К вопросу о получении доступа филиалов к информационным ресурсам вуза

Вышиванов М.А., Шахгельдян К.И.

Проект интеграции филиалов Владивостокского государственного университета экономики и сервиса (ВГУЭС) в гг. Находке и Артеме начался 1,5 года назад. Целью проекта является обеспечение доступа сотрудников и студентов филиалов ко всем ресурсам и сервисам, которые входят в корпоративную информационную среду (КИС) ВГУЭС. На текущий момент построена сетевая инфрастурктура, объединяющая ВГУЭС и филиалы, обеспечен доступ к телематическим сервисам (Интернет и электронная почта). В филиалах идет внедрение систем управление предприятием и учебным процессом. Для обеспечения доступа сотрудников и студентов филиалов, необходимо, чтобы они могли получать персонифицированный доступ на основе системы регистрации и управления правами пользователей КИС [1]. Вопросу разработки системы единой регистрации пользователей, включая пользователей филиалов, посвящен данный доклад.

Назначение системы состоит в автоматической регистрации студентов и сотрудников филиалов в КИС ВГУЭС для предоставления им доступа к ее внутренним ресурсам.

Архитектура КИС ВГУЭС базируется на службе каталогов Active Directory (AD) и включает 6 доменов, в том числе домены ВГУЭС (vvsu.ru, empl.vvsu.ru, stud.vvsu.ru, adm.vvsu.ru) и домены филиалов (artem.vvsu.ru, nakhodka.vvsu.ru). Домены empl.vvsu.ru и stud.vvsu.ru содержат учетные записи и компьютеры сотрудников и студентов ВГУЭС соответственно. Домен филиала содержит учетные записи и компьютеры сотрудников и студентов филиалов.

Автоматическая регистрация пользователя КИС ВГУЭС предполагает создание учетной записи в соответствующем пользователю домене, а так же учетной записи для доступа во внешний портал ВГУЭС. Если пользователь регистрируется в доменах empl.vvsu.ru или stud.vvsu.ru, то для него так же создаются личные каталоги на корпоративных файловых серверах.

Система регистрации сотрудников и студентов филиалов является частью распределенной системы регистрации ВГУЭС. Регистрация пользователя выполняться несколькими сервисами, которые работают на разных серверах, часть из которых расположена во внутренней сети ВГУЭС, а часть в демилиторизованной зоне (ДМЗ). В связи с этим интерфейс к системе регистрации расположен на двух веб-серверах: blackcat.vvsu.ru и reg.vvsu.ru. Сервер blackcat.vvsu.ru распложен в ДМЗ и доступен для внешней регистрации. Сервер reg.vvsu.ru доступен только внутри КИС и используется для регистрации пользователей, которые находятся в КИС. Для того, что упросить работу пользователям два DNS сервера по-разному воспринимают адрес reg.vvsu.ru. Внешний DNS переводит этот адрес в blackcat, а внутренний DNS сервер переназначает запрос на reg.vvsu.ru.

Регистрация пользователя филиала, находящегося в КИС ВГУЭС, включает несколько шагов (рис.):

1. Проверка пользователей на достоверность введенных данных – выполняется на сервере reg.vvsu.ru.
2. Обращение к клиенту сервисов регистрации (IRASClientRouter) через web-сервис.
3. Клиент сервиса регистрации определяет, к какому управляющему сервису регистрации (IRALDAPService) надо передать запрос. После выбора сервиса регистрации филиала ему предается управление. Сервис анализирует запрос и принимает решение о необходимости создание учетной записи пользователя и добавление ее в группы подразделений сотрудников или студентов филиала в AD. Для создания самой учетной записи, а также регистрации учетной записи в группах в AD используется IRALDAPService, управление которому и передаётся дальше.
4. Учетной записи устанавливаются логин и пароль, а также прописываются другая

информация, включая фамилию и имя.

5. Учетная запись заносится в те группы, которые определены по умолчанию для пользователя, работающего в данном подразделении, и имеющего данную роль. Если группа, в которую должна быть занесена учетная запись, еще не существует, то сервис создает группу и заносит туда учетную запись.
6. Учетная запись получает права определенные для нее по умолчаниию в зависимости от должности, которой занимает пользователь. В настоящий момент учитывается роли должности – руководитель подразделения и преподаватель. Руководитель подразделения заносится в определенную группу руководителей. Аналогичная группа существует для преподавателей.
7. В случае успешного создания учетной записи, и назначении прав, управление от сервиса IRAS передается web-сервису, который позволяет создать учетную запись зарегистрированных пользователей на сервере WebDB.

Если регистрация выполняется из вне КИС, то после пункта 1, сразу осуществляется переход на пункт 7. При этом учетная запись помечается, как не прошедшая регистрацию внутри КИС в AD. 1 раз в сутки, сервис IRAS обращается к сервису , который проверяет наличие таких записей, не прошедших регистрацию внутри. При наличии таких записей, для каждой из них выполняются все процедуры от 2 до 6. При успешной регистрации в AD, учетная запись на WebdDB помечается как успешно прошедшая регистрацию в AD.

Для поддержания данных в актуальном состоянии, раз в сутки на каждом из филиалов, а также во ВГУЭС, запускается процесс обновления данных. Центральным элементом этого процесса является IRADBServiceII, по одному экземпляру которого, должно быть установлено на каждом из филиалов, а также во ВГУЭС. Данный сервис работает в двух режимах. В одном он ожидает запросов от аналогичных сервисов, во втором он производит проверку учетных записей пользователей своего филиала. Для коммуникаций между экземплярами IRADBServiceII используется протокол TCP/IP через сокеты.

Рассмотрим вариант с проверкой из филиала, обслуживаемого экземпляром IRADBServiceII. Обозначим данный филиал как A

1. Для выбранного пользователя из базы данных (БД) извлекается список подразделений, принадлежащих A, в которых он числится.
2. Выполняется проверка, принадлежности учетной записи домену A. В случае положительного ответа, извлекается список групп, в которых числится учетная запись. Если у учетной записи в списке групп есть группы другого домена, то отправляется запрос на правомочность нахождения пользователя в этой группе к экземпляру IRADBServiceII, обслуживающему домен данной группы. Если учётная запись не в домене A, то запрашивается список групп от экземпляра IRADBServiceII, обслуживающего домен учетной записи.
3. При получении запроса о правомочности нахождения пользователя в определенной группе, выполняется запрос к БД, на предмет принадлежности пользователя подразделению, представленному группой.
4. После составления списка подразделений пользователя, на основании данных из AD и отбрасывания из него подразделений, не относящихся к домену A, выполняется сравнение его с аналогичным списком из БД. В случае обнаружения различий, выполняем добавление/удаление пользователя в/из требуемых подразделений.

IRADBServiceII также, содержит модуль актуализации членства пользователей в определенной группе в AD с соответствующей ролью в БД. Для примера он обеспечивает согласование списка членов группы Publicators и Teachers с ролями “Начальник” подразделения” и “Преподаватель” соответственно в филиале.

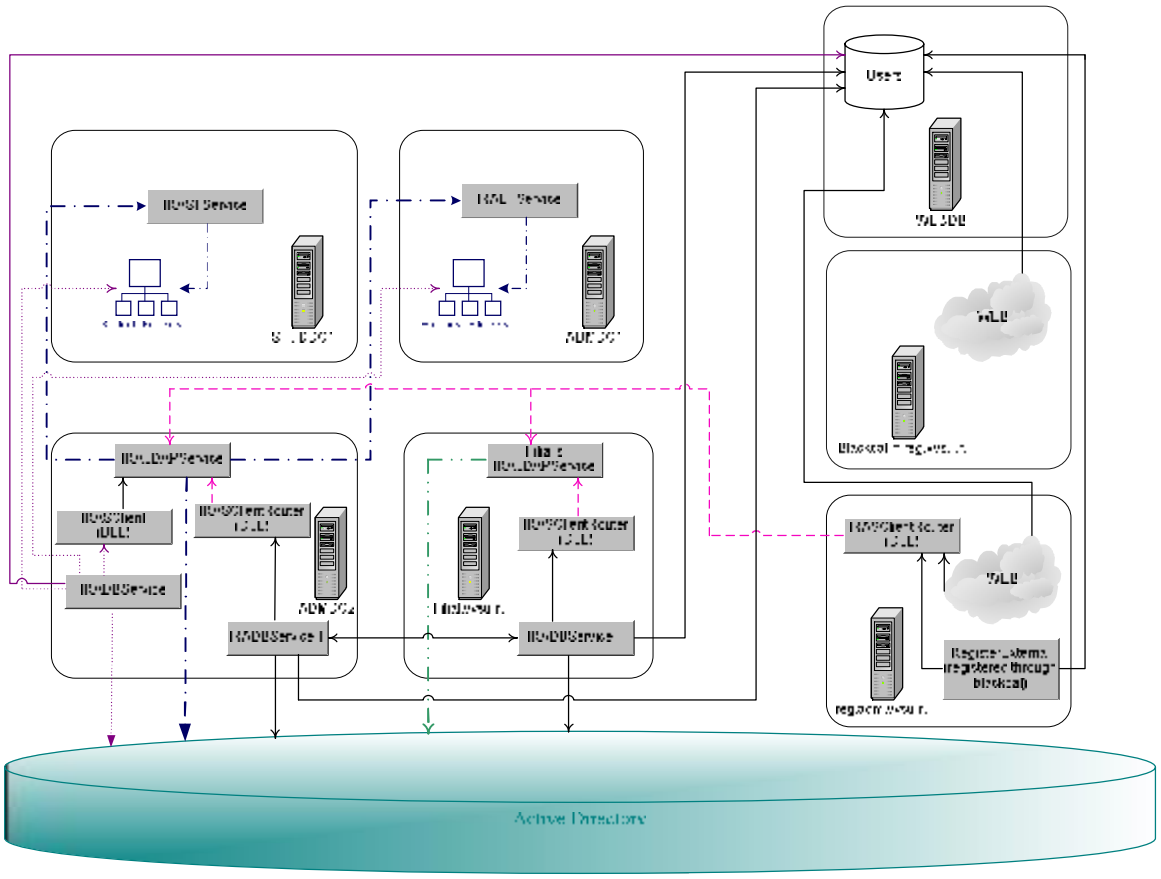

Рис. Архитектура системы

Разработанная система обеспечивает автоматическую регистрацию пользователя из филиала в КИС ВГУЭС. Система интегрирована с, разработанной ранее, системой единой регистрации пользователей, и является её расширением. В разработке находится модуль по актуализации данных в AD по сотрудникам и студентам в филиалах.

Литература

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