УДК 004.89

Буров Є. В.

КЕРУВАННЯ ДОСТУПОМ ДО РЕСУРСІВ ІНТЕЛЕКТУАЛЬНОГО ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ ОНТОЛОГІЧНИХ МОДЕЛЕЙ

Запропоновано підхід до використання онтологічних моделей для керування доступом до ресурсів. Порівняно з відомим методами RBAC та ABAC 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, онтологічна модель, моделювання бізнес-процесів, інтелектуальна система, інтелектуальне підприємство.*

1. Introduction

The growing complexity of information systems, constantly changing business environment requires adaptation of information system to those changes. One of the increasingly popular approaches to build flexible information enterprise systems is to use knowledge handling technologies, resulting in creation of intelligent enterprise [1]. An important part of adaptation processes is the continuous adjustment of access policies to business processes and environment changes.

2. Related work analysis and problem statement

Today's popular and largely used access control models are discretionary (DAC), mandatory (MAC) and role-based (RBAC). With DAC it is difficult to manage a large number of resources, it is impossible to determine and maintain complex policies [2]. MAC is widely used in systems where there is a need to control access to sensitive documents and the number of levels of secrecy is relatively small. For use in industrial systems labeled access abstraction is not flexible enough [2].

In the method of access control that uses roles (RBAC) each role is assigned to a set of access rights to resources. Users get rights by association with certain roles.

The practice of using RBAC systems also revealed their numerous flaws [3–5]:

— in large organizations access rights depend on tasks performed by users and require a constant update as tasks change;

— roles management naturally had to be performed by business professionals, which are assigning the tasks for users. However, role's and permission's correction requires substantial technical knowledge which business professionals usually don't have;

— with the passage of time the user's access rights usually expand. The reverse process of access rights removal in practice is performed with substantial delay.

In order to remove RBAC shortcomings several new access models were proposed. In ABAC access rights to resources are associated with a set of rules (policy) expressed through measurable attributes [4, 6]. Therefore, ABAC provides a precise and fine-grained access control when compared to RBAC.

In [4] ABAC method shortcomings in managing permissions across domains are highlighted and new authorization-based access control model (ZBAC) is presented. ZBAC proposes to authorize subject only in parent domain. Inter-domain authorizations are done based on inter-domain agreements.

Authors of papers [5, 7] proposed to change core access model to cover obligation, conditions, continuity, and mutability. The new model was named UCON (user control).

In [8] an extension to RBAC model was developed taking in consideration context. Sandhu in [5, 7] redefined basic control model creating ABC model, where context information is included in conditions.

In a complex Internet-like open systems, which are crossing and integrating several domains, the usage of RBAC or ABAC leads to inconsistencies and access errors. Thus, common specification is needed which describes formally the meaning of commonly used roles and attributes. The [4, 9] proposes to use an ontology as such a common specification.

In [10] task-based access control model (TBAC) is proposed. Authors argue that TBAC is aimed to provide for integrity of enterprise information system, not only for data integrity as other models.

The common flaw of existing access control models is that rules, roles and policies are often created at need without the systematic approach to enterprise security. As a result, the created set of roles and rules is hard to manage, it lacks of internal consistency. As a result overall security level of system will deteriorate.

The ultimate reason for access permission granting is provided by business processes. In our opinion the integrity of enterprise security could be provided if access rules and roles are associated with enterprise business processes and permissions are dynamically granted and revoked in context of business operations which are being executed. Taking in consideration, that business processes often are highly repetitive, they can be formalized in form of models with access management operations associated with typical business operations.

In this paper we are exploring the approach to access rights management using executable ontological business process models, analyzing the advantages of such approach, and developing access control models presentation language.

3. System architecture

Model-based access takes place in an intellectual enterprise system where business processes are modeled using ontology. The ontology has a central position in system, because it formulates concepts, attributes and relations used in intellectual system. Information base contains facts which are initialized exemplars of ontology types with specified attribute values. Ontology semantically interprets facts giving them the meaning.

Models are formulated using concepts defined in common ontology. Ontological models are in fact templates which contain the set of roles, relations, operations and constraints. Those templates can be initialized by facts. In this way fact-models are created. Fact-models describe real business processes and operations and have references to facts of different ontological types.

4. Access control model structure and processing

An important subset of ontological models is the normative models describing and enforcing business rules, corporate standards. Access control models belong to this subset. They are associated with business-operation events and relate the employees performing business operation.

Access control model defines user roles and resources needed for performing some typical task. As resources we use ontology concepts, representing business abstractions understood by business worker. The facts, derived from those concepts are used as security objects.

Before the execution of associated business-operation manager assigns specific employees to specific roles. When model execution starts, associated employees obtain access permissions. When business operation is completed, corresponding model also completes and granted permissions are revoked.

Let us illustrate the process of creation and using access control model on example of software proposal development (Fig. 1). The process starts when RFP (Request for proposal) document is received. RFP document is analyzed first by a top manager, and if it is acceptable, a team is created for the development of proposal. In process of initial evaluation top manager has read-only access to RFP document (fact-model A).

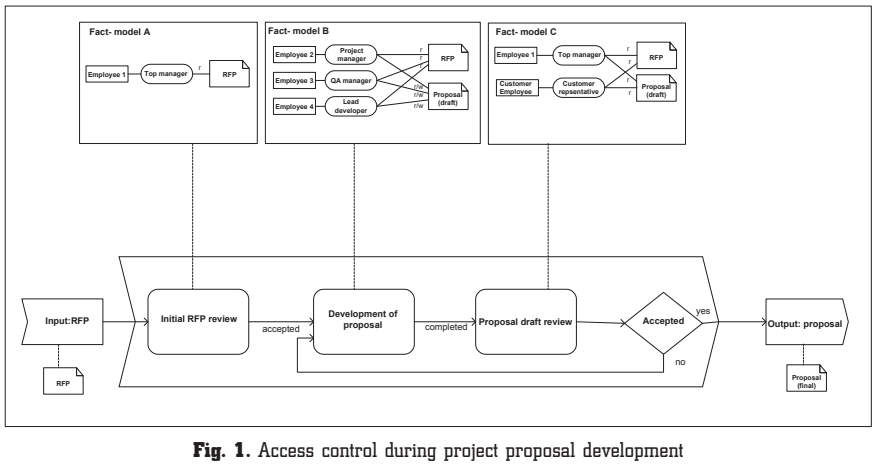

Fig. 1. Access control during project proposal development

A model for proposal development operation has specified roles and in corresponding fact-model real employees are assigned to those roles. Every team member has full (read/write) access to proposal document and read-only access to RFP document (model B). When final draft of proposal is completed, team members lose access to this document, which is forwarded for review by top-manager and customer representative. Both reviewers have read-only access to proposal and RFP (model C). If there are no corrections when review process is completed, proposal gets accepted. Otherwise, corrections are forwarded to proposal development team for proposal update. During update model B becomes active again and team members get access to proposal in order to create next draft. After this the process repeats until proposal is accepted or rejected.

When compared to currently used ABAC or RBAC proposed model-based access control has following advantages:

— access rights which are granted in any time moment correspond to business processes being executed;
— granting and revoking access rights are done dynamically;
— access control model is created and access is granted by business-worker;
— all operations with access rights are documented and archived;
— access control models are reused;
— business standards are enforced.

The language for access control model representation based on XACML was developed.

5. Conclusions

Proposed model-based access control approach allow build an information system where access rights are assigned dynamically in context with currently executed business processes and operations. The tasks of access control administration are simplified and form a part of general project management process.

Литература

1. Quinn, J. The intelligent enterprise a new paradigm [Text] / J. Quinn // Academy of Management Executive. — 2005. — Vol. 19, no. 4. — P. 109—121.
2. Ferraiolo, D. Role-based access control [Text] / D. Ferraiolo, D. R. Kuhn, R. Chandramouli. — Artech House Publishers, 1992. — P. 405.
3. Beyond Roles: A Practical Approach to Enterprise User Provisioning [Electronic resource]. — Available at: \www/ URL: http://www.idsynch.com/docs/beyond-roles.html. — 10 January 2014. — Title from the screen.
4. Karp, A. From ABAC to ZBAC : The Evolution of Access Control Models [Text] / A. Karp, H. Haury, M. Davis // Control. — April 2009. — P. 22—30.
5. Sandhu, R. Usage Control : A Vision for Next Generation Access Control [Text] / R. Sandhu, J. Park // Control. — 2003. — Vol. 2776. — P. 17—31.
6. Zhu, J. Attribute Based Access Control and Security for Collaboration environments [Text] / J. Zhu // Proc. W. W. Aerospace and Electronics conference NAECON 2008. — P. 31—35.

7. Park, J. Towards usage control models: beyond traditional access control [Text] / J. Park, R. Sandhu // Proceedings of the seventh ACM symposium on Access control models and technologies SACMAT 02. — 2002. — P. 57—64.
8. Kulkarni, D. Context-aware role-based access control in pervasive computing systems [Text] / D. Kulkarni, A. Tripathi // Proc. 13th ACM Symp. Access Control Model. Technol. SACMAT 08. — 2008. — P. 113.
9. Priebe, T. Supporting Attribute-based Access Control in Authorization and Authentication Infrastructures with Ontologies [Text] / T. Priebe, W. Dobmeier, C. Schläger, N. Kamprath // J. Software. — 2007. — Vol. 2, no. 1. — P. 27—38.
10. Thomas, R. K. Conceptual Foundations for a Model of Task-based Authorizations [Text] / R. K. Thomas, R. S. Sandhu // Proceedings of the 7th IEEE Computer Security Foundations Workshop. — 1994. — Vol. 39, no. 1. — P. 66—79.

УПРАВЛЕНИЕ ДОСТУПОМ К РЕСУРСАМ ИНТЕЛЛЕКТУАЛЬНОГО ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ ОНТОЛОГИЧЕСКИХ МОДЕЛЕЙ

Предложено подход для управления доступом к ресурсам интеллектуального предприятия, который использует онтологические модели. По сравнению с известными методами RBAC и ABAC, предложенный метод создает возможность динамического, документированного присвоения и изъятия прав доступа к ресурсам в контексте бизнес-процессов, которые выполняются в системе.

Ключевые слова: управление доступом, онтологическая модель, моделирование бизнес-процессов, интеллектуальная система, интеллектуальное предприятие.

Буров Євген Вікторович, *кандидат технічних наук, доцент, професор кафедри інформаційних систем та мереж, Національний університет «Львівська політехніка», Україна,*
e-mail: eugeneburov01@gmail.com*.*

Буров Евгений Викторович, *кандидат технических наук, доцент, профессор кафедры информационных систем и сетей, Национальный университет «Львовская политехника», Украина.*

Burov Yevhen, *National University «Lviv Polytechnic», Ukraine,*
e-mail: eugeneburov01@gmail.com

УДК 378.14+004.4

Литвинов А. Л.

АКТИВНЫЕ МЕТОДЫ ОБУЧЕНИЯ В СИСТЕМЕ КОМПЬЮТЕРНОЙ МАТЕМАТИКИ MAPLE

Представлены результаты использования системы компьютерной математики Maple для контроля знаний, объяснения задач запредельной сложности и создания виртуальных лабораторий. Используемые на разных этапах обучения, эти методы показали эффективность системы Maple, как необходимого элемента учебного процесса, использование которого позволяет повысить его эффективность.

Ключевые слова: *Maple, контроль знаний, криптография, секретный ключ, простое число, виртуальная лаборатория, эффект Гиббса, процесс.*

1. Введение

Системы компьютерной математики Mathcad, Matlab, Maple заняли прочное место при проведении научных расчетов, в анализе экспериментальных данных [1]. Особое место среди них занимает система Maple, ориентированная как на символьные, так и численные вычисления [2, 3]. В настоящее время в учебном процессе система Maple в основном используется как естественная замена системам программирования за счет огромного числа встроенных функций и процедур [4, 5]. В тоже время возможности системы Maple выходят за рамки традиционных подходов и позволяют ее использовать как активное средство обучения, позволяющее повысить качество обучения.

2. Контроль знаний с помощью системы Maple

Преподаватели тратят массу времени на составление и проверку студенческих домашних заданий. Использование системы Maple позволяет существенно снизить их нагрузку. Рассмотрим следующую задачу финансовой математики.

Создан фонд стоимостью P грн. Спустя n_1 лет его стоимость составила $S(n_1)$ грн, а спустя n_2 лет его стоимость составила $S(n_2)$ грн. Определить стоимость фонда спустя n_3 лет, если его наращение осуществляется по непрерывной ставке с силой роста, изменяющейся по линейному закону $\delta(t)=\delta_0+at$. Наращенная сумма вычисляется по формуле [6]:

$$S(n)=P\cdot\exp\left(\delta_0 n+\frac{an^2}{2}\right). \quad (1)$$

Подставив в выражение (1) данные, соответствующие времени n_1 и n_2, после соответствующих преобразований, получим систему линейных уравнений второго порядка относительно δ_0 и a:

$$n_1\delta_0+\frac{n_1^2}{2}a=\ln\left(\frac{S(n_1)}{2}\right),\ n_2\delta_0+\frac{n_2^2}{2}a=\ln\left(\frac{S(n_2)}{2}\right). \quad (2)$$

Решив систему уравнений (2) относительно δ_0 и a матричным способом, можно найти стоимость фонда в момент n_3 лет после его создания. На рис. 1 представлен фрагмент таблицы Maple для расчета наращенной суммы при конкретных значениях исходных данных.