УДК 681.324

К.И. ШАХГЕЛЬДЯН, В.В. КРЮКОВ, Д.В. ГМАРЬ

Система автоматического управления правами доступа к информационным ресурсам вуза

Аннотация

В статье рассматриваются вопросы построения системы управления правами пользователей в корпоративной интегрированной информационной среде вуза. Описана логическая, информационная, функциональная и математическая модели системы, а так же приведены примеры использования полученных решений при разработке других информационных систем вуза.

Введение

В процессе информатизации вуза можно выделить несколько этапов [1]. Как правило, в вузах используется несколько программных продуктов или информационных систем, каждая из которых имеет собственную систему регистрации и администрирования прав пользователей. Для таких систем необходимы администраторы, которые участвует в процессе управления правами, а иногда и в процессе регистрации пользователей. Кроме того, администраторы должны поддерживать данные о правах пользователей в актуальном состоянии.

Если таких систем одна или две и число пользователей невелико, то администрировать права пользователей систем можно вручную. Если же число информационных систем исчисляется десятками, а пользователей тысячами, то сопровождать процесс администрирования прав пользователей вручную становится невозможным, т.к. администраторы не успевают решать возникающие проблемы, к которым можно отнести:

- пользователи забывают несовпадающие имена и пароли в разных системах;
- некоторые системы требуют подтверждения регистрации пользователя, в котором участвует администратор;
- требуется назначение повторяющихся прав пользователей в различных системах;
- требуется поддержка прав пользователей в актуальном состоянии.

Можно предположить, что число студентов в среднем вузе составляет 10000 человек, а число сотрудников и преподавателей около 1500 – 2000. Поскольку как контингент студентов, так и персонал находятся в постоянном «движении», то возникает потребность автоматизировать процесс регистрации, управления правами и актуализации прав пользователей в корпоративной интегрированной информационной среде (КИИС) вуза.

Корпоративная интегрированная информационная среда вуза – это совокупность информационной инфраструктуры, корпоративных данных и информационных систем, работающих как единый механизм и направленных на информатизацию деловых задач и бизнес процессов, стоящих перед вузом.

Вопросам построения КИИС вуза посвящены работы [1-6], в которых обсуждаются проблемы проектирования КИИС, модели информационной среды, обязательные компоненты, входящие в среду. Одним из компонент среды является система единой регистрации и управления правами пользователей.

Вопросы, связанные с моделью управления правами пользователей на основе индивидуально-группового разграничения прав, обсуждались в нескольких работах, например, в [7]. Но данный подход применим в случае небольшого числа групп пользователей, которые, кроме того, являются статичными. В вузе число групп пользователей постоянно растет, а сами группы не являются постоянными по составу, так как организационная структура вуза часто меняется. В результате для обеспечения

автоматического управления правами пользователей требуется подход, основанный не на группах, а на динамических структурах.

В первой части работы описана архитектура системы единой регистрации и управления правами пользователей, обоснован выбор технологий и структуры. Вторая часть содержит описание моделей системы: логическая модель (описание основных понятий и их отношений), информационная модель (описание прав пользователей системы), функциональная модель и математическая модель. Третья часть работы посвящена рассмотрению результатов разработки и внедрения системы управления правами в КИИС Владивостокского государственного университета экономики и сервиса (ВГУЭС).

1. Система единой регистрации и управления правами пользователей

Назначением системы единой регистрации и управления правами пользователей (СЕРУПП) является автоматизация процедуры управления доступом пользователей к ресурсам КИИС. Ресурсы КИИС представляют собой набор информационных систем и данных, связанных с ними. Кроме того, СЕРУПП обеспечивает для разрабатываемого и поддерживаемого корпоративного программного обеспечения потребности в создании ролей и назначении прав пользователей, что освобождает разработчиков КИИС от решения этих задач в каждом отдельном приложении.

Основными функциями СЕРУПП являются:

- поддержка автоматической регистрации в КИИС персонала и студентов вуза на основании данных о них, хранящихся в корпоративных базах данных (при регистрации возможна идентификация на основании паспортных данных, ИНН, пенсионного кода и т.п.);
- управление правами доступа пользователей к информационным ресурсам вуза;

- поддержка в актуальном состоянии данных о правах пользователей с учетом любых изменений – прием (зачисление), увольнение, перевод, изменение должности, должностных обязанностей (специальности), слияние подразделений, создание новых подразделений и т.п.

Результатом внедрения СЕРУПП является наличие единого имени и пароля у каждого пользователя для входа во все программные приложения (проекты) КИИС, в том числе и в корпоративную сеть. Единая процедура управления правами во всех проектах КИИС имеет большие возможности по автоматизации процесса управления и поддержания данных в актуальном состоянии. Еще одним преимуществом внедрения СЕРУПП является исключение разработки процедуры регистрации пользователей для новых проектов. Это упрощает процесс разработки, внедрения и сопровождения информационных систем в вузе.

1.1. Технологии системы

Один из вопросов, который необходимо решить при разработке СЕРУПП, состоит в выборе технологии для хранения учетных записей пользователей.

В последнее время многие производители программного обеспечения поддерживают LDAP-серверы, чтобы управлять правами пользователей. Существуют несколько LDAP-серверов от различных производителей – Microsoft Active Directory, Sun Security Server, Novell e-Directory и другие.

Область применения LDAP-серверов в КИИС вуза имеет несколько ограничений. Во-первых, не все программное обеспечение может работать со службой каталогов и именно той, которую использует конкретный вуз. Во-вторых, не везде возможно использование этой службы из-за архитектурных ограничений, вызванных требованиями безопасности. Например, для службы каталогов Active Directory (AD), используются доменные записи, хранящиеся на контроллере домена, расположенном во внутренней сети вуза. Web-сервер, расположенный за сетевым экраном, не имеет прямого соединения с контроллерами доменов, и к нему невозможно разграничить доступ с

использованием учетных записей AD (рис.1). Кроме того, желательно обеспечить доступ к некоторым информационным ресурсам пользователям, не имеющим учетную запись в каталоге AD вуза. Например, это может относиться к внешним пользователям портала, информация о которых не хранится в корпоративной базе данных вуза.

Потребность в совмещении управления правами пользователей корпоративной сети и всех информационных ресурсов среды приводит к необходимости использования двух серверов хранения учетных записей – LDAP сервера и сервера базы данных учетных записей пользователей для ресурсов, доступ к которым нельзя организовать с использованием LDAP сервера.

1.2. Учетные записи пользователя

При регистрации пользователя в КИИС создается две учетной записи с одинаковым именем и паролем – учетная запись AD и учетная запись, используемая для доступа к ресурсам, доступ к которым нельзя организовать с использованием AD (далее будем ссылаться на нее как на UNet). Применение этих учетных записей не связано друг с другом, за исключением процедуры актуализации, которая может выполнять изменения учетных записей в двух базах данных, и процедуры удаления учетных записей.

Учетная запись AD обеспечивает доступ к следующим информационным ресурсам: корпоративная сеть, файловые серверы студентов и сотрудников, корпоративные базы данных, доступ в Интернет, на внутренний корпоративный портал, к корпоративному программному обеспечению. Учетная запись UNet обеспечивает доступ к информационным ресурсам, которые предоставлены внешним пользователям. На рис.1 показана схема использования учетных записей в КИИС вуза.

В корпоративной вычислительной сети организованы домены, соответствующие двум основным группам пользователей – студенты (Stud) и сотрудники (Empl). Деление на домены может быть организовано и по-

другому принципу, например, в соответствии с организационной структурой [3].

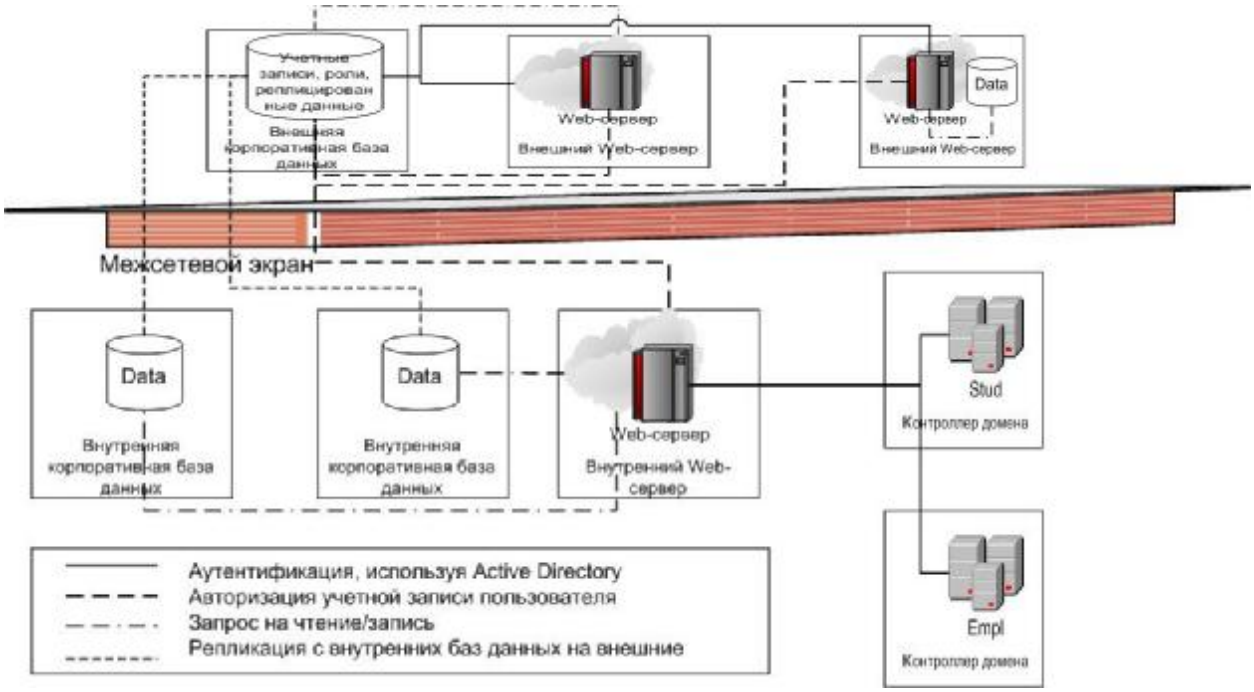

Рис.1. Схема использования учетных записей в КИИС вуза

Доступ в корпоративную сеть, к файловым серверам, к корпоративным базам данных и к внутреннему порталу осуществляется в два этапа. Аутентификация выполняется на базе учетных записей доменов Stud или Empl. Авторизация выполняется на основе системы управления правами, данные которой хранятся в базе данных, расположенной за межсетевым экраном. Доступ к внешним серверам вуза осуществляется на основе учетных записей UNet.

Для поддержания учетных записей и прав пользователей в КИИС вуза в актуальном состоянии подсистема актуализации использует информацию корпоративных баз данных, изменяет права пользователя, реализует новые связи и выполняет репликацию данных на внешние серверы.

2. Модели СЕРУПП

2.1. Логическая модель

Логическая модель СЕРУПП описывает основные понятия системы, связи и правила.

2.1.1. Проекты

Проект – это одно или несколько связанных между собой приложений КИИС, собирающих и анализирующих данные КИИС для автоматизации некоторого делового процесса. Каждый проект имеет несколько характеристик: название, описание, принадлежность к группе, начальный адрес URL (если он есть), признак доступности проекта в портале.

Описание проекта содержится в классе **Project** (рис. 2). СЕРУПП также является одним из проектов КИИС.

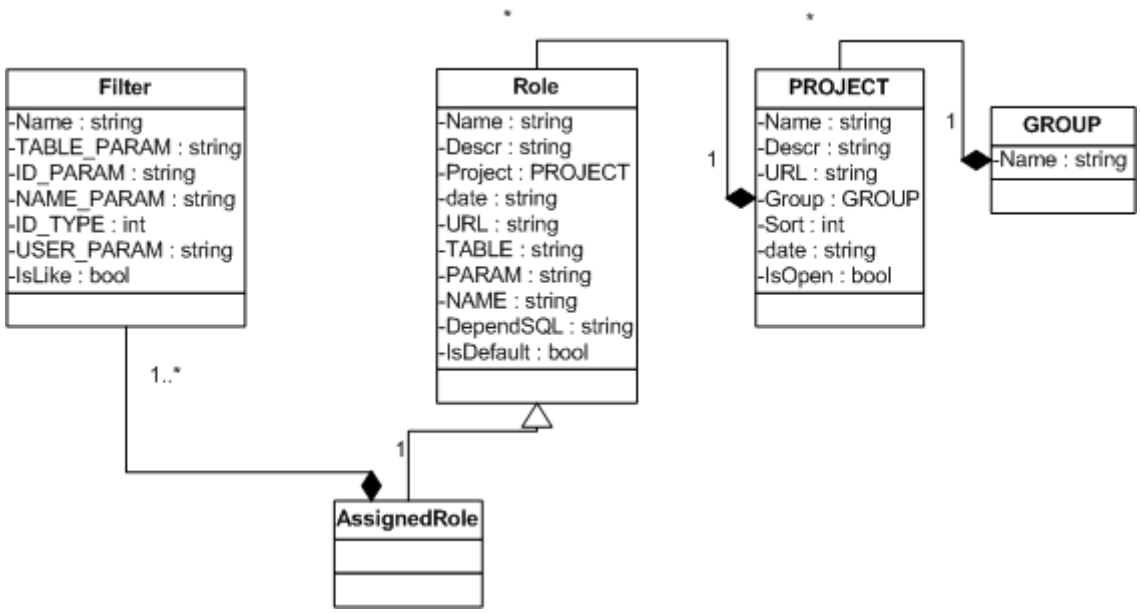

Рис.2. Диаграмма основных классов системы управления правами

2.1.2. Группы проектов

Все проекты КИИС вуза имеют целевое назначение и поэтому могут быть разбиты на группы (по назначению). Например, существуют группы образовательного блока, группа управления финансами, управления учебным процессом, личная информация и т.п. Группы формируются

администратором КИИС, исходя из концепции информационной среды. Для описания этих групп используется класс **Group** (рис.2). Группа проектов имеет атрибутом название.

2.1.3. Роль

В каждом проекте есть роли. Роль – это совокупность некоторых возможностей пользователя в рамках некоторого проекта. Описание роли содержит: название, описание, принадлежность проекту, дату создания, адрес URL для этой роли, если он отличается от основного адреса проекта, таблица базы данных (или представление), которое позволяет ограничить области видимости данных для роли, имя поля, которое используется в таблице для установления ограничений области видимости, имя поля, которое используется в таблице для отображения в приложении поля, запрос, который описывает зависимости между ролями (см. ниже описание зависимостей), признак возможности назначения роли автоматически по связи пользователя с областью видимости.

Описание роли хранится в классе **Role** (рис.2). В одних случаях роль может быть простой, т.е. не связанной ни с какой областью видимости. Например, в проекте «Цифровые учебные материалы вуза», студент получает доступ ко всем материалам без ограничений, на основании роли «Студент вуза». В других случаях роль может быть связана с некоторым набором данных, и при назначении роли пользователям необходимо ограничивать их некоторой частью этих данных.

2.1.4. Область видимости роли

Роль может иметь ограничения по области видимости. Например, в системе обмена документами, можно давать доступ пользователям к роли «Чтение документа» на объект документ «Договор на оказание услуг», что при назначении роли ограничивает ее область видимости только одним документом. Другой пример: роль директора института имеет ограничение

видимости данных по определенному институту. Ограничения по области видимости описываются в роли несколькими характеристиками:

- атрибутами таблицы, описывающей ограничения доступа (сервер, база данных, имя таблицы);
- параметром, который необходимо учитывать при ограничении области видимости (в текущей версии модели параметр только один, хотя с помощью представлений можно объединить более одного параметра);
- название параметра (для отображения его пользователям СЕРУПП).

2.1.5. Наследование прав и администрирование роли

Роли могут быть связаны отношениями наследования и администрирования роли. Если роль «А» наследуется от роли «В», то пользователи с ролью «В» имеют права пользователей с ролью «А». Роль «Администратор проекта» наследуется от роли «Главный администратор», что позволяет, всем пользователям, имеющим роль «Главный администратор», являться администраторами всех проектов КИИС. Роль «чтение документа» наследуется от роли «чтение типа документа», что фактически означает, что пользователь, имеющий роль «чтение типа документа», автоматически получает роль «чтение документа» с областью видимости всех документов данного типа. Поддерживается механизм множественного наследования.

Администрирование роли – это другой тип отношений, который позволяет тому, у кого есть некоторая роль «В», назначать пользователям роль «А», если роль «В» имеет администраторский доступ к роли «А». К роли «чтение документа» имеет администраторский доступ роль «Администратор документа». Таким образом, обеспечивается возможность пользователям с ролями «Администратор документа» давать другим пользователям право на чтение документа, присваивая им роль «чтение документа» с областью видимости конкретный документ.

2.1.6. Назначение роли

Правила назначения роли устанавливаются администратором проекта. Можно разделить три типа назначений:

1. простая роль назначается без каких-то ограничений по области видимости;
2. роль с ограничением по области видимости назначается автоматически пользователям из некоторой выборки на основании связи пользователей с областью видимости;
3. роль с ограничением по области видимости назначается пользователям из некоторой выборки на конкретную область видимости.

Рассмотрим примеры на все три типа назначений. Роль «студент» может не иметь ограничений по области видимости в некотором проекте и должна быть назначена на основании того, что пользователь является студентом. Роль «зав. кафедрой» должна иметь ограничения по области видимости – кафедра, и может быть назначена автоматически всем зав. кафедрами, так как их можно связать с их кафедрой на основании информации о пользователе в корпоративной базе данных персонала. Роль «зам. зав. кафедрой по работе со студентами» имеет ограничения по области видимости – кафедра, и не может быть назначена сразу на все кафедры. Роль может быть назначена тому преподавателю, который исполняет обязанности зам. зав. кафедрой в части работы со студентами. Информация о связи преподавателя с такими функциональными обязанностями в базе данных персонала отсутствует, поэтому такая роль должна быть назначена только вручную для каждой отдельной кафедры.

При назначении роли определяется период действия, т.е. доступ к некоторому ресурсу КИИС устанавливается на определенный период времени (возможно, неограниченный). Например, доступ к учебно-методическим материалам вуза может быть выдан внешнему пользователю на ограниченный период времени, после которого система удалит назначение этой роли на данного пользователя.

До сих пор речь шла о назначении роли со статусом «Разрешено». Но роль может быть назначена со статусом «Запрещено». Отсутствие назначения некоторой роли автоматически означает запрет на данный ресурс, тем не менее, в некоторых проектах требуется запретить доступ к ресурсу явным образом (пример такого проекта приведен в последней части работы). Поэтому при назначении роли имеется возможность назначить явный запрет этой роли некоторой выборке пользователей.

При определенном условии одному и тому же пользователю одна и та же роль с одной и той же областью видимости может быть назначена со статусом и «разрешено» и «запрещено». Правило выбора результирующего назначения следующее:

1. решение принимается на основании периода назначения, если периоды не перекрываются, то противоречия не возникает;
2. при перекрывающихся периодах результирующим будет последнее по дате назначение.

2.1.7. Фильтр

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/пользователь web-служб/пользователь приложений), работы в некотором подразделении, работы в подразделении из некоторой группы (пример, учебные подразделения), обучения в учебной группе, в некотором институте, на некоторой кафедре, и на основании того, что это - заданный пользователь.

Категории, которые позволяют выделять пользователей для назначения им прав, названы фильтрами. Для описания фильтра используются атрибуты: название фильтра, результирующая таблица, описывающая ограничения

фильтра, (например, для фильтра выбор сотрудников по подразделению, используется таблица подразделений), при этом может храниться не название таблицы, а SQL запрос ее генерирующий, поле таблицы, по которому выполняется ограничение, название параметра, поле, которое описывает зарегистрированного пользователя КИИС, используемое при выборе фильтра, категория пользователя, признак того, разрешено ли вложение подразделений (выбор сотрудников не только текущего подразделения, но и вложенных, может относиться так же и к ролям должностей и подразделений и к должностям).

При назначении роли используются фильтры, которые могут накладываться по «И» и по «ИЛИ». Наложение по «И» создают группу «согласованных» фильтров, которые могут объединяться по «ИЛИ» для создания общего списка пользователей. Например, роль декана должна получится из объединения по «И» фильтров по группе должностей (руководители) и по группе подразделений (Институты). В результате

Декан = Руководитель «И» Институт

Но поскольку некоторые деканы закреплены за подразделением из группы Деканат, то нужно добавить по «ИЛИ» еще одну группу согласованных фильтров: группа должностей (руководитель) и группа подразделений (Деканат). Таким образом,

Декан=(Руководитель«И» Институт)«ИЛИ»(Руководитель«И» Деканат)

Если при назначении требуется выбрать всех деканов кроме декана некоторого института, то для этого декана данная роль устанавливается дополнительно со статусом «Запрещено».

2.2. Математическая модель СЕРУПП

Определим СЕРУПП как совокупность абстракций – пользователи проекта, проекты КИИС, роли проекта, собственно данные, доступ к которым осуществляется с использованием проектов, фильтры, которые обеспечивают выделение подмножества пользователей, могут

комбинироваться по правилу «И» или «ИЛИ», и при наложении на них ролей ограничены периодом действия.

Определим СЕРУПП как $G = \{U, P, R, D, F, E\}$. Множество пользователей КИИС вуза $U = \{u_n\}_{n=1}^{N}$, N – число пользователей информационных ресурсов КИИС. Можно отметить, что пользователями КИИС могут быть не только субъекты системы (т.е. сотрудники, студенты, внешние пользователи), но и некоторые приложения, которые через СЕРУПП получают доступ к другим приложениям (чаще всего приложениям среднего слоя).

Множество проектов КИИС $P = \{p_k\}_{k=1}^{K}$, программные средства доступа к информации, управления, и анализа данных.

Множество ролей k—го проекта $R_k = \{r_{kj}\}_{j=1}^{J_k}$ - совокупность правил поведения с некоторыми данными в k –ом проекте.

Для каждого проекта можно выделить доступное ему множество данных D_k. Объединение множеств данных всех проектов представляет собой общее множество данных КИИС вуза.

$$D = \bigcup_{k=1}^{K} D_k \qquad (1)$$

Пересечение множеств D_k не пусто, так как в интегрированной информационной среде различные проекты используют одни и те же данные.

Для каждой роли r_{kj} возможно выделение подмножества данных $\{d_{kj}^m\}_{m=1}^{M_{kj}}$, определяющих область видимости для пользователя, которому назначена роль r_{kj}. Объединение всех областей видимости для всех ролей проекта представляет собой множество данных проекта

$$D_k = \bigcup_{j=1}^{J_k} \bigcup_{m=1}^{M_{kj}} d_{kj}^m , \qquad (2)$$

пересечение областей видимости не является пустым $\bigcap_{j=1}^{J_k} \bigcap_{m=1}^{M_{kj}} d_{kj}^m \neq 0$.

Подставляя (2) в (1), получим общее множество данных КИИС вуза

$$\bigcup_{k=1}^{K}\bigcup_{j=1}^{J_k}\bigcup_{m=1}^{M_{kj}} d_{kj}^{m} = D. \qquad (3)$$

Множество фильтров, позволяющих выделять некоторое подмножество множества пользователей $F = \{f_l\}_{l=1}^{L}$.

Множество назначений роли $E = \{e_{kj}^{nm}\}$ на области данных d_{kj}^{m}, которое определяется

$$e_{kj}^{nm} = \begin{cases} 1 - \textit{если роль } r_{kj} \textit{ (} j - \textit{ая роль в } k - \textit{ом проекте) назначена} \\ \quad n - \textit{ому пользователю на } m - \textit{ом множестве данных} \\ 0 - \textit{если роль } r_{kj} \textit{ не назначена } n - \textit{ому пользователю} \\ -1 - \textit{если роль } r_{kj} \textit{ запрещена } n - \textit{ому пользователю} \end{cases}. \qquad (4)$$

Как видно из определений, общее число назначений ролей пользователям КИИС равно

$$L = \sum_{k=1}^{K}\sum_{j=1}^{J^k}\sum_{m=1}^{M^{(kj)}} 1 \times N.$$

Для КИИС среднего вуза – 15 тыс. пользователей, 30 проектов, по 5 ролей, с 10 областями данных, число назначений L=22,5 млн. Создание и сопровождение такого количества назначений возможно только автоматически.

Рассмотрим назначение ролей. Назначение простой роли пользователю выполняются следующим образом.

1. Выделяется подмножество пользователей, которым следует назначить роль, с помощью фильтра

$$U_l^i = \left(U \;\hat{\mathbf{I}}\; f_l^t\right), \qquad (4)$$

где операция $\hat{\mathbf{I}}$ - определяет наложение фильтра на множество пользователей, t - определяет параметр фильтра, используемый при наложении.

2. Так как при назначении ролей может использоваться несколько фильтров, соединенных по «И», то соотношение (4) имеет следующий вид

$$\hat{U}_1 = \bigcap_{l \in L}\left(U \;\hat{\mathbf{I}}\; f_l^{t_l}\right) = \left(U \;\hat{\mathbf{I}}\; f_{ll}^{t_{ll}}\right)\hat{\mathbf{I}}\bigcap_{l \in L} f_l^{t_l}, \qquad (5)$$

где f_{ll} - один из накладываемых по «И» фильтров (обычно первый). $\hat{U}_1$ - это один согласованный фильтр, который используется при назначении.

3. Так как согласованные фильтры могут быть объединены по «ИЛИ», то соотношение (5) перепишется следующим образом

$$\hat{U} = \bigcup_{i=1}^{I} \hat{U}_i \ , \tag{6}$$

где I - число объеденных по «ИЛИ» согласованных фильтров. Соотношение (6) определяет множество всех пользователей КИИС, которым должна быть назначена простая роль r_{kj}

4. Роль r_{kj} без ограничений по области видимости назначается множеству пользователей $\hat{U}$

$$r_{kj} \oplus \hat{U} = \left\{ e_{kj}^{n} \right\}_{u_n \in \hat{U}} . \tag{7}$$

Символом $\oplus$ мы определяем связь между ролью и пользователями.

Опишем назначение роли с определенной областью видимости.

1. Соотношение (6) так же как и в предыдущем случае описывает выбор пользователей, для которых выполняется назначение.
2. Роль r_{kj} с ограничением области видимости d_{kj}^{m} назначается множеству пользователей $\hat{U}$

$$\left(r_{kj} \Theta d_{kj}^{m} \right) \oplus \hat{U} = \left\{ e_{kj}^{nm} \right\}_{u_n \in \hat{U}} . \tag{8}$$

Символ Θ определяет связь между ролью и областью видимости. Подставив (6) в (8), получим множество назначенных прав пользователей для назначения роли с определенной областью видимости

$$\left(r_{kj} \Theta d_{kj}^{m} \right) \oplus \bigcup_{i=1}^{I} \hat{U}_i = \bigcup_{i=1}^{I} \left(\left(r_{kj} \Theta d_{kj}^{m} \right) \oplus \hat{U}_i \right) = \left\{ e_{kj}^{nm} \right\}_{u_n \in \bigcup_{i=1}^{I} \hat{U}_i} . \tag{9}$$

В соотношении (9) роль назначается только тем пользователям, которые вошли в множество, полученное в результате объединения выборок пользователей, сформированных из пересечения наложенных на все множество пользователей фильтров с некоторым значением параметра фильтра.

Назначение роли с ограниченной областью видимости в зависимости от связи пользователя и области видимости определяется следующим образом.

1. Соотношение (6) описывает то множество пользователей, из которых будут выбираться пользователи, связанные с областью видимости на основании некоторого условия.
2. Условие связи пользователей и областей видимости описывается фильтром с параметром соответствующим области видимости. Таким образом, для каждой области видимости d_{kj}^{m} множество пользователей выбирается по $\hat{U}\ \hat{\mathbf{I}}\ f_l^m$.
3. Назначение описывается следующим соотношением

$$\left\{\left(r_{kj}\Theta d_{kj}\right)\oplus\left(\hat{U}\ \hat{\mathbf{I}}\ f_l^m\right)\right\}_{m=1}^{M_{kj}}=\left\{\left\{e_{kj}^{nm}\right\}_{u_n\in\hat{U}}\right\}_{m=1}^{M_{kj}}. \qquad (10)$$

Результирующим будет множество назначений некоторой роли по всем ее областям видимости. Подставляя (6) в (10), получим результирующее отношение для автоматического назначения ролей без определения области видимости

$$\left\{\left(r_{kj}\Theta d_{kj}\right)\oplus\left(\bigcup_{i=1}^{I}\hat{U}_i\ \hat{\mathbf{I}}\ f_l^m\right)\right\}_{m=1}^{M_{kj}}=\left\{\left\{e_{kj}^{nm}\right\}_{u_n\in\bigcup_{i=1}^{I}\hat{U}_i}\right\}_{m=1}^{M_{kj}}. \qquad (11)$$

Различные назначения одной и той же роли с одной и той же областью видимости данных на одного пользователя возможны при использовании различных фильтров, соединенных по «ИЛИ». При этом результирующее назначение определяется как результат операции наложения назначений (таблица 1., операция $\wedge$). Определим так же в этой таблице, используемые в дальнейшем операции агрегации $\vee$, поиск противоречия $\neg$, поиск избыточности $\div$.

Таблица 1. Операции над назначениями

Оп1	Оп 2	Оп1 $\wedge$ Оп2	Оп1 $\vee$ Оп 2	Оп1 $\neg$ Оп 2	Оп1 $\div$ Оп 2
1	1	1	1	1	0
1	0	1	1	0	0
1	-1	-1	1	0	1

0	-1	-1	0	0	0
0	0	0	0	0	0
0	1	1	1	0	0
-1	1	1	1	0	1
-1	-1	-1	0	1	0
-1	0	-1	0	0	0

Как видно из таблицы 1, операция наложения назначений не коммутативна. Если первой была операция запрет, а второй - разрешение, то приоритет имеет разрешение, и наоборот, если первой было разрешение, а вторым запрет, то приоритет имеет запрет. Состояние «не назначена» всегда имеет меньший приоритет, чем разрешение и запрет, в независимости от порядка следования. Результирующее назначение прав пользователя, по которому СЕРУПП допустит пользователя u_n к проекту p_k с ролью r_{kj} в область видимости d_{kj}^m определяется соотношением

$$\tilde{e}_{kj}^{nm} = \bigwedge_{i=1}^{I} e_{kj}^{nm}. \qquad (12)$$

Наложение происходит по всем, используемым в назначении, согласованным фильтрам (6).

В КИИС должен существовать такой фильтр, по крайне мере один, что наложение его на множество пользователей со всеми возможными параметрами даст полное множество пользователей КИИС вуза.

$$U = \bigcup_{m=1}^{Max_l} \left(U \;\hat{\mathbf{I}}\; f_l^m \right)$$

Такой фильтр f_l - необходим, чтобы назначать некоторые проекты КИИС в публичный доступ. Примером такого фильтра может быть фильтр по категориям пользователей – сотрудник/студент/внешний пользователь/отчисленный студент/уволенный сотрудник/приложение/web-служба.

Для повышения эффективности управления правами пользователей КИИС администраторам проектов и главному администратору КИИС необходимо учитывать различные характеристики.

Матрица связи пользователя u_n с проектом p_k определяется соотношением

$$\left\{e_k^n\right\} = \bigvee_{j=1}^{J_k} \bigvee_{m=1}^{M_{kj}} \tilde{e}_{kj}^{nm}, \tag{13}$$

$$e_k^n = \begin{cases} 1, n-ый\ пользователь\ имеет\ права\ в\ k-ом\ проекте \\ 0, n-ый\ пользователь\ не\ имеет\ прав\ в\ k-ом\ проекте \end{cases}$$

Операция агрегации назначений определена в таблице 1 (операция $\vee$). Из соотношения (13) можно определить абсолютное и относительное число пользователей p_k-го проекта, которое может служить одним из критериев оценки востребованности проекта

$$H_k = \sum_{n=1}^{N} e_k^n = \sum_{n=1}^{N} \bigvee_{j=1}^{J_k} \bigvee_{m=1}^{M_{kj}} \tilde{e}_{kj}^{nm},\ V_k = \frac{H_k}{N} \times 100\%. \tag{14}$$

В работающем проекте КИИС необходимо, чтобы все роли были назначены по крайне мере одному пользователю. Отсутствие назначение роли пользователю свидетельствует либо о том, что некоторая работа не будет выполнена, либо о том, что проект разработан некорректно. Для определения наличия назначения роли r_{kj} по крайне мере на одного пользователя используется выражение

$$e_{kj} = \bigvee_{n=1}^{N} \bigvee_{m=1}^{M_{kj}} \tilde{e}_{kj}^{nm} \tag{15}$$

Если e_{kj} равна 1, то роль r_{kj} назначена хотя бы одному пользователю КИИС. Число пользователей некоторой роли определяется следующим соотношением

$$h_{kj} = \sum_{n=1}^{N} \bigvee_{m=1}^{M_{kj}} \tilde{e}_{kj}^{nm} \tag{16}$$

При автоматическом анализе КИИС вуза на корректность назначения ролей данный параметр может быть индикатором востребованности роли.

Для этого возможно использовать относительный показатель (число пользователей роли r_{kj} в проекте p_k) $h_{kj}/H_k \times 100\%$.

Еще одним важным показателем корректности назначения ролей является показатель использования области видимости

$$e_{kj}^m = \vee_{n=1}^{N} \tilde{e}_{kj}^{nm}. \quad (17)$$

Параметр e_{kj}^m равен 1, если роль r_{kj} с областью видимости d_{kj}^m назначена по крайне мере одному пользователю. Иначе, параметр e_{kj}^m равен 0. С помощью данного параметра можно автоматически отслеживать те области видимости, которые оказались неохваченными в процессе назначения прав доступа или в процессе выполнения процедуры актуализации данных в результате увольнения (или перевода) сотрудников, которые отвечали за данные области.

В некоторых случаях в результате, например, ошибочных назначений, или в силу наследования ролей, пользователям может быть установлено избыточное назначение прав или противоречивость прав. К последнему относится одновременное назначение одному и тому же пользователю одной и той же роли с одной и той же областью видимости, со статусами «Запрещено» и «Разрешено». Как разрешается это противоречие определено в таблице 1, операция $\wedge$, но может оказаться, что при назначении противоречивых прав администратор не учел порядок следования фильтров. Для этого возможно составления отчетов по противоречивым правам.

Для поиска противоречивых прав определим операцию поиск противоречия, признак противоречия 0, так как в этой операции назначены могу быть только разрешения (1) и запрещения (-1) (таблица 1, операция $\neg$).

Как видно из таблицы 1 параметр устанавливается в 0 и сохраняется при дальнейшем выполнении операции по всем назначенным фильтрам, как только встречается первое противоречивое назначение

$$e'^{nm}_{kj} = \neg_{l \in L} e_{kj}^{nm}$$

При отсутствии противоречивости назначения параметр установлен в 1.

Избыточность назначений возникает тогда, когда одному и тому же пользователю назначена одна и та же роль по одной и тоже области данных. Определить избыточность можно следующим образом.

Как видно из таблицы 1 параметр избыточности $\div$ устанавливается в 0 и остается неизменным для всех дальнейших фильтров, как только встретится первая избыточность

$$e''^{nm}_{kj} = \div \underset{l \in L}{e^{nm}_{kj}} .$$

В целом, наличие нескольких назначений одному и тому же пользователю одной и той же роли по одной и той же области видимости всегда означает или противоречивость или избыточность.

Для контроля управления доступом интерес может представлять так же ранжирование пользователей по объему доступа к информационным ресурсам. Определим операцию доступности ресурса (таблица 2).

Таблица 2. Доступности ресурса

Операнд	$\forall$ Операнд
1	1
0	0
-1	0

Тогда общий объем доступных пользователю областей видимости по всем ролям всех проектов КИИС определяется по следующему соотношению в абсолютном

$$Y_n = \sum_{k=1}^{K} \sum_{j=1}^{J_k} \sum_{m=1}^{M^{kj}} \forall \tilde{e}^{nm}_{kj}$$

или относительном виде

$$y_n = \frac{Y_n}{\sum_{k=1}^{K} \sum_{j=1}^{J_k} \sum_{m=1}^{M^{kj}} 1} \times 100\% .$$

Высоким этот показатель должен быть для тех пользователей, у кого в соответствие с должностными обязанностями, имеются широкие полномочия в КИИС вуза.

Роли могут наследоваться. Если роль r_{kj} наследуется от r_{ki} ($r_{ki} \to r_{kj}$), то

$$\left\{e_{kj}^{nm_j}\right\}_{m_j=M_i^{kj}}^{M_{i+1}^{kj}} = e_{ki}^{nm_i},, \; m_i \in M_{ki}, \quad M_{kj}^{i}, M_{kj}^{i+1} \in M_{kj} \tag{18}$$

Т.е. назначение некоторой базовой роли с одной областью видимости может привести к назначению производных ролей с одной или несколькими областями видимости.

2.3. Информационная модель СЕРУПП

В СЕРУПП есть три роли: главный администратор КИИС, администратор проекта, администратор роли.

Роль «Главный администратор» создается вручную, так как только главный администратор может создать новый проект, в том числе, проект СЕРУПП, который обеспечит создание любой роли. Роль «Главный администратор» – простая, назначить и удалить ее можно в СЕРУПП.

Роль «Администратора проекта» позволяет создавать и редактировать роли в определенном проекте, создается вручную, так как создание любой роли – это функция «Администратора проекта». Роль «Администратор проекта» не может быть назначена автоматически, назначается только «Главным администратором», имеет ограничения по области видимости - проекты.

Роли «Администратор проекта» и «Главный администратор» связаны отношением наследования. «Администратор проекта» наследуется от «Главного администратора», что приводит к тому, что все «Главные администраторы» КИИС имеют роль «Администратор проекта» для всех проектов КИИС.

Роль «Администратор роли» дает право назначать некоторую роль пользователям, имеет ограничения области видимости – определенную роль. «Администратор роли» не имеет права на создание, удаления и

редактирования роли, но имеет права на назначение роли. Роли «Администратор роли» и «Администратор проекта» связаны отношением наследования. «Администратор проекта» имеет функции «Администратора роли» на все роли своего проекта.

2.4. Функциональная модель СЕРУПП

Система СЕРУПП позволяет

1. Регистрировать пользователей в КИИС вуза, создавая две учетные записи: в AD и UNet.
2. Создавать персональные каталоги и каталоги подразделений на файловых серверах сотрудников и студентов и устанавливать на них разграниченный доступ.
3. Определять учетные записи AD в группы, соответствующие месту работы пользователя, его должности и типу должности.
4. Создавать проекты КИИС вуза.
5. Создавать роли в проекте и определять параметры роли, в том числе параметр области видимости, тип назначения.
6. Задавать зависимости между ролями.
7. Задавать правила назначения роли, используя фильтры и устанавливая период действия и статус назначения.
8. Автоматически генерировать назначение роли на основании правил.
9. Поддерживать данные о правах пользователей КИИС в актуальном состоянии.
10. Поддерживать в актуальном состоянии каталоги на файловых серверах.
11. Поддерживать в актуальном состоянии вхождение учетных записей AD в соответствующие группы.
12. Вычислять различные характеристики, описанные в математической модели СЕРУПП.

Процедура актуализации СЕРУПП один раз в сутки выполняет актуализацию прав пользователей на основании данных о них в

корпоративных базах данных и выполняет все изменения прав пользователя, которые можно выполнить на основании правил назначения ролей.

3. СЕРУПП ВГУЭС

Концепция развития КИИС ВГУЭС может быть охарактеризована как интеграция технологий, приложений, функций и данных. Объединение систем вокруг единой концепции, выделение общих частей с единой реализацией и реализация специфики гетерогенными средствами – это основа развития КИИС ВГУЭС.

Все проекты, разрабатываемые в КИИС ВГУЭС, опираются на СЕРУПП. На СЕРУПП переведены и многие унаследованные приложения, которые были разработаны задолго до СЕРУПП. В настоящий момент в КИИС ВГУЭС содержит около 40 проектов, из которых 30 настроены на СЕРУПП.

Использование СЕРУПП значительно упрощает управление КИИС и разработку новых проектов. В этой части работы приведем примеры различного использования СЕРУПП.

3.1. Система доступа в Интернет

Доступ в Интернет во ВГУЭС осуществляется через прокси-сервер squid, настроенный с помощью программного обеспечения Samba, на учетные записи AD. В AD есть несколько групп, вхождение в которые учетной записи, обеспечивает выход пользователя в Интернет. Там же существует группа, вхождение в которую запрещает выход пользователя в Интернет.

Доступ в Интернет осуществляется на основании ограничений трафика пользователя. Для различных категорий пользователей определены различные объемы допустимого трафика.

В СЕРУПП создан проект «Интернет», в котором определена роль «Доступ в Интернет», имеющая область видимости – размеры доступного трафика. Администратор прокси-сервера, которому определена роль

«Администратор проекта» с областью видимости проект «Интернет», назначает роль «Доступ в Интернет» с определенным объемом трафика, различным категориям пользователей. Например, для руководителей учебных подразделений (деканы и заведующие кафедрами) назначено ограничение в 150 Мб/месяц.

Приложение проекта «Интернет» ведет журнал использованного трафика пользователя и при превышении положенного лимита пользователю автоматически назначается роль «Доступ в Интернет» со статусом «Запрещено» до конца определенного периода (обычно текущего месяца). Кроме этого, приложение проверяет наличие у пользователей ролей со статусом «Запрещено» и записывает таких пользователей в группу AD, вхождение в которую обеспечивает запрет на использование Интернет. Те пользователи, которые входят в эту группу AD, но не имеют назначения со статусом «запрещено», удаляются приложением из группы.

СЕРУПП проверяет назначения прав пользователей и по окончанию срока действия назначения удаляет данное назначение у пользователя, что приводит к возможности вновь использовать Интернет по окончанию периода.

Использование СЕРУПП, которое взяло на себя значительную часть работы системы доступа в Интернет на основе ограничения трафика, позволило создать систему доступа в Интернет за 2 дня.

3.2. Создание обобщенных адресов

СЕРУПП может использоваться как базовая система для других систем, с помощью нее могут быть решены вопросы, на первый взгляд, не связанные с назначением прав. Примером такой системы может быть сервис рассылок, или точнее один из его модулей – создание обобщенного почтового ящика. Обобщенный почтовый ящик – это набор адресов некоторых пользователей с общим именем. В рамках вуза в обобщенные адреса должны входить адреса пользователей, выбранные по определенным

правилам. Все эти правила описаны в СЕРУПП. Таким образом, роль «Вхождение в адрес», должна быть присвоена некоторой выборке пользователей, используя фильтры с ограничением области видимости – конкретный обобщенный адрес.

Программа системы «Создания обобщенных адресов» проверяет наличие у пользователей роли «Вхождение в адрес» и по области видимости (определенному адресу) создает на почтовом сервере «алиас» для тех электронных почтовых адресов, которые связанны с пользователями КИИС, имеющими данное назначение.

3.3. Система успеваемости

Система успеваемости студентов вуза автоматизирует процесс контроля успеваемости от создания электронной ведомости, до выставления оценок (баллов для рейтинговой системы) и подписи всеми участниками (преподавателем, зав. кафедрой, деканом). Отчеты по успеваемости по определенным областям видимости доступны для сотрудников кафедр, деканатов, учебного управления и, конечно, для самих студентов.

В СЕРУПП создан проект «Успеваемость» с ролями «Студент», «Преподаватель», «Заведующий кафедрой», «Декан», «Сотрудник деканата», «Заместитель декана», «Сотрудник кафедры».

Простая роль «Студент» назначается всем студентам вуза, опираясь на фильтр, выделяющий пользователей по категориям пользователей. Роль «Преподаватель» имеет ограничения по области видимости – кафедра, при этом такое назначение можно сделать автоматически по всем кафедрам, так как в базе корпоративных данных существует связь преподавателя и кафедры. То же самое касается и роли «Заведующий кафедрой», «Сотрудник кафедры», «Декан», «Сотрудник деканата» за исключением того, что для выделения пользователей используются различные фильтры и областью видимости в последних двух случаях являются институты. Роль «Заместитель декана» имеет область видимости институт и должна

назначаться с привязкой к области видимости, т.е. роль назначается с учетом определенного института. Для сотрудников учебного управления выдаются права «Сотрудников деканата», но с несколькими областями видимости (для каждого института).

4. Заключение

Одной из ключевых задач создания эффективной информационной среды является автоматизация управления доступом к информационным ресурсам и сервисам, на которые переносятся процессы, обеспечивающие непосредственную деятельность вуза. Если говорить об учебном процессе и управлении в вузе, то для них информационные технологии и аппаратно-программное обеспечение являются основным средством, которое позволит создать преимущества в конкурентной среде. В этой связи становится особенно важной задача обеспечения управляемости и доступности всего комплекса информационных ресурсов и сервисов, а также определение соответствия ИТ-инфраструктуры стратегическим целям вуза. Комплексное управление ключевыми информационными ресурсами и сервисами позволит обеспечить работу информационной инфраструктуры вуза в соответствии с действующей организационной структурой и принятыми бизнес-правилами.

Ввод в эксплуатацию СЕРУПП в 2003 году позволил ВГУЭС существенно повысить эффективность управления доступом к информационным ресурсам и упростить администрирование применяемых приложений и сервисов.

Литература

1. Shakhgeldyan C., Kryukov V.. Integration of University Information Resources into the Unified Information Environment//Proceedings of the 10-th International Conference of European University Information Systems (ENUS 2004). Slovenia, 2004. – pp. 321-327.

2. Крюков В.В., Шахгельдян К.И. Проблемы интеграции данных и унификации доступа к приложениям в единой информационной среде вуза// Труды XI Всерос. н.-метод. конф. «Телематика-2004», Т.1, СПб., 2004.

3. Крюков В.В., Шахгельдян К.И. Типовые организационные и технологические решения для создания региональной информационной среды вуза и филиалов //Открытое образование. – 2004. – №5. с. 38-52

4. Крюков В.В., Шахгельдян К.И. Развитие информационной инфрастуктуры вуза для решения задач управления // Университетское управление. – 2004. – №4. – с.67–77.

5. Гмарь Д.В., Крюков В.В., Майоров В.В., Шахгельдян К.И. Единая система регистрации и управления доступом к информационным ресурсам вуза//Труды Всероссийской научной конференции Научный сервис в сети Интернет. – Новороссийск. –2003. – с. 135–138.

6. Крюков В.В., Шахгельдян К.И. Формирование корпоративной информационной среды вуза // Труды Межд. конгресса «Информационные технологии в образовании». – М., Просвещение, 2003.

7. Гайдамакин Н.А. Количественные характеристики и методы анализа индивидуально-группового разграничения доступа к компьютерным системам//НТИ Сер.2. Информационные процессы и системы.– 2003.– №4.– с. 16-24.