УПРАВЛЕНИЕ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СРЕДОЙ С ИСПОЛЬЗОВАНЕМ ОНТОЛОГИЙ

Шахгельдян К.И.

Введение

Корпоративную информационную среду (КИС) вуза определяют как совокупность взаимосвязанных на разных уровнях – данных, приложений, пользователей и процессов, - информационных систем (включая аппаратную, в том числе и сетевую, информационную и программную составляющие), которые обеспечивают поддержку выполнения бизнес-процессов, унифицированного доступа к данным и представления данных на уровне организации [1].

Необходимость построения жизнеспособной КИС возникает в большой организации с постоянно меняющимися процессами, каковой является вуз. Жизнеспособность КИС связана с двумя основными характеристиками – адаптируемостью и адаптивностью [2]. Под адаптивностью понимается способность КИС самой настраиваться на изменения в инфраструктуре, данных, системах, аппаратном обеспечении и т.п.

КИС вуза – это сложная система со сложной, часто меняющейся инфраструктурой, с большим числом систем, серверов, данных и пользователей. Сложность эксплуатации КИС объясняется взаимозависимостью между частями КИС и тем, что изменения в одной части ведут к изменениям в большом числе связанных объектов (данных, сервисов, систем, серверов и т.п.) КИС.

В рамках построения жизнеспособной КИС ставится вопрос об автоматизации управления собственно КИС. Таки фирмы как IBM, Microsoft, Hewlett Packard занимаются исследованием в направлении автоматизации управления сетью на основе онтологий [3]. Но эти исследования направлены на низкоуровневое управление сетевой инфраструктурой. В рамках построения КИС интерес представляет также и высокоуровневое управление, которое связано с управлением средним программным слоем КИС, а также с

управлением доступом между различными объектами КИС, в том числе и с высокоуровневыми объектами – проектами, пользователями, серверными компонентами, базами данных.

В работе [4] автором рассмотрен общий подход на основе онтологий к построению КИС вуза. В рамках этого подхода рассматриваются три области понятий – понятия предметной области, понятия области ИТ и понятия области управления процессами. Использование ИТ-области позволяет автоматизировать управление КИС на уровне инфраструктуры и работы со средним слоем, обеспечивающим выполнение бизнес-логики.

Онтологический подход

К понятиям области ИТ можно отнести *Сервер, Компьютер, Базу данных, Источник данных, Пользователя, Проект, Роль, Фильтр, Метод, Серверный компонент, VLAN* и т.п. Область ИТ можно рассматривать с одной стороны как совокупность проектов, серверных компонентов, пользователей, данных и т.п., с другой – как совокупность серверов, компьютеров, коммуникационных устройств. Первый уровень относится к управлению КИС. Второй уровень - к физической инфраструктуре КИС. Таким образом, ИТ-область можно представить как совокупность логического управления, сетевой инфраструктуры и взаимоотношений между ними.

$$IT = \langle Control, Infrastructure, R_{CI} \rangle$$

Инфраструктура КИС представляет собой соединения компьютеров и коммутирующих устройств или последних друг с другом, а также виртуальных подсетей.

$$Infrastructure = \langle ITDevice, VLAN, R_{\text{inf } rastructure} \rangle$$

Понятие **ITDevice** описывает ИТ-устройства, которые формируют инфраструктуру сети. Понятие компьютер**,** производное от **ITDevice,** предназначено для описания используемых в КИС компьютеров. Оно является базовым к понятиям – сервер и персональный компьютер. Понятие

коммуникационное устройство, производное от **ITDevice**, предназначено для описания используемых в КИС телекоммуникационных устройств. Понятие **VLAN** определяет виртуальные подсети.

Управление КИС можно представить как

$$Control = \langle U, P^G, F, S, D, B, R_{Control} \rangle,$$

где U - пользователи КИС, P^G - проекты КИС, объединенные в группы, F - условия для выделения пользователей, S - серверные компоненты КИС, D - понятие как метаописание понятий (базовое для всех понятий КИС понятие Object), B - объект базы данных, $R_{Control}$ - различные отношении между ИТ-понятиями области управления КИС.

Пользователь – это обобщенное понятие того, кто получает доступ к ресурсам вуза (в том числе к ресурсам КИС). Пользователь может ассоциироваться с субъектом, а также и с проектом или серверной компонентой. Проект – это одно или несколько связанных между собой приложений КИС, решающих некоторую задачу или группу связанных задач. Все проекты КИС вуза имеют целевое назначение и поэтому могут быть разбиты на группы (по назначению).

В каждом проекте есть роли. Роль является либо совокупностью функциональных возможностей, либо способом группировки пользователей. Роль может быть связана с понятием, которое позволяет ограничить области видимости данных для пользователя, которому назначена роль. При назначении роли требуется выделить некоторых пользователей, чтобы им назначить выбранную роль. Пользователи могут быть выделены на основе некоторого признака. В частности, пользователей можно выделить на основании: должности, группы, в которую входит должность (пример, руководители, преподаватели, проректоры и т.п.), категории (студент/сотрудник/внешний пользователь/отчисленный студент/уволенный сотрудник/серверная компонента/проект), работы в некотором подразделении, работы в подразделении из некоторой группы (учебные

подразделения, бухгалтерия и т.п.), обучения в учебной группе, в некотором институте, на некоторой кафедре, наличия учетной записи в службе каталогов, а также любые другие основания. Понятие, которое позволяет выделять пользователей для назначения им прав - это условие.

Серверная компонента – это понятие, обеспечивающее реализацию бизнес-логики, (так называемый средний слой). Архитектура КИС предполагает работу проектов с серверными компонентами для взаимодействия с базами данных и обработки данных. От серверной компоненты наследуются такие понятия как: веб-служба**,** CORBA объект, COM объект, веб-приложение.

Серверная компонента состоит из методов, которые представляют собой интерфейсы к серверной компоненте. Методы, имеют описание входных и выходных параметров, целевое назначение, URL метода.

Понятие объект базы данных является базовым к источнику данных, хранимой процедуре, триггеру.

В работе [4] рассматривались отношения проекции между понятиями КИС и источниками данных: отношения проекции $p(X,b)$ являются базовыми к отношениям проекции на чтение/запись экземпляров понятия в источник данных $p_1(X,b)$, и на чтение экземпляра понятия из источника данных: $p_2(X,b)$.

Отношения между компьютерами и коммуникационными устройствами

Рассмотрим подробнее отношения между IDDevice и VLAN $R_{\text{inf}\,rastructure}$. Основное отношение между компьютерами X и коммуникационным оборудованием Y, между компьютерами, а так же между коммуникационным оборудованием, - это отношение «соединен с»: $L(X,X),L(X,Y),L(Y,Y)$. Между виртуальными сетями и компьютерами – отношения включает: $I(N,X)$.

Для автоматизации управления используются следующие аксиомы и утверждения.

Аксиома 1.

Отношение «соединен с» является симметричным : $\forall X,Y : L(X,Y) \Leftrightarrow L(Y,X)$

$\forall x_1, x_2 \in \overline{X} : l(x_1, x_2) \Leftrightarrow l(x_2, x_1)$, $\forall y_1, y_2 \in \overline{Y} : l(y_1, y_2) \Leftrightarrow l(y_1, y_2)$,

$\forall x \in \overline{X}, y \in \overline{Y} : l(x, y) \Leftrightarrow l(y, x).$

Здесь $\overline{X}$ - определяет множество всех экземпляров понятия X, x - экземпляр понятия X, $l(x,y)$ - экземпляр отношений $L(X,Y)$ между экземплярами x и y.

Аксиома 2.

Отношение «соединен с» является транзитивным: $\forall X,Y : L(X,Y) \wedge L(Y,X) \Rightarrow L(X,X)$, $\forall y_1, y_2, y_3 \in \overline{Y} : l(y_1, y_2) \wedge l(y_2, y_3) \Rightarrow l(y_1, y_3)$,

$\forall x \in \overline{X}, y_1, y_2 \in \overline{Y} : l(x, y_1) \wedge l(y_1, y_2) \Rightarrow l(x, y_2)$, $\forall x_1, x_2, x_3 \in \overline{X} : l(x_1, x_2) \wedge l(x_2, x_3) \Rightarrow l(x_1, x_3)$

Для составления общей картины взаимодействия компьютеров нет необходимости в полном описании всех связей, для определения результирующего отношения используются аксиомы 1 и 2.

Характеристикой отношения «соединен с» является объем канала связи $l(x, y|t|)$, где t - пропускная способность канала. При этом определена следующая аксиома.

Аксиома 3.

$$\forall x_1, x_2, x_3 \in \overline{X} \cup \overline{Y} : l(x_1, x_2|t_1|) \wedge l(x_2, x_3|t_2|) \Rightarrow l(x_1, x_3|\min(t_1, t_2)|)$$

На основании этой аксиомы может быть вычислена пропускная способность между любыми двумя узлами в сети.

Если $\exists x, y \in \overline{X} \cup \overline{Y} : \neg l(x, y)$, то, следовательно, сеть вуза не имеет общую корпоративную инфраструктуру.

Отношения между ролями

Роли принадлежат проекту, следовательно, между ними определены отношения включения $I(P,R)$ - проект P включает роли R. Роли могут быть связаны отношениями обобщения $\tilde{Q}(R,R)$ и отношениями администрирования роли $\tilde{Q}(R,R)$. Определены отношения и между пользователями и ролями – пользователю назначена роль $Z(U,R)$, пользователь имеет право назначать роль $\tilde{Z}(U,R)$.

Роль может иметь область видимости, которая позволяет ограничивать доступ к данным, выделенным по некоторому признаку. Для этого должны быть определены отношения между экземплярами роли и понятием C, отвечающим за область видимости: $r \in \overline{R} : E(r, C)$.

Можно выделить три варианта отношений назначения:

Аксиома 4.

Простая роль назначается без каких-то ограничений по области видимости $\overline{Z(U,R)} = \{z(u,r), u \in \overline{U}, r \in \overline{R}\}$.

Аксиома 5.

Роль с ограничением по области видимости назначается пользователям на конкретную область видимости $\overline{Z(U,R^C)} = \{z(u,r^c), u \in \overline{U}, r \in \overline{R}, c \in \overline{C} : E(r,C)\}$.

Аксиома 6.

Роль с ограничением по области видимости назначается автоматически пользователям из некоторой выборки на основании связи пользователей с областью видимости $\overline{Z(U^D,R^C)} = \{r(u^d,r^c), u \in \overline{U}, r \in \overline{R}, P'(D,C) \vee D = C, S(U,D)\}$.

Последний вариант означает, что для существования отношений назначения, необходимо, чтобы существовали некоторые явные отношения $S(U,D)$ между ограничениями на выборку пользователей и пользователем, а так же отношения наследования между ограничениями на область видимости роли и одним из ограничений на выборку пользователей $P'(D,C)$, либо эти понятия должны совпадать $D = C$.

Различия в вариантах отношений назначения реализуется атрибутами отношений. К атрибутам отношения назначения относятся так же период действия назначения, т.е. доступ к некоторому ресурсу КИС устанавливается на определенный период времени (возможно, неограниченный), статус назначения, который может быть определен как Разрешено/Запрещено. Временные атрибуты отношений назначения позволяет не только устанавливать периоды действия, но и задавать более сложные временные последовательности действия роли. Для этого используются атрибуты,

уточняющие период: дни недели, время начала и окончания в течение суток, четность даты.

Аксиома 7.

Если роль r_1 обобщает роль r_2: $\forall r_1, r_2 \in \overline{R}, \phi(r_1, r_2)$, то пользователи с ролью r_1: $u \in \overline{U} : z(u, r_1)$, где $\overline{U}$ - множество всех пользователей КИС, имеют права пользователей с ролью r_2: $z(u, r_2)$, т.е. $\forall r_1, r_2 \in \overline{R} : \phi(r_1, r_2) \wedge z(u, r_1) \Rightarrow z(u, r_2)$

Для ролей с ограниченной областью видимости аксиома 7 должна быть уточнена.

Аксиома 8.

Пусть роли r_1 и r_2 имеют одно и то же понятие в качестве области видимости, т.е. определены отношения между ролью и некоторым понятием C: $E(r_1, C), E(r_2, C)$. Если $\exists \phi(r_1, r_2)$, то пользователи с ролью r_2 имеют права пользователей с ролью r_1 на ту же область $c \in C$: $\forall r_1, r_2 \in \overline{R}, \forall c \in C : \phi(r_1, r_2) \wedge E(r_1, C) \wedge E(r_2, C) \wedge z(u, r_1^c) \Rightarrow r(u, r_2^c)$.

Аксиома 9.

Пусть определены отношения $E(r_1, C), E(r_2, D)$, а так же существуют экземпляры отношений обобщения $\phi(r_1, r_2)$. Тогда пользователи с ролью r_1^c: $c \in C$ имеют права пользователей с ролью r_2^d : $z(u, r_1^c) \Rightarrow z(u, r_2^d)$. Последнее означает, что между C и D должны существовать некоторые отношения $P''(D, C)$, которые позволяют по определенным экземплярам понятия C: $c \in C$, получить соответствующие экземпляры понятия D: $\forall c \in C, d \in D : p''(d, c)$, т.е. $\forall r_1, r_2 \in \overline{R}, \forall c \in \overline{C}, d \in \overline{D}, u \in \overline{U} : p''(d, c) \wedge \phi(r_1, r_2) \wedge z(u, r_1^c) \Rightarrow z(u, r_2^d)$

Аксиома 10.

Если определены отношения между ролью и областью видимости $E(r_2, D)$, а так же между ролями: $\phi(r_1, r_2)$, то назначение определяется следующим образом: $\forall r_1, r_2 \in \overline{R} : \phi(r_1, r_2) \wedge e(r_2, d) \wedge z(u, r_1) \Rightarrow \forall d \in \overline{D} : z(u, r_2^d)$.

Аксиома 11.

$\forall r_1, r_2 \in \overline{R} : \phi(r_1, r_2) \wedge E(r_1, C) \wedge z(u, r_1^c) \Rightarrow z(u, r_2)$.

Аксиома 12

Отношения обобщения между ролями являются транзитивными, т.е. $\forall r_1, r_2, r_3 \in \overline{R} : g(r_1, r_2) \wedge g(r_2, r_3) \Rightarrow g(r_1, r_3)$, причем с соответствующими ограничениями по областям видимости.

Администрирование роли – это другой тип отношений между ролями, который позволяет тому, у кого есть некоторая роль $r_1 \in \overline{R}$, назначать пользователям роль $r_2 \in \overline{R}$.

Аксиома 13.

Если роль r_1 имеет администраторский доступ к роли r_2, то пользователь с ролью r_1 имеет право назначать другим пользователям роль r_2 : $\forall r_1, r_2 \in \overline{R}, u \in \overline{U} : \tilde{q}(r_1, r_2) \wedge z(u, r_1) \Rightarrow \tilde{z}(u, r_2)$.

Эти отношения также требуют уточнения в связи с присутствием у роли области видимости.

Аксиома 14.

Если роли r_1 и r_2 имеют одно и то же понятие C в качестве области видимости и роль r_2 имеет администраторский доступ к роли r_1: $\tilde{q}(r_1, r_2)$, то пользователи с ролью r_1 , ограниченные областью $c \in \overline{C}$, имеют права назначать пользователям роль r_2 с тем же ограничением c . $\forall r_1, r_2 \in \overline{R}, u \in \overline{U}, c \in \overline{C} : \tilde{q}(r_1, r_2) \wedge s(r_1, c) \wedge s(r_2, c) \wedge z(u, r_1^c) \Rightarrow \tilde{z}(u, r_2^c)$

Аксиома 15.

Если роль r_1 имеет понятие C в качестве ограничения области видимости и роль r_2 имеет понятие D в качестве ограничения области видимости, то если роль r_1 с ограничением по области $c \in \overline{C}$ имеет административный доступ к роли r_2, ограниченной областью $d \in \overline{D}$, то пользователи с ролью r_1 на область c имеют права назначать пользователям роль r_2 с ограничением на область c , где экземпляр c имеет отношение с экземпляром d : $\forall r_1, r_2 \in \overline{R}, u \in \overline{U}, c \in \overline{C}, d \in \overline{D} : \tilde{q}(r_1, r_2) \wedge e(r_1, c) \wedge e(r_2, c) \wedge p''(c, d) \wedge z(u, r_1^c) \Rightarrow \tilde{z}(u, r_2^d)$.

Отношения $P''(C,D)$ могут быть как некоторыми специфичными отношениями, так и отношениями наследования и агрегирования между понятиями, описывающими область видимости.

Аксиома 16.

Если роль r_2 имеет понятие D в качестве ограничения области видимости и роль r_1 не имеет ограничений, то если роль r_1 имеет администраторский доступ к роли r_2 , то пользователи с ролью r_1 имеют права назначать пользователям роль r_2 с любым из ограничений: $\forall r_1, r_2 \in \overline{R}, u \in \overline{U} : \tilde{q}(r_1, r_2) \wedge S(r_2, D) \wedge z(u, r_1) \Rightarrow \forall d \in \overline{D} : \tilde{z}(u, r_2^d)$.

Отношения административного доступа не транзитивны. Между двумя ролями разрешено иметь одновременно отношения обобщения и административного доступа. Это позволяет обеспечить ситуацию, когда тот, кто имеет права назначать пользователям роль, автоматически сам эту роль имеет.

Пользователи КИС являются отражением некоторой сущности, которая должна получить доступ к ресурсам вуза (необязательно информационным). Для пользователя КИС определено отношение ассоциации с различными понятиями КИС:

$$A(U, Object) = A\left(U, \begin{bmatrix} Student, Employee, External, Employer, Parents, Ex-Student, \\ Ex-Employee, Scholar, \Pr oject, ServerComponent \end{bmatrix}\right).$$

Если пользователь ассоциируется с проектом или серверной компонентой, то проект или серверная компонента использует учетную запись этого пользователя для доступа к другим серверным компонентам.

Для одного и того же пользователя разрешено иметь несколько разных отношений ассоциации.

Отношения между онтологиями управления КИС и инфраструктуры

Между серверной компонентой S и методами V определено отношение включения $I(S,V)$. Серверные компоненты «функционируют на» серверах,

поэтому определены отношения $C(S,X)$, где S - серверная компонента, X - сервер.

Если серверная компонента реализуется с помощью хранимой процедуры, то между ними определены отношения: $F(S,B)$. Между сервером и базой данных определены отношения включения $I(X,D_B)$, где X - сервер, D_B - база данных. Между базой данных и объектом базы данных определены отношения включения $I(D_B,B)$, где B - объект базы данных.

Утверждение 1.

$\forall x \in \overline{X}, d \in \overline{D}, b \in \overline{B} : i(x,d) \wedge i(d,b) \Rightarrow i(x,b)$

Утверждение основывается на транзитивности отношений включения.

Аксиома 17.

Если объект базы данных является хранимой процедурой и одновременно серверной компонентой, то отношения включения эквиваленты отношению функционирует $\forall x,s,b : i(x,b) \wedge f(s,b) \Rightarrow c(x,s)$.

Отношения доступа

Между различными понятиями ИТ-области возможны отношения доступа $W(X,Y)$, т.е. экземпляр понятия X имеет доступ к экземпляру понятия Y. На основе отношений доступа выполняется управление доступом к ресурсам КИС.

Аксиома 18.

Если пользователю назначена некоторая роль $z(u,r)$, тогда у пользователя есть доступ к соответствующему проекту $\forall p,u,r : i(p,r) \wedge z(u,r) \Rightarrow w(u,p)$.

Аксиома 19.

Между проектом и методом серверной компоненты определен доступ, если пользователю, ассоциированному с проектом $a(u,p)$, назначена роль «Доступ для метода серверной компоненты» r^v к методу v_s серверной компоненты s $\forall u,p,v : a(u,p) \wedge z(u,r^v) \Rightarrow w(p,v_s)$. Эти отношения эквивалентны: $w(u,v_s)$.

Понятие виртуальных подсетей имеет отношение «доступ разрешен» с самим собой $W(N,N)$. Это позволяет для каждой подсети определить те подсети, доступ к которым разрешен из подсети.

Аксиома 20.

Отношения «доступ разрешен» для виртуальных сетей являются симметричными (в смысле экземпляров понятий), но не транзитивными.

$$\forall n_1, n_2 : w(n_1, n_2) \Leftrightarrow w(n_2, n_1)$$

Это, например, означает, что если из студенческой и офисной подсетей разрешен доступ в виртуальную подсеть студенческих серверов, то это не мешает запретить доступ из студенческой в офисную подсеть.

Между узлами и коммуникационными устройствами также могут быть определены отношения «доступ разрешен». Чаще всего такие отношения связывают серверы между собой или компьютеры и серверы: $W(X,X)$.Эти отношения не являются ни транзитивными, ни симметричными.

Определим отношения доступности двух узлов $x_1, x_2 \in \overline{X} : w'(x_1, x_2)$.

Аксиома 21.

Отношения доступности представляют собой

$$\forall x_1, x_2 \in \overline{X}, n_1, n_2 \in \overline{N} :$$
$$w'(x_1, x_2) \Rightarrow l(x_1, x_2) \wedge i(n_1, x_1) \wedge i(n_2, x_2) \wedge (w(n_1, n_2) \vee n_1 = n_2) \wedge w(x_1, x_2)'$$

т.е. отношения доступности двух узлов определены тогда, когда, во-первых, определено соединение между узлами, во-вторых, узлы включены в виртуальные подсети, между которыми доступ разрешен, и, в-третьих, между узлами так же разрешен доступ. Отношения доступности имеют характеристику пропускной способности, которая определяется аналогичной характеристикой отношения «соединен с».

$$\forall x_1, x_2 \in \overline{X}, n_1, n_2 \in \overline{N} :$$
$$w'(x_1, x_2 | t|) \Rightarrow l(x_1, x_2 | t|) \wedge i(n_1, x_1) \wedge i(n_2, x_2) \wedge (w(n_1, n_2) \vee n_1 = n_2) \wedge w(x_1, x_2)'$$

Так как отношения «доступ разрешен» между узлами (и/или коммуникационными устройствами) не являются симметричными, то и отношения доступности двух узлов не являются симметричными. Так как

отношения между виртуальными подсетями не являются транзитивными, то и отношения доступности между узлами также не являются транзитивными.

Между методами серверных компонент и понятиями КИС определены отношения доступа $W(V,D)$, при этом так же определены производные отношения $W_1(V,D)$ - чтение/запись методом V экземпляров понятия D и $W_2(V,D)$ - чтение методом V экземпляров понятия D.

Утверждение 2.

Если пользователь, ассоциированный с некоторым проектом $a(u,p)$ имеет доступ к методу v: $w(u,v)$, а метод имеет доступ к понятию $w(v,d)$ ($w_1(v,d)$ или $w_2(v,d)$), то определен соответствующий доступ пользователя (соответствующего проекта) к понятию $w(u,d)$ ($w_1(u,d)$ или $w_2(u,d)$). $\forall u,v,d: w(u,v) \wedge w(v,d) \Rightarrow w(u,d)$ ($\forall p,v,d: w(p,v) \wedge w(v,d) \Rightarrow w(p,d)$).

Утверждение 3.

Если проект p имеет доступ к понятию d : $w(p,d)$, а понятие d имеет отношения проекции с источником b : $p(d,b)$ ($p_1(d,b)$ или $p_2(d,b)$), то определен доступ проекта к источнику данных $w(p,b)$ ($w_1(p,b)$ или $w_2(p,b)$). $\forall p,v,d: w(p,d) \wedge p(d,b) \Rightarrow w(p,b)$.

Утверждение 4.

Если метод серверной имеет компоненты v имеет доступ к понятию d : $w(v,d)$, а понятие d имеет отношения проекции с источником b : $p(d,b)$ ($p_1(d,b)$ или $p_2(d,b)$), то определен доступ метода серверной компоненты к источнику данных $w(v,b)$ ($w_1(v,b)$ или $w_2(v,b)$). $\forall p,v,d: w(v,d) \wedge p(d,b) \Rightarrow w(v,b)$.

Аксиома 22.

Между серверными компонентами определен доступ, если пользователю, ассоциированному с серверной компонентой $a(u,s)$, назначена роль «Доступ для метода серверной компоненты» r^{v_s} к серверной компоненте s $\forall u,s_1,s_2: a(u,s_1) \wedge i(s_2,v_2) \wedge z(u,r^{v_s}) \Rightarrow w(s_1,s_2)$.

Аксиома 23.

Если между серверными компонентами s_1 и s_2 установлены отношения доступа $w(s_1, s_2)$(т.е. между одной серверной компонентной и по крайне мере одним методом другой серверной компоненты), то между серверами, на которых функционируют эти компоненты, должен быть обеспечен доступ

$\forall s_1, s_2, v_2 : w(s_1, v_2) \wedge i(s_2, v_2) \wedge f(s_1, x_1) \wedge c(x_2, s_2) \Rightarrow w'(x_1, x_2)$

Аксиома 24.

Между серверной компонентой s и понятиями d определен доступ на чтение/запись или на чтение, если пользователю, ассоциированному с серверной компонентой $a(u,s)$, назначена роль «Доступ разрешен на чтение/запись» r_1^d или «Доступ разрешен на чтение» r_2^d соответственно: $\forall u, s, r^d : a(u,s) \wedge z(u, r^d) \Rightarrow w(s,d)$.

Аксиома 25.

Между понятием d и источником b определен доступ, если определены соответствующие отношения проекции: $p_1(d,b) \Rightarrow w_1(d,b)$, $p_2(d,b) \Rightarrow w_2(d,b)$

Аксиома 26.

Между методами серверных компонентов определен доступ, если пользователю, ассоциированному с серверной компонентой $a(u,s_1)$, назначена роль «Доступ для метода серверной компоненты» $r^{v_{s2}}$ к методу v_{S_2} серверной компоненте s_2 $a(u,s_1) \wedge z(u, r^{v_{s2}}) \wedge i(s_2, v_2) \Rightarrow \forall v_1 : i(s_1, v_1) \wedge w(v_1, v_2)$.

Аксиома 27.

Между серверной компонентой и источник данных определен доступ, если определен доступ между серверной компонентой и понятием, а также между понятием и источником данных $\forall s, d, b : w(s,d) \wedge w(d,b) \Rightarrow w(s,b)$.

Реализация управления в КИС на основании отношений

Аксиомы и утверждения позволяют автоматизировать управление в КИС.

Генерация назначения ролей пользователям в КИС выполняется на основании аксиом 4-6.

Если пользователю назначена роль, которая связаны отношением обобщения с другими ролями, то на основании аксиом 7-12 генерируются соответствующие назначения ролей пользователю.

Если пользователю u назначена роль проекта $p:i(p,r_p)$, то на основании аксиомы 18 ему разрешен доступ к проекту: $w(u,p)$. На основании этих отношений пользователю при входе в портал предлагаются доступные ему проекты. Каждый проект должен выполнять проверку прав пользователя с помощью специализированной серверной компоненты, которая возвращает все доступные роли для пользователя в проекте, основываясь на аксиомах 4-12.

Если пользователю назначена роль, связанная административным доступом с другими ролями, то на основании аксиом 13-16 пользователю становится доступным в системе управления правами режим назначения для соответствующих ролей и с соответствующими областями видимости.

Метод серверной компоненты проверяет легитимность вызова на основании отношений доступа $w(p,v)$ (аксиома 19) и на основании $w(v_1,v_2)$ (аксиома 26).

Так как серверная компонента s имеет отношения функционирования с серверами $x:c(x,s)$, в тоже время в соответствии с аксиомой 27 компонента имеет доступ с источниками данных b, расположенными на серверах $y:i(y,b)$, то значит должен быть обеспечен доступ между серверами $w'(x,y)$. Отношения доступа так же определены между серверами на основе аксиомы 23. Соединение между серверами определяется на основании аксиом 1 и 2.

Поскольку для обеспечения доступа согласно аксиоме 21 необходимо обеспечение прозрачности соответствующих виртуальных подсетей, настройки безопасности на серверах, то такие процедуры могут быть осуществлены автоматически с помощью специализированных компонент управления коммуникационным оборудованием и серверами.

Серверные компоненты, реализуя бизнес-логику, работают с понятиями, имеющими проекцию на источники данных. В результате, во-

первых, определены отношения доступа между методами серверных компонентов и источниками данных, согласно утверждению 4, во-вторых, должны существовать пользователи, от имени которых методы обращаются к базам данных, где расположены соответствующие источники.

Последнее означает, что для метода серверной компоненты необходимы права доступа к базе данных. Предпочтительным является подход, который состоит в автоматическом создании учетной записи пользователя базы данных, соответствующей одной серверной компоненте, и автоматическое установление для нее прав в базе данных.

Итак, для каждого вновь созданной серверной компоненты (ее учетной записи $u_s : a(u_s, s))$ могут быть созданы соответствующие учетные записи в базах данных: u_{db}. Для реализации этого используется следующая аксиома.

Аксиома 28

$$\forall u_s, b, d : a(u_s, s) \wedge w_1(v_s, b) \wedge i(d, b) \Rightarrow \exists u_{db} : i(d, u_{db}) \wedge w_1(u_{db}, b)$$

$$\forall u_s, b, d : a(u_s, s) \wedge w_2(v_s, b) \wedge i(d, b) \Rightarrow \exists u_{db} : i(d, u_{db}) \wedge w_2(u_{db}, b)$$

$$w_1(u_{db}, b) \Rightarrow w_2(u_{db}, b).$$

Аксиома определяет необходимость в пользователи базы данных, который создается на основании существования пользователя, ассоциированного с серверной компонентой, и отношения прав доступа между методом серверной компоненты и источником данных. Кроме этого, так определяется доступность чтения при наличии прав на чтение/запись.

Права доступа $w_1(u_{db}, b)$ определяются права доступа к соответствующим таблицам на INSERT, UPDATE, DELETE и SELECT, для отношения $w_2(u_{db}, b)$ права определены на SELECT. Если источники данных в разных методах расположены на разных серверах, то пользователей баз данных должно быть несколько (с одинаковым именем и возможно разными правами).

Если в качестве метода серверной компоненты рассматривается процедура базы данных, то для вызова процедуры должен быть пользователь базы данных:

Аксиома 29

$$\forall u_s, b, d : a(u_s, s) \wedge z(u_s, r_b^{P_2}) \wedge i(d, b) \Rightarrow \exists u_{db} : i(d, u_{db}) \wedge w(u_{db}, b) \ .$$

Если серверная компонента меняет правила работы с понятиями, то автоматически, согласно аксиоме 28, меняются права соответствующих учетных записей баз данных.

Во многих случаях проблемы производительности в КИС связаны с большими нагрузками на серверы, где функционируют серверные компоненты. Для решения таких проблем используется алгоритм баланса нагрузки, когда одна и та же серверная компонента размещается на нескольких серверах и для достижения эффективности работы используется наиболее подходящий сервер.

В основе алгоритма лежит алгоритм, предложенный автором в работе [5]. В общем случае приоритет сервера, который выбирается для реализации очередного запроса к методу серверной компоненты, может быть вычислен по формуле

$$\lambda = \sum_i a_i v_i \ ,$$

где v_i - характеристика сервера или окружения КИС, которая влияет на выбор сервера, a_i - весовой коэффициент характеристики.

Рекомендуемые характеристики в КИС описаны в соотношении

$$\lambda = a_1 p + a_2 v + a_3 n \ ,$$

где p – относительная загруженность процессоров сервера, v – пропускная способность канала между серверами (определяется из аксиомы 21); n - обратная величина к числу необработанных в методе серверной компоненты запросов.

В процессе сопровождения возникает необходимость в изменениях, семантики понятий, и, следовательно, в соответствующих источниках

данных. В этом случае необходимо рассмотреть все процедуры, использующие измененные данные. Автоматически такую информацию можно получить на основании аксиом 24, 25, 27 и утверждений 2-4.

Заключение

КИС Владивостокского государственного университета экономики и сервиса (ВГУЭС) является распределенной гетерогенной средой, объединяющей в единое пространство среды двух филиалов, 25 тыс. пользователей, около 5 млн. назначений ролей, 12 серверов баз данных, 300 описанных понятий, 70 серверных компонентов. Автоматизация управления в такой среде является одной из первоочередных задач. В результате применения предложенного в работе подхода в КИС ВГУЭС автоматизированы все процессы, связанные с управлением правами пользователей, с управлением серверными компонентами, с обеспечением баланса нагрузки.

Литература

[1] Игнатова И.Г. Принципы образовательной и научно-технической информатизации вуза//Высшее образование сегодня.-2004.-№11.-с.55-56.

[2] Herring C. Viable Software. The intellint control paradigm for adaptable and adaptive architecture. PhD Thesis.- Australia.-2002.

[3] Stojanovic L., Schneider J., Maedche A., Libischer S., Studer R., Lumpp Th., Abecker A., Breiter G., Dinger J.. The role of ontologies in autonomic computing systems//IBM Research Journal. - 2004.-vol.43-№4

[4] Шахгельдян К.И. Применение онтологического подхода в корпоративной информационной среде вуза//НТ Ведомости СПбГПУ.-2007.-№4-2 (52).-189-194.

[5] Крюков В.В., Майоров В.С., Шахгельдян К.И. Алгоритм баланса нагрузки для обеспечения режима реального времени в распределенной системе сбора и обработки данных//Информационные технологии.- 2004.-№7.-с. 11-17.