованого проектування та моделювання розподілених інформаційних систем. ІС в [5] описана трьома специфікаційними мережами, між якими встановлено відображення:

$$S = \{NPc, N\Pr, NPt, NDv\}$$

де NPc – мережа процесів, $N\Pr$ – мережа процесорів, NPt – мережа прототипів, NDv - мережа компонент. Процес проектування починають з визначення структури бізнес-процесів підприємства та виокремлення процесів, які відбуваються за участю інформаційної системи. Будують параметричні моделі окремих складових операцій мережі процесів.

На ранніх етапах проектування під процесом розуміють бізнес-процес – певну процедуру, зрозумілу замовнику. На подальших етапах проектування процес – це операція, яка супроводжується перетворенням інформації (матеріальних потоків, параметрів системи). Мережа процесів визначає послідовність операцій у системі, їх взаємозв'язок.

Мережа процесорів NPr є подальшим кроком у побудові специфікації системи. Специфікація ускладнюється за рахунок розкриття структури розподілених процесів, визначення та ідентифікації компонент багаторазового використання – системних сервісів, а також визначення та опису об'єктів-виконавців процесів (процесорів). На цьому етапі приймають загальноархітектурні вирішення.

На етапі побудови мережі прототипів NPt кожному процесору ставиться у відповідність певний прототип пристрою, програмного забезпечення або технічного вирішення. При цьому використовують прості експертні системи.

При побудові мережі компонент NDv для кожного прототипу визначають марки та моделі реальних пристроїв або компонент програмного забезпечення, виконують необхідні вимірювання та експерименти.

Після побудови усіх специфікаційних мереж стає можливими проектування окремих підсистем та вирішення прикладних задач з налаштування ІС.

Підсистема керування доступом (ПКД) – це одна з підсистем ІС. Вона встановлює відношення між об'єктами – користувачами та функціями і ресурсами ІС. Вона є динамічною структурою, зі значним темпом змін.

Структура КД накладається, існує та розробляється паралельно з усіма специфікаційними мережами РІС. Паралельно з ними вона й деталізується. Водночас, вона може розглядатися як окрема структура та використовуватися для розв'язання задач на етапах проектування і супроводу системи.

ВИДІЛЕННЯ НЕ ВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРІ РОЗГЛЯДАЮТЬСЯ У СТАТТІ

В існуючих системах проблема керування доступом вирішується, як правило, на нижніх, реалізаційних рівнях. Кожна операційна система, СУБД, інші аналогічні продукти пропонують власні механізми керування доступом. Незважаючи на наявність в таких системах концептуально подібних вирішень та механізмів, кожен з них має свою специфіку. У великих багатомашинних, гетерогенних мережах, які працюють з різними ОС, СУБД проблеми прозорого керування доступом великої кількості користувачів достатньо складні. Власне через ці проблеми великою є і вартість адміністрування таких комплексів.

Проблемою є також формулювання єдиної прозорої політики щодо прав доступу у гетерогенній мережі, а потім проведення її на рівні різних ОС, СУБД та інших застосувань, які керують доступом користувачів. Одним з можливих вирішень цієї проблеми є розробка засобів автоматизованого проектування, які дозволяють сформулювати політику доступу на високому рівні абстракції, і яка потім однозначно транслювалася в командні скрипти різних систем. При цьому необхідно сформулювати загальні правила, обов'язкові для всіх користувачів, що виконуються автоматично, без участі адміністратора.

Частковим вирішенням на шляху до спрощення керування є впорядкування мережевих об'єктів (користувачів, ресурсів, об'єднань користувачів,...) з використанням служб каталогів. Сьогодні відсутні засоби проектування системи прав доступу логічно вищого рівня, які працювали би з логічною моделлю бізнес-процесів та бізнес-функцій системи. Інтуїтивно зрозуміле оператору призначення права доступу у системі таких функцій транслювалося би автоматично в набори команд підсистеми адміністрування, які забезпечували би задане право доступу для всіх потрібних ОС та СУБД.

У сучасних операційних системах та СУБД адміністратор може багатьма способами призначити права доступу до інформаційного ресурсу. Структуру прав доступу рідко зберігають у вигляді прямих призначень. Для надання системі гнучкості структура справ доступу складається з багатьох правил (ACE) у певній базі даних прав доступу (ACL), які мають різний пріоритет. Зі списку правил вибираються ті, що належать до певного об'єкта, розташовуються у порядку пріоритетів, і за результуючим списком приймається рішення.

Правила мають найекономічніше, найточніше визначати права. Визначені такі механізми призначення прав.

- Пряме присвоєння

Пряме присвоєння права використовується в останню чергу. Це найбільш трудомісткий механізм присвоєння, водночас він гарантує надійне присвоєння права. Знищення цього права вимагатиме адресного втручання адміністратора.

Окрему групу правил становлять правила, дія яких є результатом співвідношення з певним об’єктом-посередником. Права надаються посереднику, а між об’єктом-користувачем та посередником задається відношення належності.

До таких правил належать:

- Членство у групі

Посередником Посередником тут є група користувачів, визначена за певною ознакою їх спільних властивостей.

- Займання посади

Посередником є об’єкт “посада” з чітко визначеними правами. Зручно проводити операції займання посади та звільнення з неї.

- Еквівалентність прав

Посередником є інший об’єкт-користувач. Це правило найбільш вразливе до непередбачуваних змін. При зміні прав основного користувача неявно модифікуються права і всіх інших користувачів, еквівалентних йому.

- Структурне наслідування

Структурне наслідування прав реалізується в ієрархічній структурі вкладених контейнерів (наприклад, організацій та підрозділів). Право, яке присвоюється об’єкту на рівні певного контейнера, автоматично поширюється на всі вкладені у контейнер об’єкти, в тому числі і на інші контейнери. Структурне наслідування – потужний механізм визначення прав.

- Атрибут

Атрибут дозволяє обмежити коло операцій без залежності від об’єкта, що вимагає доступу. Атрибут присвоюється безпосередньо об’єкту.

Крім механізмів присвоєння прав, існують і механізми їх явного обмеження.

Зазвичай правила заборони мають вищій пріоритет, ніж правила дозволу.

Обмеження прав

- Явна заборона

Вказується вид операцій, яка явно заборонена.

- Атрибут

Атрибут забороняє виконувати певну операцію з об’єктом та не залежить від об’єкта доступу.

- Фільтр наслідуваних прав

Обмежує права доступу, які наслідуються у ієрархічних структурах і є одним з механізмів обмеження, властивим для ієрархічних схем виділення прав.

- Бізнес-правило

Бізнес-правило – це чітко визначена функція визначення доступу до операції залежно від динамічних умов. Може бути потрібно додаткове звертання до інших баз даних. Бізнес-правила в сучасних ОС не застосовуються.

Сьогодні все більшої популярності набуває керування окремими компонентами ІС (наприклад, КМ [6]) на основі політик. Цей підхід можна розширити і на всю систему загалом. Політика безпеки – це сукупність загальних для організації правил. Сьогодні на рівні ІС така політика не має інструментальної підтримки. Вона існує у вигляді паперових документів, інструкцій для користувачів та адміністраторів. Система керування ІС не відслідковує дотримання політики.

При всій різноманітності механізмів призначення прав доступу , великій кількості об'єктів та суб'єктів доступу відсутні механізми роботи з цими правами на вищих рівнях абстракції. Зараз адміністратор тримає цю інформацію у пам'яті. Такі структури не документуються, а тим більше не опрацьовуються. Водночас підтримка відповідності прав доступу такій структурі дало б змогу прозоріше керувати правами доступу, легше знаходити помилки та вузькі місця, краще захистити систему. З іншого боку, не досліджений вплив структури операцій задачі на структуру прав доступу.

Як правило, в інформаційній системі вирішується багато задач та існує багато користувачів. Оптимальне керування правами користувачів в таких умовах непросте завдання, яке вимагає підтримки на рівні інструментальних засобів.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАДАЧІ)

Суттєво зменшити вартість адміністрування користувачів можна, якщо реалізувати підтримку задачі контролю системи прав доступу інструментальними засобами, інтегрувати задачу керування користувачами у загальну систему проектування РІС.

До системи керування правами доступу (ПД) висуваються такі вимоги:

- забезпечення мінімальної достатності прав доступу для вирішення задач системи;
- гнучкість;
- простота переналагодження, наочність;
- адміністрування доступом на основі системи загальних правил (політики);
- інтелектуальність, можливість динамічної зміни прав доступу на основі політики, без втручання адміністратора.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ З ПОВНИМ ОБҐРУНТУВАННЯМ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

Розглянемо об'єкти, інформаційні сутності та загальні поняття стосовно підсистеми керування доступом

Людина (фізична особа)

Конкретна фізична особа, яка однозначно ідентифікується біометричними засобами. Вона має історію роботи в організації, займає певну посаду, має інші характеристики, які зберігаються у БД відділу управління персоналом. Має вона й історію роботи з інформаційною системою, яка може вестися ІС (згідно з визначеною політикою). Людина не обов'язково є користувачем ІС. Але вона може працювати від імені декількох користувачів (мати декілька різних бюджетів для різних систем, що контролюють доступ, наприклад – для операційної системи та СУБД).

Користувач

Інформаційна сутність, яка відображає користувача системи. Це точка контакту людини з інформаційною системою. Як правило, якщо людина працює з інформаційною системою, вона має свого користувача. Водночас існують користувачі, за якими не закріплено конкретних людей (root, daemon, ...). Інколи користувач відображає не конкретну людину, а роль (наприклад, адміністратора системи, баз даних). Важливим є те, що всі операції у системі на базовому, нижньому рівні виконуються від імені конкретного користувача, що визначає результуючі права доступу до інформаційних ресурсів. Користувач є носієм прав доступу.

Механізми та об'єкти призначення прав доступу

На практиці дуже рідко права доступу присвоюють конкретному користувачу. Частіше використовують інші схеми та механізми, які відображають реальні прикладні процеси та залежності в системах. Вони дозволяють більш ефективно керувати доступом груп користувачів. Ці об'єкти є посередниками між користувачами та сукупностями прав доступу (СПД).

Отже, права присвоюють не користувачам, а об'єктам-посередникам. Об'єкти-посередники можуть залежати один від одного. Наприклад, для вкладених контейнерів виконується відношення успадкування. Залежності визначені типом посередника та моделюються його методами.

До об'єктів-посередників належать ролі, групи користувачів, посади, організаційні підрозділи.

Об'єкт-посередник діє від імені користувача і має тип користувача. Це ідеалізований, узагальнений користувач, який характеризується певними ознаками.

Об'єкти доступу

Об'єктами доступу є процеси та ресурси. Доступ до процесу передбачає дозвіл на виконання цього процесу (операції). Дозвіл на відповідні ресурси дублює дозвіл на процеси і має сенс тільки для відображення наявної тенденції, коли мережеві ресурси подаються у Службі каталогів (СК) і доступ визначається у формі операції над ресурсом. Крім того, це має сенс і при об'єктному відображенні ресурсів системи.

На етапі побудови мережі процесів діють тільки визначення прав доступу до певних операцій процесу. Таке процедурне визначення згодом, при деталізації процесу також деталізується. Процедурне визначення одночасно є і обґрунтуванням права доступу, яке дає змогу проаналізувати ці права на відсутність надлишковості.

На етапі побудови мережі сервісів формується об'єктне подання системи як сукупності сервісів (ресурсів та операцій з ними). У практиці сучасних ОС та СУБД лежить пряме присвоєння права доступу користувача до операції сервісу або типу сервісу. Зрозуміло, що в даному випадку відсутнє обґрунтування (часто воно інтуїтивне, залишається в пам'яті адміністратора), відсутнє також і відображення на попередні етапи проектування.

Для спрощення схеми можна визначати шаблони та загальні правила адміністрування. Наприклад:

- визначати узагальнений сервіс певного типу (файловий сервіс) з визначеними операціями і окремо – конкретні реалізації для конкретного посередника та каталогу.
- визначати загальні правила адміністрування, наприклад, кожен користувач повинен мати свій каталог –home з однаковою схемою прав доступу.

Сукупність прав доступу (СПД)

Сукупність прав доступу має різний вигляд для різних етапів проектування і різних специфікаційних моделей.

На етапі побудови мережі процесів сукупність прав доступу виглядає як таблиця Користувач (ініціатор, або виконавець) процесу – процес – додаткові обмеження. Треба розрізняти випадки, коли процес ініціюється користувачем, виконується з участю користувача та виконується автоматично від імені користувача. В процесі деталізації процесу деталізуються і права доступу. Більш загальні права доступу (наприклад, право

адміністратора, право виконання резервних копій) деталізуються та конкретизуються. Кожне загальне право визначається як сукупність детальніших прав на виконання операцій та доступу до сервісів.Тобто, специфікація прав доступу на цьому етапі пов'язана з конкретною специфікацією процесів та сервісів.

На рівні специфікації пристроїв специфікація прав доступу трансформується в узагальнену таблицю для кожного мережевого ресурсу. З цієї таблиці легко отримати ACL для кожної операційної системи. Кожен елемент ACL визначає операцію, об'єкт доступу, функцію доступу.

Відношення "користувач – посередник"

Відношення користувач – посередник визначає належність користувача до посередника. Посередник може виступати від імені користувача, а також відношення може містити параметричне бізнес-правило, яке обмежує відношення, і при певних умовах може розірвати його.

Відношення "посередник – СПД"

За своїм типом таке відношення є стабільнішим ніж відношення "користувач – посередник". Такий зв'язок встановлюється під час проектування алгоритму роботи системи або його модифікації. Деактивація такого відношення може блокувати виконання певних бізнес-процесів взагалі. Водночас воно може також містити бізнес-правило. Це передбачає "колективну", або посадову відповідальність користувачів. За набором параметрів таке відношення ідентичне зв'язку "користувач – посередник". Може бути і пряме відношення "користувач – СПД".

Подія

Подія є ключовим поняттям специфікації ПД. Підсистема моделювання та керування за подіями описана у [7]. Специфіковані події керують роботою автоматизованої системи адміністрування і дають змогу дотримуватися правил політики. До специфікованих подій визначаються методи, які реалізують певні бізнес-правила. Ці методи можуть бути записані в об'єктах-посередниках, користувачах та ін. З іншого боку, виконання процесу чи процедури також може генерувати подію. Планування та специфікація подій у системі – одна з головних задач налаштування та програмування системи керування доступом.

Політика доступу

Сукупність параметричних правил, які діють для об'єктів та суб'єктів керування доступом. Вона може динамічно присвоювати користувачу певні ролі (наприклад, "Новачка" або "Порушника правил", "Підозрілої особи" та ін.). Кожна роль має додаткові правила опрацювання. Наприклад, для "Підозрілої особи" можна включити аудит подій та вчинків.

Можна визначити декілька типів правил, які в сукупності складають політику доступу.

- Бізнес-правила, пов'язані з відношенням. Перевіряються кожного разу при ініціалізації процесу та спрацюванні зв'язку. Бізнес-правило може деактивізувати відношення між конкретним користувачем та процесом або представником користувача та процесом.
- Методів та процедур, пов'язаних з певними подіями. Такі бізнес-правила найбільш загальні. Вони дають змогу слідкувати за роботою системи та користувачів, автоматизувати реагування системи на визначені заздалегідь ситуації.

- Загальних правил, сформульованих для всіх користувачів мережі. Підтримка таких правил повинна бути забезпечена на рівні подій. Але може вирішуватися і задача з перевірки дотримання сукупності загальних правил з вказанням невідповідностей.

Отже, програмування політики дає змогу автоматизувати роботу адміністратора, зробити її більш оперативною, підвищити безпеку системи.

Процес

Кожен процес виконується від імені певного користувача. Користувач може ініціювати процес, а також бути джерелом та отримувачем потоку. Крім того, користувач може розглядатися і як ресурс, необхідний для реалізації процесу. Найчастіше замість користувача тут використовують його преставника-посередника (роль, группу, посаду, підрозділ). Якшо конкретний користувач ініціює процес, то просто перевіряється його відношення до посередника. Посередника використовують у специфікаціях.

Задачі етапу початкового аналізу

На етапі системного аналізу одночасно з визначенням бізнес-процесів системи доцільно визначити типових користувачів, які характеризуються однотипною професійною діяльністю. Для таких типових клієнтів визначаються відповідні ролі. Прикладом такої ролі є роль працівника бухгалтерії, розробника програмного забезпечення, адміністратора ресурсів мережі та ін.

Визначення типових ролей дозволяє:

а) зменшити розмірності задачі аналізу та проектування;

б) отримати дані для подальшої розробки та побудови профілів клієнтів, забезпечення якості обслуговування кожної категорії клієнтів;

в) налагодити мережу на потреби категорій клієнтів, визначити параметри обслуговуючих сервісів, проектувати мережі під потреби клієнтів;

г) отримати інформацію для подальшої розробки схеми прав доступу до інформаційних ресурсів та сервісів мережі.

Типізація клієнтів може проводитися

- апріорі при проектуванні системи на підставі аналізу технології роботи ролі або експертних оцінок;
- апостеріорі, в результаті аналізу діяльності клієнтів існуючої системи для уточнення параметрів функціонування мережі та профілів клієнтів. Як правило, такі оцінки будуються на основі статистичних даних, зібраних за достатньо великий проміжок часу.

Користувачі (або відповідні ролі) можуть бути ініціаторами процесів і ресурсами, необхідними для їх виконання. Коли користувач розглядається як ресурс, то його участь в організації процесу може не деталізуватися. Визначаються загальні концептуальні правила роботи різних категорій користувачів, які складають основу системної політики.

Задачі етапу аналізу та побудови мережі процесів

На етапі роботи з мережею процесів специфікація доступу деталізується паралельно з деталізацією мережі процесорів. Деталізують функції, процеси, визначаються права доступу до деталізованих функцій. Можна сказати, що загальніші, не завжди конкретні права доступу на цьому етапі конкретизуються. Кожний процес виконується від імені

певного користувача. Ім'я користувача є одним з параметрів процесу. Під час процесу можна звертатися до ресурсу мережі (даних, матеріальних об'єктів). У схемі проектування ми вказуємо не конкретного користувача, а його представника (група, роль, організація). Отже, формується ланцюжок "представник – процес – ресурс", який повинен мати право виконання. Визначення таких ланцюжків – одне з завдань проектування. На цьому етапі проектування користувачі як категорія об'єктів не використовуються, тільки їх представники.

Визначається участь представників у виконанні процесів: коли користувачі потрібні для виконання і коли процес виконується сам, від імені користувача.

Задачі специфікації мережі сервісів та процесорів

На цьому етапі поряд з подальшою деталізацією функціональної структури, побудовою агрегатів функцій визначають параметри та моделюють участь користувачів у процесі роботи системи. Паралельно зі зміною специфікації процесів (наприклад, визначенням сервісів та процесорів), відповідно модифікується і специфікація прав доступу, наприклад, замість зв'язку між користувачем та процесом визначається відношення між користувачем та однією з функцій сервісу, яка відображає цей процес.

Важливим завданням етапу є визначення параметрів взаємодії представника користувача та процесу. Ці параметри дають змогу проводити параметричний аналіз. Визначені попередньо параметри можуть уточнюватися в результаті вимірювань.

Подальший аналіз проводиться для кожної ролі окремо. Визначається схема звертання до процесів мережі. Вона будується на основі аналізу потреб професійної діяльності ролі. Визначається множина операцій ролі, числові параметри кожної операції. Наприклад, такими параметрами можуть бути частота виконання операції, часові обмеження щодо отримання відповіді, об'єм інформації, який передається та отримується в результаті операції. Кожна така елементарна операція – це взаємодія з певним сервісом мережі або "внутрішня" операція (без взаємодії з сервісом). Отже, аналізується технологічний процес певної ролі, будується схема технологічного процесу (процесів) з оцінкою параметрів проміжних операцій. При неможливості чи недоцільності побудови та аналізу схем технологічного процесу зв'язки між роллю та сервісом можуть бути визначені експертно. Параметри кожної операції доцільно поділити на групи згідно з розмірністю параметра (див. вектор параметрів у формальній специфікації). Приклади найвживаніших параметрів:

θ – частота виконання операції,

$\lambda_{вх}$ – обсяг інформації, що передається в запиті до сервісу (клієнт->сервіс);

$\lambda_{вих}$ – обсяг інформації, що передається у відповідь на запит (сервіс-> клієнт);

$\tau_{від}$ – обмеження щодо часу відповіді,

π – пріоритет (важливість) операції.

При початковому аналізі зв'язків між клієнтами та процесами можна визначити

- дозволені та недозволені операції;
- основні та другорядні операції;
- часті та епізодичні операції.

Після побудови схем технологічних процесів вони узагальнюються у схему звертання до сервісів мережі. Спочатку роль та сервіс з'єднує максимум один відношення (асоціація) з відповідним вектором параметрів.

$$\mathbf{l = \{l\alpha, kl, sl, lp, lc\},}$$

де **lα** – ідентифікатор відношення, **kl, sl** – ідентифікатори клієнта та сервіса, що зв'язані l, **lp** – вектор параметрів відношення, **lc** – коментар.

Якщо відношення узагальнює декілька операцій, то параметри кожного типу визначаються за параметрами складових операцій за правилами, окремими для кожного типу параметрів. Наприклад, для наведених вище параметрів можуть бути використані такі правила:

$$\theta` = \Sigma\, \theta_l;$$
$$\lambda`_{вх} = \Sigma\, \lambda_{вх};$$
$$\lambda`_{вих} = \Sigma\, \lambda_{вих};$$
$$\tau`_{від} = \min(\tau_{від});$$
$$\pi` = \max(\pi).$$

Після визначення параметрів можуть розв'язуватися задачі параметричного моделювання, визначення впливу користувачів на роботу системи, визначення вузьких місць у системі безпеки, впорядкування роботи користувачів. Окреме місце займають процеси, які вирішуються вручну (тобто процесором тут є користувач). Такі процеси наближені до процесів, в яких використовується ресурс – користувач.

Задачі специфікації мережі прототипів

На цьому етапі аналізують сукупність визначених представників-користувачів на повноту, несуперечливість, відсутність дублювання. Система мінімізується та нормалізується. Правилом є один представник – один процес. Відношення "один до багатьох" та "багато до одного" неприпустимі. Якщо змінюється схема прав доступу, то змінюються і параметри. Політики досліджують на несуперечливість, коректність.

Задачі етапу мережі пристроїв та експлуатації системи

На етапі аналізу мережі пристроїв розглядають реальних користувачів та співвідносять їх з представниками. Вирішується задача повного та мінімального призначення прав користувачу.

Отже, задачами цього етапу є визначення прав користувача та позбавлення його надлишкових прав. Якщо схема представників добре спроектована, то достатньо розірвати одне відношення з відповідним представником.

На цьому ж етапі досліджують профілі користувачів, вимірюють їх параметри, оновлюють параметричну складову специфікації, адаптують роботу системи до зміни профілю, визначають сценарії керування системою, пов'язані з користувачами. На цьому етапі працюють з людьми-користувачами, ідентифікованими біометрично.

Системні політики реалізують у системі та відслідковують коректність роботи, у разі потреби – модифікують.

Визначимо формальні специфікації для підсистеми керування доступом.

Фізична особа

Для коректного адміністрування ІС відслідковувати інформацію за категорією "користувач" буває недостатньо. Точніше та адекватніше працювати з категорією "фізична особа". Крім того, ця категорія пов'язана з категорією "працівник" та інформацією про нього з БД відділу керування персоналом.

Фізична особа Ps:

$$Ps = \{idPs, M(idUs), PbPs, CmPs\},$$

де idPs – ідентифікатор особи, M(idUs) – множина ідентифікаторів користувачів, з якими може працювати особа, PbPs – блок параметрів, CmPs – коментар.

Користувач

Користувач є логічним об'єктом, який відображає фізичну особу для адміністративної підсистеми ІС. Користувач Us

$$Us = \{idUs, PbUs, CmUs\},$$

де idUs – ідентифікатор користувача, PbUs – блок параметрів, CmUs – коментар.

Об'єкти-посередники

Для призначення прав доступу на практиці часто використовують об'єкти-посередники. Кожен з цих об'єктів відображає один з механізмів керування доступом, який відповідає реальній практичній задачі. Приклади об'єктів- посередників: групи, посади, організаційні об'єкти – контейнери. Адміністратором системи можуть визначатися й інші посередники (наприклад, робочі групи, особи, що мають допуск до секретної інформації та працюють над певним проектом та ін.) Виходячи з цього, недоцільно визначати типи посередників на рівні метаданих. Це – інструментальні дані проектування.

Об'єкт-посередник пов'язаний, з одного боку, з користувачем, а з іншого – з об'єктом доступу та визначеною конфігурацією прав доступу. Як правило, відношення з об'єктом доступу є тривалішим та формується під час визначення порядку роботи системи. Відношення посередника з користувачем є менш тривалим і може перериватися без впливу на працездатність системи. Крім того, найчастіше з одним посередником пов'язано багато користувачів.

Посередник Br

$$Br = \{idBr, TyBr, PbBr, CmBr\},$$

де idBr – ідентифікатор посередника, TyBr – ідентифікатор типу посередника, PbPr – блок параметрів, CmBr – коментар.

Тип посередника попередньо реєструється в репозиторії проектування. Він визначає зміст блоку параметрів. Між об'єктами певних типів можуть бути залежності. Наприклад, вкладені в контейнери об'єкти успадковують права доступу від контейнера. Такі залежності реалізуються відповідними методами, які розміщені у блоці параметрів та запускаються як реакція на певну подію (наприклад, створення об'єкта, або модифікація прав доступу).

Адміністратор системи може

- створювати свої об'єкти-посередники
- задавати правила класифікації користувачів, згідно з якими встановлюються зв'язки з посередниками.

Відношення

Відношення користувач – посередник та посередник – СПД відображають залежність між сполучуваними об'єктами. Їх формальне визначення подібне.

Відношення між користувачем та посередником.

$$LnUb = \{idLnUb, idUs, idBr, [FnLnUb,] PbLnUb, CmLnUb\},$$

де IdLnUb – ідентифікатор відношення, idUs , idBr – ідентифікатори сполучуваних об'єктів, PbLnUb – блок параметрів, FnLnUb – параметрична функція керування відношенням, CmLnUb – коментар.

Блок параметрів містить поточні параметри зв'язку. Фактично – це пам'ять зв'язку, яка може відображати передісторію, історію поведінки користувача. Серед всіх параметрів є один (AtPr), який набуває булевого значення і служить для активізації/деактивізації зв'язку.

Необов'язкова параметрична функція керування зв'язком визначає активність зв'язку залежно від параметрів ІС. Фактично – це бізнес-правило, за яким за деяких умов відношення деактивізується.

Отже,

$$\mathrm{ZnAtPr} = \mathrm{FnLnUb}\,.$$

Відношення між посередником та процесом визначається аналогічно.

$$\mathrm{LnBp} = \{\mathrm{idLnBp},\ \mathrm{idBr},\ \mathrm{idPc},\ [\mathrm{FnLnBp},]\ \mathrm{PbLnBp},\ \mathrm{CmLnBp}\}\,.$$

Аналогічно визначається і відношення між користувачем та процесом.

Сукупність прав доступу

Сукупність прав доступу – це таблиця, яка може бути (це необов'язково) доповненням до певної специфікації (процесу або його деталізації). Право доступу для посередника встановлюється тоді, коли, виходячи зі специфікації або деталізації процесу, його участь необхідна для ініціалізації або виконання процесу.

СПД може бути безпосередньо отримана зі специфікації процесу, об'єктів користувачів, посередників та їхніх зв'язків. Іншим шляхом побудови СПД є її безпосереднє завдання у вигляді таблиці без прив'язки до специфікації процесу.

Тобто для окремого процесу право доступу фіксує наявність відношення між процесом та посередником, яке цей процес ініціалізує або виконує.

$$\mathrm{Ar} = \{\mathrm{idAr},\ \mathrm{idPc},\ \mathrm{LnOb},\ [\mathrm{DtAr},]\ \mathrm{PbAr},\ \mathrm{CmAr}\}\,,$$

де idAr – ідентифікатор СПД, idPc – ід. процесу, LnOb набуває значення з множини типів {idBp, idUp} , DtAr – деталізація СПД, PbAr – блок параметрів, CmAr – коментар.

Функціонально СПД повністю визначається процесом, на який вона вказує. Решта інформації відображає додаткові характеристики СПД.

Деталізація DtAr – це множина вказівників на СПД для процесів нижчих ієрархічних рівнів. Це трансляція узагальненого права доступу у скупність детальніших, дрібніших прав.

$$\mathrm{DtAr} = \{\mathrm{idAr}\}\,,$$

$$\forall\ \mathrm{idPc}' \in \mathrm{DtAr}\ (\mathrm{idPc}' \in \mathrm{DtPc}) \wedge (\mathrm{idPc} \in \mathrm{Ar})\,.$$

З використанням специфікації процесу або послідовності деталізації процесу можна вирішити задачу доведення мінімальної достатності прав доступу для кожного посередника.

Вирішення задач проектування має поступовий характер. Специфікація керування доступом на кожному наступному етапі проектування деталізується. Задачі проектування СПД доповнюють задачі розробки інших специфікацій та безпосередньо залежать від них.

Задачі етапу побудови мережі процесів

На етапі розробки концепції системи та системного аналізу

- визначають ролі користувачів системи та закріплені за ними функції. Ролі та функції відображають у таблицях;
- визначають (неформально) загальні правила надання доступу до ресурсів, що діють для всієї системи, фіксують ці правила у вигляді документа;
- визначають та розділяють операції, які виконуються вручну, автоматично або в результаті людино-машинної взаємодії;
- попередньо та експертно визначають параметри трудомісткості, обсягів робіт тощо.

Результатом є таблиці “Ролі – функції”, які можуть бути використані, наприклад, для побудови штатного розкладу. Як правило, ролі в них відповідають об’єктам-посередникам у наступних специфікаціях, а функції – процесам вищих рівнів деталізації. Таблиці використовують для створення початкових специфікацій процесів.

Під час розбудови специфікацій мережі процесів паралельно розбудовуються і специфікації доступу. При цьому виконують два типа операцій:

- деталізація функцій для визначених посередників;
- визначення функцій для посередників – ресурсів.

Для посередників, які є ініціаторами процесу, таблиця доступу добудовується операціями деталізації, які виконуються від імені цього посередника. Будується відповідність AR – > DtAr . При цьому дотримуються вимоги мінімальності – деталізація прав доступу повинна бути достатньою і не вводити надлишковості прав.

В деяких випадках під час операції деталізації посередники, які відображалися на діаграмі у вигляді ресурсів (тобто їх вплив детально, на рівні структури процесу, не визначався), стають ініціаторами для складових процесів деталізації. При цьому визначають процеси, що виконуються від іх імені.

На етапі побудови специфікації процесів конкретизують і політику доступу. Ця політика реалізується на рівні мереж процесів та описується логічними структурами.

Задачі етапу мережі сервісів та процесорів

На етапі побудови мережі сервісів та процесів специфікація контролю доступу відображає зміни логічної специфікації сервісів. Так, при створенні нового сервісу та агрегуванні в нього функцій зв’язки доступу спрямовуються до цих функцій сервісу. Для кожного створеного сервісу визначають перелік посередників які мають доступ до нього та функцій, які вони виконують.

- Задачі, пов’язані з сервісами

Аналогічно до попереднього етапу тут також вирішують задачі деталізації доступу та структури доступу.

- Задачі деталізації та визначення структури доступу

Інколи окремо розглядають важливі транзакції та аналізують їх на предмет обмеження доступу користувачів, більш захищеного проходження транзакції, визначення та мінімізації кола осіб, які впливають на транзакцію.

- Задачі логічного аналізу транзакцій

У випадку, коли якийсь посередник виконує складний набір взаємопов’язаних функцій, може вирішуватися задача дослідження функціонування цього представника як процесора. Визначають порядок виконання окремих операцій, їхні пріоритети, політику виконання функцій. Результатом вирішення задачі може бути посадова інструкція. Моделюється виконання функцій залежно від параметрів та вплив параметрів цього виконання на інші процеси.

Задачі етапу прототипів

На етапі побудови мережі прототипів приймають архітектурні рішення та обирають прототипі для процесорів. Логічна та структура параметричної частини специфікації на цьому етапі сформована, що дає змогу оцінювати закінчену специфікацію загалом.

Для системи контролю доступу тут вирішують такі задачі:

- аналіз визначеної системи прав доступу, його верифікація. Доведення його достатності, мінімальності (відсутності надлишковості), коректності (відсутності протиріч, операцій, які не виконуються ніколи через відсутність прав доступу та ін.).

- врахування впливу обраних архітектурних вирішень та прототипів на СПД. Деякі архітектурні вирішення та прототипи (особливо у сфері безпеки даних) можуть вплинути на структуру зв'язків між представниками та процесами, запровадити нові процеси, ввести додаткові обмеження, змінити політику.
- комплекс задач параметричного моделювання. Завданнями параметричного моделювання є дослідити вплив користувачів на виконання БП, знайти вузькі місця, спростити специфікацію за рахунок виключення або автоматизації ручної роботи, проаналізувати та оцінити доцільність будь-яких змін у системі, частину операцій якої виконують люди.
- дослідження політик на несуперечливість та коректність.

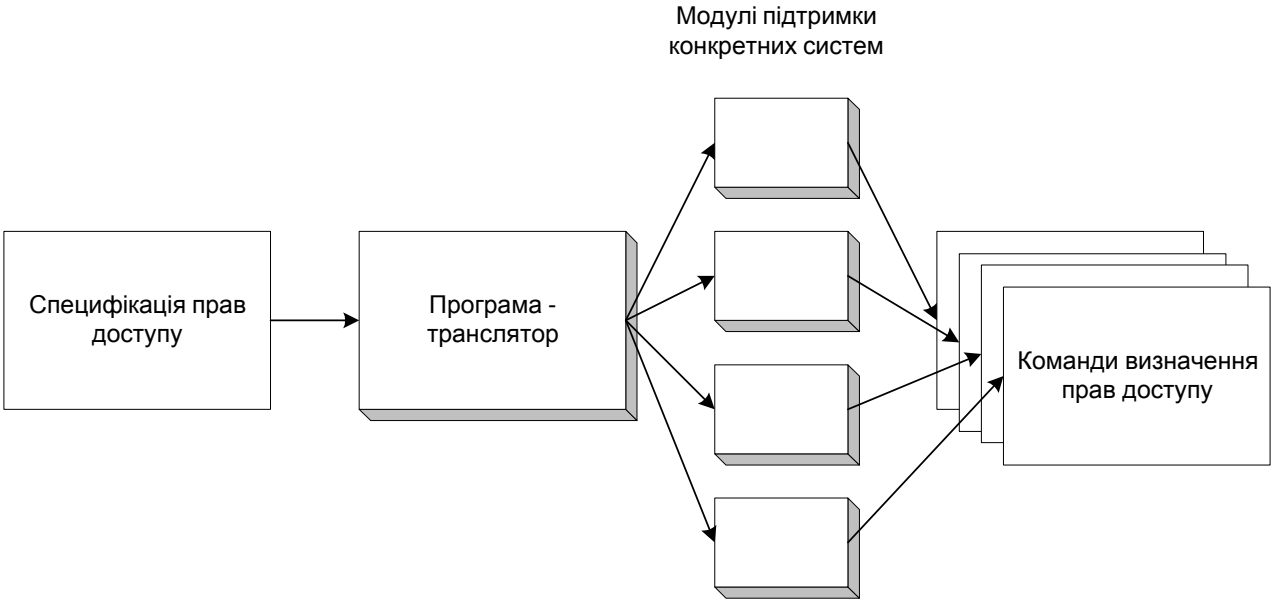
Задачі етапу мережі пристроїв.

На етапі мережі пристроїв працюють з об'єктами-користувачами та фізичними особами. Тут розв'язують такі задачі:

- встановлення зв'язків між об'єктами-користувачами та посередниками, керування цими зв'язками;
- відображення специфікації доступу на мові керування конкретних ОС та СУБД. Для розв'язання цієї задачі потрібно спроектувати програму- транслятор, яка, сприймаючи специфікацію доступу на вході, генерує скрипт командної мови, специфічний для обраної ОС.

Програма-транслятор (рисунок) повинна працювати як в пакетному режимі (коли генерують скрипти для системи специфікацій взагалі), так і в оперативному режимі, коли зміна специфікації доступу однозначно транслюється в команди зміни СПД визначеної ОС.

- проведення в життя системної політики, аналіз та корекція системної політики.



Структурна схема генерації команд для зміни прав доступу

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМКУ

Формальні специфікації для проектування системи прав доступу в розподіленій інформаційній системі будуть корисними і для аналізу процесу функціювання системи, внесення змін. Вони виступають складовою частиною системи специфікацій для проектування розподілених інформаційних систем.

1. Козак Н. Сертификация по ISO 9000 : 2000 года как способ оптимизации управления предприятием // Управление компанией. № 3 март 2001. http://www.management.com.ua/qm/qm007.html 2. Міжнародні стандарти якості ISO 9000. http://www.rmpu.com.ua/index.php?pub=4 3. Марк С.Паулк. Насколько стандарт ISO 9001 сопоставим с CMM ? http://www.management.com.ua/qm/qm027.htm 4. ISO/IEC 15504 – An Emerging Standard on Software Process Assessment. http://www.sei.cmu.edu/iso-15504/ 5. Буров Є.В. Система формальних специфікацій для проектування розподілених інформаційних систем // Вісн. Держ. ун-ту "Львівська політехніка". – 2000. – № 406. – С. 50–59. 6. Elizabeth Clark. The Mechanics of Policy-Based Management. Network Magazine, March 2000. 7. Буров Є.В. Система формальних специфікацій моделювання подій для САПР розподілених інформаційних систем // Вісн. Держ. ун-ту "Львівська політехніка". – 2000. – № 413. – С. 47–51.

УДК 51.001.57+371.214

О.М. Верес
Національний університет "Львівська політехніка",
кафедра "Інформаційні системи та мережі"

МЕТОДИ РОЗПОДІЛУ РЕСУРСІВ СЛАБКОСТРУКТУРОВАНОЇ ЗАДАЧІ УКЛАДАННЯ РОЗКЛАДУ

Methods and algorithms of allocation of basic resources of semistructured task of forming of curriculum of lessons are resulted. In the article the process of forming of semester curricula and algorithm of organization of primary informative base is described.

Наведено методи та алгоритми розподілу основних ресурсів слабкоструктурованої задачі формування розкладу навчальних занять. У статті описано процес формування семестрових навчальних планів та алгоритм упорядкування первинної інформаційної бази.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ

На початку нового тисячоліття швидкий розвиток і поширення сучасних інформаційних технологій в усі види суспільної діяльності робить перехід до автоматизації адміністративного життя вищого навчального закладу нагальною потребою. Метою створення автоматизованої системи керування вищим навчальним закладом є своєчасне отримання достовірної та повної інформації про контингент навчального закладу та