

УДК 004.78:351.85

*М.А. Вышиванов, Д.В. Гмарь, В.А. Князев, К.И. Шахгельдян*

## ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ В КОРПОРАТИВНУЮ ИНФОРМАЦИОННУЮ СРЕДУ ВУЗА

*Вышиванов М.А.* – вед. программист отдела информационных сервисов и корпоративных приложений ВГУЭС

*Гмарь Д.А.* – вед. программист отдела информационных сервисов и корпоративных приложений ВГУЭС

*Князев В.А.* – вед. программист отдела информационных сервисов и корпоративных приложений ВГУЭС

*Шахгельдян К.И.* – доцент, к.т.н., начальник отдела информационных сервисов и корпоративных приложений ВГУЭС

### **Введение**

Корпоративная информационная среда (КИС) вуза может быть построена на основе либо единого, например, ERP-решения, либо с помощью технологий интеграции.

В последние годы все чаще КИС строится на базе нескольких решений, где одним из составляющих может быть и решение класса ERP.

Среди технологий интеграции можно выделить направления

1. интеграции данных;
2. интеграции приложений;
3. интеграции пользователей;
4. интеграции бизнес-процессов.

Интеграция данных объединяет несколько подходов – репликация данных, логическая интеграция на лету и агрегированные хранилища данных. Интеграция приложений подразумевает передачу сообщений между различными приложениями и генерацию и обработку событий в приложениях. Интеграция пользователей позволяет использовать одну учетную запись пользователя во многих системах. Интеграция бизнес-процессов реализует формирование сквозных бизнес-процессов, часть из которых реализуется в одной системе, а часть – в другой.

Жизненный цикл КИС достаточно длительный, в некотором смысле бесконечный, так как устаревшие системы заменяются на новые, реализуются новые функциональности в рамках работающих систем и внедряются новые информационные системы, которые могут быть разработаны сторонними компаниями.

Предметом доклада является обсуждение вопросов внедрения сторонних информационных систем в КИС, построенную на принципах интеграции.

### **Интеграция на уровне пользователей**

Интеграция на уровне пользователей корпоративной информационной среды (КИС) предполагает использование одних и тех же учетных записей в различных системах. Для таких целей могут использоваться учетные записи сервера каталогов, например, LDAP-серверов Active Directory, e-Directory и т.п. Могут так же использоваться учетные записи, которые хранятся в некоторой базе данных.

В КИС ВГУЭС 6 лет работает система единой регистрации и управления правами пользователей [1], которая обеспечивает создание и управление учетными записями сотрудников и студентов вуза в службе каталогов Active Directory (AD) и в таблицах базы данных.

КИС содержит проекты, у каждого из которых могут быть роли. Роли назначаются пользователям, имеют ограничения области видимости и могут быть назначены в автоматическом или ручном режиме. Модель управления правами КИС ВГУЭС базируется на RBAC-модели [2], но является ее расширением в область автоматизации управления правами, в связи с невозможностью управлять в вузе правами вручную.

Реализация интеграции на уровне пользователей зависит от приложения. Двухуровневые клиент-серверные приложения могут быть интегрированы практически без изменений, если выполнены следующие условия:

- установление свойств соединения с базой данных на наиболее удобный механизм аутентификации в СУБД, например, для MS SQL Server таким механизмом будет аутентификация на базе учетных записей AD;
- разработка процедуры синхронизации пользователей информационной среды и пользователей базы данных с автоматической генерацией ролей пользователю базы данных на основе ролей пользователя в КИС.

Для трехуровневых приложений интеграция в КИС может иметь различные формы, в зависимости от внутренней организации приложений. Рассмотрим проблему аутентификации, т.е. валидности имени и пароля.

Некоторые сторонние приложения могут допускать изменения кода, выполняющего аутентификацию пользователя. Тогда, чтобы интегрировать это приложение в КИС, код аутентификации заменяется на вызов метода специализированной веб-службы аутентификации.

Это означает, что в стороннем приложении пароли пользователей не хранятся, что позволяет избежать проблем безопасности.

Если стороннее трехуровневое приложение использует пользователей LDAP-сервера для доступа к системе, то эта проблема легко решается, так как в системе регистрации, предусмотрено создание учетных записей LDAP-сервера в КИС вуза при регистрации пользователя КИС. Если для этих целей используются различные LDAP-серверы, то между ними может быть настроена миграция, либо коммерческими системами (например, Tivoli), либо могут быть написаны несложные системы миграции учетных записей для определенных серверов.

Процедура авторизации несколько сложнее. Авторизация пользователей может выполняться в системе самым разным образом. Например, если унаследованное приложение работает с учетными записями LDAP-сервера, в этом случае такие системы имеют администраторский инструментарий, позволяющий давать права группам пользователей LDAP-сервера. Такие группы могут быть созданы автоматически на основании заданных прав пользователей в КИС и более того, права на группы тоже могут быть сгенерированы автоматически в сторонней системе.

Например, система управления контентом имеет административный инструмент, позволяющий давать права публикатора в рамках некоторого сайта определенным группам пользователей в LDAP-сервере. Тогда в КИС создается проект, соответствующий данной системе управления контентом и создается роль Публикатор с областью видимости – «сайт» из системы управления контентом (система управления правами может воспринимать таблицу сайтов системы управления контентом как источник данных, связанный отношением проекции с областью видимости для роли публикатор).

На основании этих данных система актуализации создает группы пользователей в службе каталогов (с названием, совпадающим с названием сайта) и заносит в группы LDAP-сервера тех пользователей, которым даны права в системе управления правами. Так как система управления контентом настроена на тот же LDAP-сервер, то администратор системы видит созданные группы и определяет им права для доступа на сайт. Возможен и другой вариант, когда сопоставление групп службы каталога и сайтов выполняется автоматически в системе управления контентом. Второй вариант предпочтителен, так как позволяет управлять правами автоматически. Так как система актуализации работает периодически (обычно раз в сутки), то все изменения в правах пользователя (увольнение, перевод,

отчисления) сразу скажутся на вхождении их в группу LDAP-сервере, и соответственно на правах пользователей в системе управления контентом.

Если сторонняя система не может работать с LDAP-сервером, но позволяет заменить функцию аутентификации, то возможен следующий вариант интеграции. Так как система имеет своих собственных пользователей, то должна быть настроена репликация между пользователями КИС и пользователями системы. Если система поддерживает модель RBAC, то в системе должно быть описано соответствие между пользователем, ролью и некоторым ограничением роли (аналог области видимости).

### **Интеграция на уровне данных**

Интеграция на основе данных предполагает обеспечение репликации данных, интеграции на лету и организации агрегированного хранилища данных.

Репликация данных организуется в случаях

1. Если данные располагаются на различных серверах, имеющих разную модель данных.
2. Если данные необходимы на различных серверах, расположенных часто либо удаленно друг от друга, либо разделены сетевым экраном.

Интеграция на лету организуется там, где требуется обеспечить логически интегрированные данные, т.е. в одном запросе выполняется обращение к нескольким разным базам данных.

Агрегированные хранилища обеспечивают анализ агрегированных данных из разных областей деятельности вуза. В хранилище данные попадают из разных систем.

В большинстве случаев на первом этапе внедрения информационной системы в КИС речь идет о репликации данных. В этом случае необходимо определить области пересечения данных. Для этих данных необходимо определить то приложение, которое является первоисточником.

1. Если внедряемое приложение определено как первоисточник пересекаемых данных, то, во-первых, должно быть запрещены функции в КИС, которые обеспечивали создание этих данных в других приложениях. Во-вторых, должна быть организована репликация в источники данных, которые соответствуют пересекаемым данным в КИС.
2. Если внедряемая система использует данные, первоисточниками которых являются действующие системы КИС, то, во-первых, функция создания и редактирования

данных должна быть закрыта во внедряемой системе, во-вторых, должна быть либо организована репликация данных из КИС в источники данных внедряемой системы, либо организована интеграция данных на лету для приложений, их использующих.

Система управления понятиями КИС ВГУЭС [3] позволяет создавать недостающие данные, если при внедрении сторонней системы, требуются данные, которых нет в КИС.

Например, при внедрении системы управления доступом в помещения вуза на основе идентификационных пластиковых карт требуется использование данных по помещениям вуза. Такого приложения в КИС вуза может и не быть. В этом случае с помощью системы управления понятиями создается понятие помещений и зданий (а также все необходимые сопутствующие понятия). Система управления понятиями позволяет не только создавать понятия и отношения между ними, но позволяет создавать и экземпляры понятий. В приведенном примере система управления понятиями может использоваться как система учета помещений вуза.

При использовании системы управления понятиями для создания недостающих данных должна быть организована репликация данных из системы управления понятиями во внедряемую информационную систему.

### **Интеграция приложений**

Интеграция приложений позволяет использовать бизнес-логику различных систем. Интеграция приложений осуществляется либо передачей сообщения либо с помощью генерации событий и их дальнейшей обработкой.

Интеграция приложений возможна там, где используется промежуточный слой для работы с данными, в том числе для выборки из базы данных, для обработки и для редактирования данных в базе данных.

Интеграция приложений может возникнуть, например, если внедряемое приложение имеет собственную систему аутентификации, которую необходимо заменить на аутентификацию КИС, для обеспечения интеграции на уровне пользователей.

В этом случае процедура аутентификации внедряемой системы заменяется на вызов метода веб-службы аутентификации и авторизации пользователей КИС.

В случае если внедряемая система имеет промежуточный слой с открытым интерфейсом это приложение должно быть зарегистрировано в КИС в виде серверной компоненты с описанием методов и параметров методов. Такая каталогизация позволяет другим

системам КИС использовать открытый интерфейс к внедряемой системе.

Если внедряемая система имеет возможность генерировать события, то такие события должны быть каталогизированы в КИС с той же целью, чтобы другие системы КИС могли среагировать на события, происшедшие во внедряемой системе.

### **Интеграция бизнес-процессов**

Интеграция бизнес-процессов подразумевает формирование составного процесса из различных частей, реализованных в различных приложениях.

При интеграции на уровне бизнес-процессов необходимо связать две системы, каждая из которых не знает ничего о другой системе, при этом автоматизируется процесс, который берет данные из одной системы, преобразует их согласно некоторым бизнес-правилам и генерирует данные в другую систему.

Примером такой интеграции могут быть интеграция процесса начисления стипендии. КИС имеет системы учета контингента студентов и успеваемости, а так же систему учета стипендии. Используя систему управления бизнес-процессами формируются бизнес-правила, на основании которых формируется стипендия с учетом успеваемости и дополнительных сведений о студентах. Для реализации полного бизнес-процесса к системе управления должны быть дописаны веб-службы извлечение информации о студентах и их успеваемости, формирования проекта приказов, сохранении стипендии в системе учета стипендии.

### **Заключение**

Интеграция на уровне пользователей КИС является обязательным условием построения КИС на базе интеграции. Без этого условия в КИС вуза, где большое число пользователей и большой процент обновляемости контингента, внедрение систем в вузе выполнить невозможно.

Интеграция на основе данных является обязательным, так как для интегрированной информационной среды необходимо, чтобы существовал единственный первичный источник одного понятия. Так как каждая информационная система использует некоторые данные и производит новые и при этом такие системы могут работать с разными СУБД, то, следовательно, необходимы процедуры репликации данных.

Интеграция приложений может являться обязательным, если ключевые функции, необходимые многим приложениям, выполняются с помощью сервисных компонентов.

Остальные формы интеграции являются желательным, но не обязательным условием построения интегрированной информационной среды вуза, особенно на первом этапе.

#### **Библиографические ссылки**

1. Шахгельдян К.И., Крюков В.В., Гмарь Д.В. Система автоматического управления доступом к информационным ресурсам вуза//Информационные технологии. 2006.-№2.-с.19-29.

2. Ferraiolo D., Kuhn R. Role-based access controls. In 15th NIST-NCSC National Computer Security Conference, pp. 554-563, Baltimore, MD, October 13-16 1992.

3. Крюков В.В., Шахгельдян К.И. Корпоративная информационная среда вуза: методология, модели решения. Монография//Владивосток: Дальнаука.- 2007.- 308 с.