References

1. Osipyan V.O., Osipyan K.V. *Kriptografiya v zadachax i uprazhneniyax* [Cryptography problems and exercises]. Moscow, Gelios ARV Publ., 2004. 144 p.
2. Moldovyan N.A. *Praktikum po kriptosistemam s otkrytym klyuchom* [Workshop on publickey cryptosystems]. St. Petersburg, BXV-Peterburg Publ., 2007. 304 p.
3. Alekseev A.P., Orlov V.V. *Steganograficheskie i kriptograficheskie metody zashchity informatsii: uchebnoe posobie* [Steganographic and cryptographic methods of information protection]. Samara, PSUTI Publ., 2010. 330 p.
4. Alekseev A.P. *Informatika dlya kriptoanalitikov: uchebnoe posobie* [Informatics for cryptanalysts]. Samara, PSUTI Publ, 2015. – 376 p.
5. Alekseev A.P. *Informatika 2015* [Informatics 2015]. Moscow, SOLON-Press Publ., 2015. 400 p.
6. Stanev S. *Steganologichna zashhita na informacijata*. Universitetsko izdatelstvo «Episkop Konstantin Preslavski». Shumen, 2013. 320 p. (In Bulgarian).
7. Alenin A.A., Alekseev A.P. Pomexoustojchivoe steganograficheskoe vnedrenie informacii v zvukovy'e fajly [Interference steganography introduction of information into audio files]. *Voprosy zashhity informacii,* 2013, no. 1, pp. 15 – 19.
8. Alekseev A.P., Makarov M.I. Pat. RF. *Sposob skrytoi peredachi zashifrovannoi informatsii po mnozhestvu kanalov svyazi* [Method of secure data transmission of encrypted information over multiple communication channels]. Patent RF, no. 2462825, 2012.
9. Orlov V.V., Alekseev A.P. *Aktivnaya skrytaya peredacha informatsii v setyakh TCP/IP* [Active secure communication in networks TCP / IP.]. *Tezisy dokladov Shestoi Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii «Problemy tekhniki i tekhnologii telekommunikatsii 2008»*, Kazan, 2008, pp. 446-447.
10. Cryptography I – Coursera. Available at: https://www.coursera.org/course/crypto. (accessed 9.06.2015).
11. Applied Cryptography and Encryption Class Online - Udacity. Available at: https://www.udacity.com/course/cs387. (accessed 9.06.2013).
12. Paar. C., Pelzl, J. *Understanding Cryptography*. Springer, 2010. 372 p.
13. Junod P. *A Classical Introduction to Cryptography Exercise Book.* Springer Science & Business Media, 2005. 254 p.
14. Stanev S., Zhelezov S., Paraskevov X. *Obuchenieto po kompyuturna steganografiya v Shumenskiya universitet «Episkop Konstantin Preslavski». Nauka, obrazovanie, sigurnost.* Sofiya, Izdatelstvo na NBU, 2013, pp. 445-451. (In Bulgarian).
15. Stanev S., Zhelezov S. Pervye rezul'taty vnedreniya kursa «Kompyuternaya steganografiya» v Shumenskom universitete [The first results of the implementation of the course «Computer steganography» in Shoumen University]. *Trudove na mezhdunarodnata nauchno-prakticheska konferenciya na VDPU «Kocyubinski»,* Vinnica, Ukraina, 2012, pp. 205 – 207.

Reseived 26.06.2015

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 004.65:378

УПРАВЛЕНИЕ ДОСТУПОМ ПОЛЬЗОВАТЕЛЕЙ КОРПОРАТИВНОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВУЗА

Болодурина И.П., Волкова Т.В., Ащеулова Н.А.
Оренбургский государственный университет, Оренбург, РФ
E-mail: prmat@mail.osu.ru

В статье рассматриваются вопросы управления правами доступа пользователей корпоративной автоматизированной информационной системы (КАИС) вуза в целях назначения субъекту доступа минимально необходимых привилегий. Представлена модель политики управления доступом, соединяющая ограничения предметной области и мандатной политики доступа СУБД Oracle. Модель позволяет гибко реагировать на изменения принадлежности субъекта и объекта доступа к тем или иным узлам иерархии подчинения подразделений вуза и внедрена в рамках проекта «Информационно-аналитическая система Оренбургского государственного университета».

Ключевые слова: интегрированная база данных, субъект доступа, объект доступа, модель управления доступом, ограничения предметной области.

Введение

КАИС является системой, функционирующей на основе интегрированной базы данных и развитой телекоммуникационной инфраструктуры вуза [1]. Информационные ресурсы КАИС обрабатываются значительным числом пользователей, имеющих различные права доступа. Проектирование и реализация подсистемы управления доступом пользователей КАИС вуза требует выполнения определенных и трудоемких работ в соответствии с используемой политикой доступа (см. таблицу 1). При этом необходимо решать задачу предоставления субъекту прав доступа, строго не превышая уровня требований предметной области. В целях обеспечения эффективной защиты корпоративных данных, обрабатываемых в распределенном режиме, необходимо решать задачу минимизации привилегий пользователей КАИС.

Таблица 1. Перечень задач управления правами доступа пользователей КАИС

Уровень проекта КАИС	Пользователи (субъекты доступа)	Данные (объекты доступа)	Операции с данными	Комментарий
Внешний (обобщенное представление всех пользователей)	Выделение, мониторинг, учет изменения состава пользователей	Выделение категорий, первичный учет, отслеживание изменения состава обрабатываемых данных	Выделение возможных операций манипулирования данными (добавление, обновление, чтение)	Уровень доступа пользователя зависит от принадлежности к уровню иерархии организационной структуры подразделений вуза
Концептуальный (представления разработчиков компонентов КАИС)	Проектирование функциональной составляющей подсистемы управления доступом, структур объектов доступа			Выделение связанных подмножеств объектов и субъектов доступа
Внутренний (физическая реализация проектных решений)	Проектирование объектов базы данных (таблицы, пользователи, роли, представления, пакеты, хранимые процедуры и др.)			Реализация политики управления доступом

Постановка задачи

КАИС вуза является либо собственной автоматизированной системой, либо приобретенным программным продуктом и функционирует на основе систем управления базами данных (СУБД) Oracle, MS SQL, FireBird, платформе SAP/R3 и др. Данные КАИС отражают информационные потоки, связанные с образовательной, научной, маркетинговой, управленческой и другими видами деятельности вуза, и вносят значительный вклад в формирование единой информационной среды вуза. Информационные ресурсы КАИС доступны как в открытом (свободном) режиме доступа посредством сайта образовательной организации, так и в режиме авторизации пользователя. Функции добавления и обновления сведений в рамках КАИС доступны достаточно широкому кругу пользователей – работникам различных подразделений вуза.

Решение задач управления доступом пользователей КАИС требует проведения ряда проектных мероприятий (см. таблицу 1), включающих административно-правовые, технические, технологические и другие виды работ на всех этапах проектирования компонентов, и далее – на всех последующих этапах жизненного цикла системы.

На внутреннем уровне проекта КАИС в рамках задач управления доступом пользователей описываются:

- функции идентификации пользователей, обработки событий успешной или неуспешной авторизации пользователей, настройки взаимодействия прикладной программы с объектами интегрированной базы данных КАИС и др.;
- объекты базы данных для реализации политики управления доступом (представления, функции, пакеты, пользователи, роли и др.).

Интегрированные процессы обработки информации в КАИС, как правило, состоят из раз-

нообразных операций; участники процесса, задействованные в отдельных операциях, имеют различные привилегии доступа к данным.

Для каждого отдельного пользователя достаточно трудно определить состав минимально необходимых привилегий. Зачастую их дается больше, чем необходимо для выполнения конкретных действий с данными, что может привести к нарушению целостности данных системы. Появляется задача минимизации привилегий, решение которой позволяет определить ограничения, накладываемые на функции, выполняемые в базе данных пользователем. Ограничения формулируются на основе правила: участники процесса обработки данных должны быть наделены теми и только теми привилегиями, которые естественно и минимально необходимы для получения заданного результата. Данное правило лежит в основе проектирования отношений между субъектами и объектами доступа в распределенной автоматизированной системе, управления этими отношениями.

Ограничения моделей управления доступом современных СУБД

В современных СУБД на физическом уровне реализовано несколько моделей управления доступом, которые необходимо знать и учитывать при проектировании объектов базы данных: политика ролевого управления доступом (RBAC); избирательное управление доступом (DAC); мандатное управление доступом (MAC). Результат анализа трех СУБД (Oracle 11g, MySQL, MS SQL Server 7.0), нашедших самое широкое применение на современном рынке, и поддерживаемых ими политик доступа показал, что нельзя осуществить четкое разграничение прав доступа на уровне структуры объекта доступа - каждый пользователь КАИС вуза получает более широкие полномочия, чем необходимо. Также проведенные исследования привели к выводу, что только поддержка мандатной политики дает возможность поднять класс защищенности автоматизированной системы до необходимого.

Рассмотрим реализацию управления доступом субъектов к объектам доступа в СУБД Oracle [2-3]. Для данной СУБД субъект доступа всегда строго определен, если он прошел процедуру аутентификации и идентификации. Субъект доступа имеет право на один или несколько процессов, исполняемых с определенными правилами (полномочиями) доступа. Полномочия зафиксированы административными регистрационными записями. Субъект характеризуется следующими атрибутами мандатного управления доступом: действующий идентификатор владельца процесса; идентификатор классификационной метки; массив меток на максимально доступный уровень секретности на выполнение действий с данными.

Объектами доступа в базе данных под управлением СУБД Oracle являются: таблицы (реляционные отношения), представления, процедуры, функции, пакеты. На все объекты базы данных распространяются правила дискреционной и ролевой политик управления доступом. На ряд объектов, содержащих конфиденциальную, секретную или коммерческую информацию, может распространяться мандатное управление доступом. При мандатном управлении различают следующие типы доступа: чтение данных (для таблиц, представлений, функций); добавление, удаление, обновление данных (для таблиц и представлений). При попытке субъекта осуществить доступ к объекту производится проверка прав доступа строго в следующем порядке:

- выполняются правила дискреционной и ролевой политик управления доступом. Если субъект не имеет прав доступа к объекту на основании указанных политик, СУБД выдает отказ в доступе, иначе доступ к объекту разрешается;
- выполняются правила мандатной политики управления доступом. Если выявлено, что субъект не имеет прав доступ к объекту, СУБД выдает отказ в доступе, иначе доступ к объекту разрешается.

Мандатная модель в СУБД Oracle реализуется путем использования механизма Oracle Label Security (OLS) [2]. Использование мандатной политики позволяет для заданного кортежа реляционного отношения (РО) присвоить метку с уровнем конфиденциальности доступа. Очевидным недостатком становится тот факт, что мандатная политика не поддерживает в полном объеме ограничения предметной области на проведение операций на уровне отдельных атрибутов РО. Еще одним недостатком мандатной политики является то, что установленные администратором базы данных (АБД) метки не могут динамически (без участия АБД) изменяться в соответствии с изменениями, происходящими в предметной области, влияющими на состав субъектов, объектов и правила доступа, то есть АБД не имеет возможности переложить правила подчинения данных в предметной области на уровень политики меток.

Отношения между классами объектов предметной области в рамках реализации мандатной модели управления доступом можно представить в виде информационно-логической модели (ИЛМ) предметной области в нотации Ричарда Баркера (см. рис. 1); знак «#» в данной методоло-

гии отражает уникальный идентификатор класса объектов, знак «*» - опциональность (обязательность значения) свойства класса объектов.

Каждая устанавливаемая метка должна относиться к одному конкретному субъекту доступа, правилу доступа (добавить, обновить, удалить, читать данные) и конкретному значению свойства объекта доступа. Объект доступа представлен именем и должен иметь одно или более свойств (структура объекта). Каждому свойству может соответствовать одно или более значений. Со стороны классов объектов «ЭЛЕМЕНТ ЗАГОЛОВКА ОБЪЕКТА ДОСТУПА», «СУБЪЕКТ ДОСТУПА», «ПРАВИЛО ДОСТУПА» и «МЕТКА» отношения (связи) необязательные – метка может устанавливаться не сразу.

Рассмотрим правило предметной области (далее – Правило): «Субъект доступа с именем «Субъект_1» имеет правило доступа «читать» у объекта доступа с именем «Объект_1» и заголовком, включающим атрибуты «А1», «А2» и «А3», только значения атрибута «А2», отвечающие заданному условию (далее – Условие)». Для реализации Правила на основе мандатной политики доступа в реляционной базе данных КАИС вуза осуществляются шаги:

1. На основе ИЛМ формируется схема реляционной базы данных, содержащая три главных

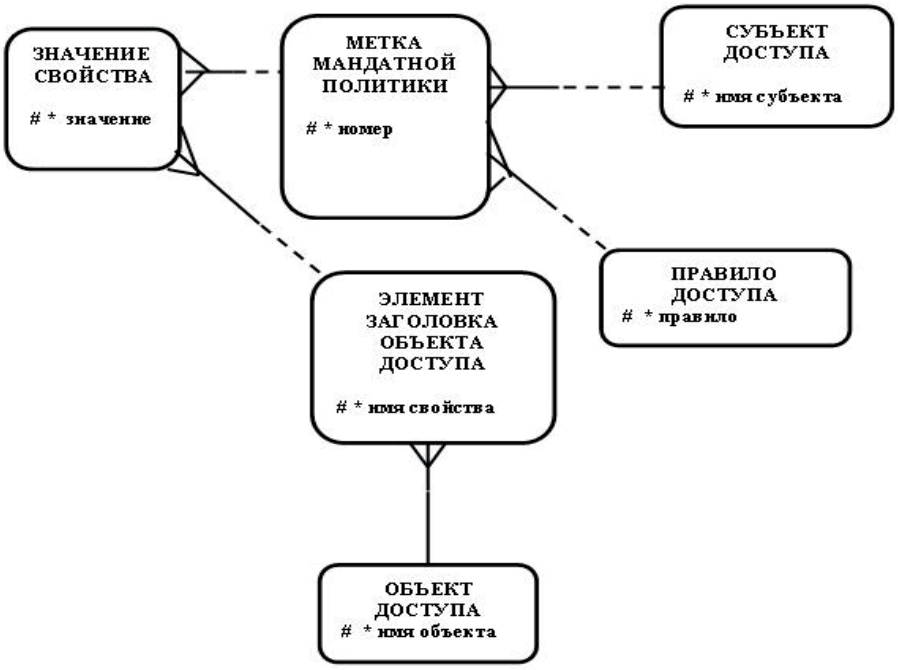

Рис. 1. ИЛМ реализации мандатной модели управления доступом

и три подчиненных реляционных отношения (см. таблицу 2); где FK – внешний ключ, реализующий связи между реляционными отношениями.

2. Выполнение операции соединения между реляционными отношениями SD, «M», «PD», «OD», «ZOD», «ZS» по равенству значений внешних ключей (FK). Формируется реляционное отношение «R», отражающее представление субъектом доступа «Субъект_1» структуры объекта доступа «Объект_1» - субъект доступа не имеет никаких прав на выполнение операций со значениями свойств объекта доступа.

Представление отражено на рис. 2а – все строки и столбцы PO, реализующего в базе данных объект доступа, заштрихованы – данные всего отношения не доступны субъекту для выполнения операций.

3. Удаление в реляционном отношении «R» строк и столбцов в соответствии с Правилом и реализацией мандатной политики доступа. Формируется отношение «R1», отражающее результирующее, заданное представление субъектом доступа «Субъект_1» структуры объекта доступа «Объект_1» – субъект доступа имеет право «Читать» значения заданных строк (метка устанавливается в соответствии с Условием). Представление отражено на рисунке 2б – строки, соответствующие Условию, не заштрихованы – данные этих строк отношения доступны субъекту для выполнения операций.

Таблица 2. Формирование реляционной структуры данных

Класс объектов предметной области	Реляционное отношение
СУБЪЕКТ ДОСТУПА (имя субъекта)	SD (IS)
ОБЪЕКТ ДОСТУПА (имя объекта)	OD (IO)
ЭЛЕМЕНТ ЗАГОЛОВКА ОБЪЕКТА ДОСТУПА (имя свойства)	ZOD (IS, IO(FK))
ПРАВИЛО ДОСТУПА (правило)	PD (P)
МЕТКА (номер)	M(NM, IA(FK), P(FK))
ЗНАЧЕНИЕ СВОЙСТВА (значение)	ZS (Z, IS (FK), NM (FK))

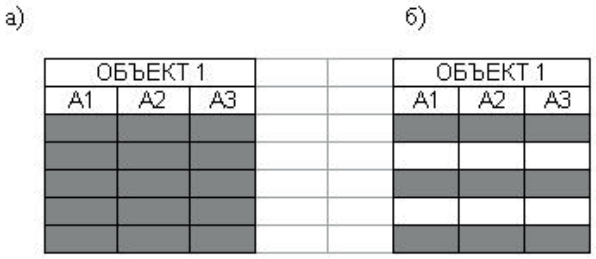

Рис. 2. Вид представления структуры объекта доступа субъектом доступа до и после наложения ограничений мандатной политики

Таким образом, мандатная политика управления доступом позволяет накладывать ограничения, установленные Правилом предметной области, но на физическом уровне субъект доступа имеет более широкие права (субъект доступа в действительности может видеть значения всех атрибутов заданной строки), что ведет к возникновению угрозы нарушения конфиденциальности данных. Также остается нерешенной задача актуальной поддержки безопасности данных с учетом изменения правил подчинения данных субъектам доступа, которые присущи предметной области в достаточно большом количестве (изменение организационной структуры вуза, добавление, обновление, удаление направлений подготовки, движение контингента обучающихся и работников и др.) – каждый раз АБД на уровне физической модели базы данных необходимо анализировать связи между существующими метками и строками таблиц и представлений, вносить соответствующие изменения в структуры объектов базы данных (представления, роли и др.).

Собственная модель управления доступом КАИС вуза

После проведенного анализа предметной области и требований к информационной безопасности КАИС стало очевидным, что необходимо разработать собственную модель управления правами доступа, основываясь на мандатной политике. Модель управления, реализуемая на основе СУБД Oracle, должна учитывать ограничения доступа на заданные свойства объекта доступа и гибко реагировать на изменения принадлежности субъекта и объекта доступа к тем или иным узлам иерархии организационной структуры вуза – см. рис. 3.

Модель, представленная на рис. 3, в сравнении с предыдущей моделью поддерживает следующие ограничения предметной области:

- каждый субъект и объект доступа должен относиться к одному конкретному структурному подразделению;
- каждому структурному подразделению может соответствовать один или более субъектов и объектов доступа.

Данные ограничения позволяют накладывать дополнительные условия на выборку тех или иных объектов доступа при реализации разграничения полномочий. В модели также реализована связь между элементом заголовка объекта доступа и меткой, что позволяет управлять разграничением доступа на уровне отдельных свойств объекта доступа.

Для реализации рассматриваемого правила на основе собственной политики управления доступом в реляционной базе данных КАИС вуза осуществляются следующие шаги.

1. В соответствии с ИЛМ формируется схема реляционной базы данных, содержащая два главных и пять подчиненных реляционных отношения (см. таблицу 3).

2. Выполнение операции соединения между реляционными отношениями «IPP», «SD», «M», «PD», «OD», «ZOD», «ZS» по равенству значений внешних ключей (FK). Формирование результирующего РО «RR», отражающего представление субъектом доступа «Субъект_1» структуры объ-

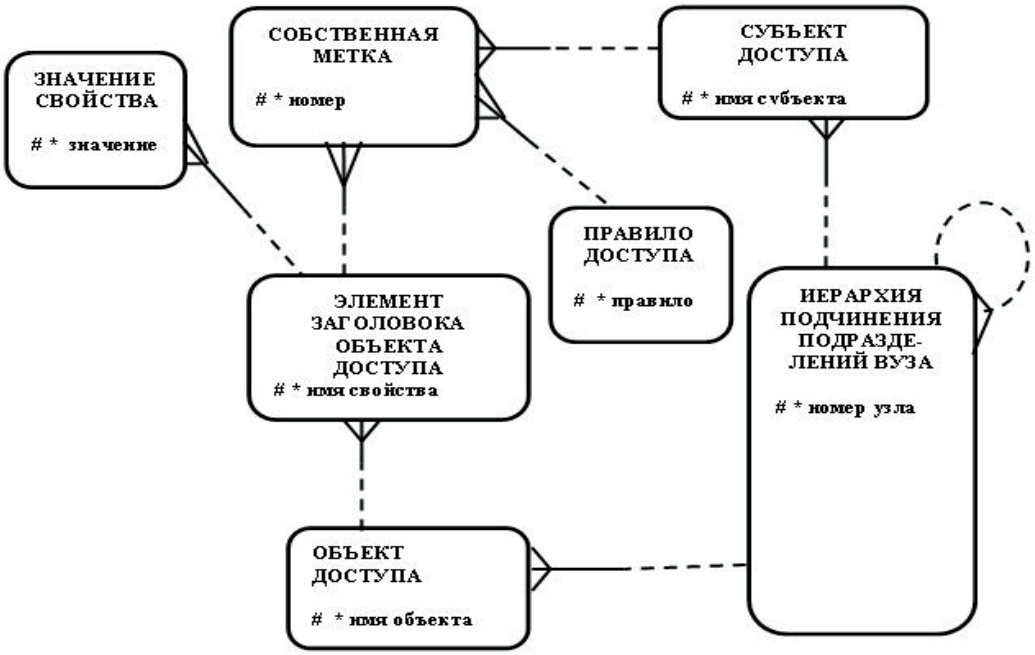

Рис. 3. ИЛМ реализации собственной политики управления доступом

Таблица 3. Формирование реляционной структуры данных

Класс объектов предметной области	Реляционное отношение
ИЕРАРХИЯ ПОДЧИНЕНИЯ ПОДРАЗДЕЛЕНИЙ (номер узла)	IPP (NU, NUR (FK)
СУБЪЕКТ ДОСТУПА (имя субъекта)	SD (IS, NU (FK))
ОБЪЕКТ ДОСТУПА (имя объекта)	OD (IO, NU (FK))
ЭЛЕМЕНТ ЗАГОЛОВКА ОБЪЕКТА ДОСТУПА (имя свойства)	ZOD (IS, IO(FK))
ЗНАЧЕНИЕ СВОЙСТВА (значение)	ZS (Z, IS (FK))
ПРАВИЛО ДОСТУПА (правило)	PD (P)
МЕТКА (номер)	M(NM, IA(FK), IS(FK), P(FK))

екта доступа «Объект_1» на основе мандатной политики. Представление отражено на рис. 3а: данные незаштрихованных строк доступны субъекту для выполнения операций.

3. Удаление в реляционном отношении «RR» строк и столбцов в соответствии с условиями предложенной модели предметной области и Правила. Формирование результирующего РО «RR1», отражающего заданное представление субъектом доступа «Субъект_1» структуры объекта доступа «Объект_1» - субъект доступа имеет право «Читать» только заданные значения (строки) заданного свойства «A2» (столбца) объекта доступа. Представление отражено на рис. 3б: незаштрихованные ячейки – уровень доступа субъекта; данные только этих ячеек доступны для операций субъекту доступа.

Предложенная модель политики доступа позволяет соединить ограничения предметной области и мандатной политики доступа.

Заключение

Реализация в КАИС вуза связи между субъектами доступа, объектами доступа и структурными подразделениями и отслеживание изменения состояния контингента субъектов доступа позволяет достаточно тонко реализовать правила конфиденциальности данных предметной области.

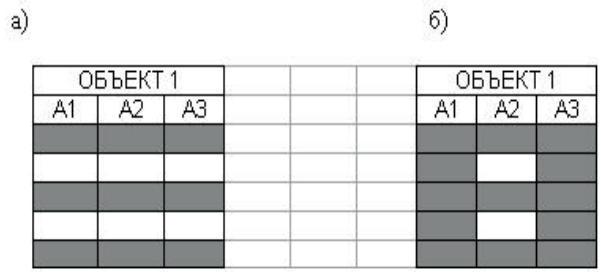

Рис. 3. Вид представления структуры объекта доступа субъектом доступа на основе собственной модели доступа

Предложенная политика управления доступом реализована в рамках проекта информационно-аналитической системы Оренбургского государственного университета (ИАС ОГУ, ias.osu.ru), относящейся к классу корпоративных автоматизированных информационных систем. ОГУ является крупным региональным вузом, осуществляющим образовательные услуги по более 80 направлениям подготовки и специальностям; в качестве пользователей (субъектов доступа) ИАС ОГУ зарегистрировано свыше 900 человек. Особенно актуально использование представленной модели для управления доступом пользователей функциональных подсистем ИАС ОГУ: «Приемная комиссия», «Деканат», «Делопроизводство», «Организация учебного процесса», «Социальная и воспитательная работа», «Организация СКУД», поскольку с задачами данных подсистем работают как в локальной вычислительной сети, так и через службы Интернет сотрудники значительного количества подразделений университета, включая филиалы и колледжи.

Литература

1. Болодурина И.П., Волкова Т.В. Распределенная обработка данных средствами автоматизированных систем вуза // Программные продукты и системы. №4, 2011. – С. 186-188.
2. Кайт Т. Oracle для профессионалов. М.: Вильямс. 2008. – 848 с.
3. Фейерштейн С., Прибыл Б. Oracle PL/SQL для профессионалов. СПб.: Питер. 2004. – 941 с.

Received 06.03.2015

Болодурина Ирина Павловна, д.т.н., профессор, заведующая Кафедрой прикладной математики (ПМ) Оренбургского государственного университета (ОГУ). Тел. (8-353) 237-25-36. E-mail: prmat@mail.osu.ru

Волкова Татьяна Викторовна, к.т.н., начальник отдела информационных систем (ИС) ОГУ. Тел.: 8 (3532) 37-25-93; E-mail: tv@mail.osu.ru

Ащеулова Надежда Алексеевна, заведующая сектором систем баз данных (СБД) ОГУ. Тел.: 8 (3532) 37-25-93; E-mail: nadya@mail.osu.ru

USER ACCESS MANAGEMENT FOR UNIVERSITY CORPORATIVE AUTOMATED INFORMATION SYSTEM

Bolodurina I.P., Volkova T.V., Ashcheulova N.A.
Orenburg State University, Orenburg, Russian Federation
E-mail: prmat@mail.osu.ru

University automated information system is based on integration of data and advanced telecommunication infrastructure with great number of users (access subjects) with varied access rights to different data elements (access objects). Problem of minimization of information system user access privilege should be solved to provide effective corporate data protection. We present model of user access policy which joins restrictions of subject domain and capability access policy DBMS Oracle. Here restrictions of subject domain under permitted access are defined by user affiliation to hierarchy nodes that corresponds to university department organizing structure. Model provides flexible response to variation of user affiliation to nodes of university department hierarchy. It was implemented to Orenburg State University as a part of project «Orenburg State University Information Analysis System».

Keywords: integrated database, access subject, access object, model of access management, restrictions of subject domain

DOI: 10.18469/ikt.2015.13.3.16

Bolodurina Irina Pavlovna, Doctor of Technical Science, Professor, the Head of Department of Applied Mathematics, Orenburg State University, Orenburg, Russian Federation. Tel.: +73532372536. E-mail: prmat@mail.osu.ru.
Volkova Tatyana Victorovna, PhD in Technical Science, the Head of Department of Information Systems, Orenburg State University, Orenburg, Russian Federation. Tel.: +73532372593. E-mail: tv@mail.osu.ru.
Ashcheulova Nadezhda Alekseevna, the Head of Sector of Database Systems, Orenburg State University. Tel.: +73532372593. E-mail: nadya@mail.osu.ru

References

1. Bolodurina I.P., Volkova T.V. Raspredelennaya obrabotka dannykh sredstvami avtomatizirovannykh sistem vuza [Distributed data processing means of the autometed systems of the university]. *Programmnye produkty i sistemy,* 2011, no. 4, pp. 186–188.
2. Kite T. *Oracle dliy professionalov* [Oracle for professionals]. Moscow, Williams Publ., 2008. 848 p.
3. Feuerstein S., Pribyl B. *Oracle PL/SQL dliy professionalov* [Oracle PL/SQL for professionals]. St. Petersburg, Piter Publ., 2004. 941 p.

Received 06.03.2015

УДК 621.391.83.004: 621.395.374

РАСЧЕТ КОНТРОЛЬНЫХ ДОПУСКОВ НА ПАРАМЕТРЫ ДИНАМИЧЕСКОГО ОБЪЕКТА

Овсянников А.С.[1], Бурова М.А.[2]
[1]Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
[2]Самарский государственный университет путей сообщений, Самара, РФ
E-mail: oats23@mail.ru

Рассматривается методика расчета контрольных допусков на параметры динамического объекта по независимым параметрам с учетом памяти результатов контроля.

Ключевые слова: контроль, динамический объект, принятие решения, гарантийный допуск, контрольный допуск, память результатов контроля.

Введение

Контроль динамических объектов в зависимости от типа, назначения, сложности и т.д. может осуществляться по одному параметру или по нескольким параметрам. При контроле объекта в процессе эксплуатации принимается решение о его состоянии – допустить ли его к дальнейшей эксплуатации (работоспособен) или не допустить (неработоспособен). Такое решение осуществляется по результатам измерения параметров динамического объекта.

В соответствии с этим процесс контроля состоит из двух этапов: измерение параметров и принятие решения по результатам измерений. При расчете контрольных допусков на параметры объекта в статье учитываются следующие допущения:

- в качестве моделей процессов изменения во времени параметров динамического объекта для целей контроля принимаются стационарные нормальные случайные процессы;
- наблюдаемый при измерении каждого параметра процесс является аддитивной смесью истинного значения параметра и ошибок измерителя;
- процессы изменения во времени каждого параметра и ошибок измерителя независимы друг от друга;
- существует память в результатах измерения каждого параметра.

Постановка задачи

Предположим, что параметры динамического объекта независимы друг от друга и для каждого параметра определено поле гарантийного допуска $\Delta_1^{(i)}; \Delta_2^{(i)}$ (допуска, определяемого соответствующими нормами и ГОСТ). С учетом этих условий за обобщенный показатель качества W динамического объекта принимается произведение характеристических функций полей гарантийных допусков [1]:

$$W = \prod_{i-1}^{N} l_i(U_i), \qquad (1)$$