Единая система регистрации и управления доступом к информационным ресурсам вуза

Д.В. Гмарь, В.В. Крюков, В.С. Майоров, К.И. Шахгельдян
Владивостокский государственный университет экономики и сервиса
э. почта: carinash@vvsu.ru

Во Владивостокском государственном университете экономики и сервиса (ВГУЭС) корпоративная информационная среда создается на основе интеграции различных информационных сервисов и технологий: корпоративное клиент-серверное программное обеспечение, веб-серверы, системы управления базами данных, системы обеспечения групповой работы, корпоративный портал. Для обеспечения персонифицированного доступа к ресурсам и сервисам среды используется система единой регистрации пользователей интегрированной информационной среды вуза.

Интегрированная информационная среда вуза должна основываться на системе учетных записей пользователей, для которых определены права и привилегии работы в среде. В качестве базы данных учетных записей могут использоваться LDAP серверы от Sun, Oracle, или служба каталогов Active Directory (AD) от Microsoft. База данных учетных записей может представлять собой и отдельную разработанную базу данных пользователей информационных ресурсов вуза. Оба подхода имеют свои преимущества и поэтому в разрабатываемой единой системе регистрации-управления доступом к информационным ресурсам ВГУЭС используются и служба каталогов AD и база данных зарегистрированных пользователей к информационным ресурсам университета.

Система единой регистрации пользователей информационных ресурсов вуза позволяет автоматически создавать учетные записи в AD и в базе данных зарегистрированных пользователей веб-ресурсов вуза. Необходимость объединения этих двух способов объясняется следующим причинами.

1. Большая часть серверов портала вуза располагается в демилитаризированной зоне (ДМЗ), отделенной от внутренней корпоративной сети межсетевым экраном, который не пропускает запросы внешних пользователей во внутреннюю сеть. Это приводит к невозможности выполнить аутентификацию пользователей портала на основе учетных записей AD.
2. В среде портала используются наряду с веб-сервером Microsoft IIS, и веб-сервер Apache, который на момент разработки не поддерживал аутентификацию на базе учетных записей AD.
3. Корпоративный информационный портал вуза доступен и для внешних зарегистрированных пользователей, которых не следует регистрировать в AD, чтобы не перегружать контроллеры доменов лишней, не связанной с их основной функцией информацией.

Разработанная и внедренная система единой регистрации и управления доступом к информационным ресурсам вуза обеспечивает следующие функции.

1. Регистрация и управление доступом к ресурсам студентов, сотрудников, преподавателей вуза (внутренние пользователи) и внешних пользователей. В результате регистрации внутренних пользователей создаются две учетные записи с одинаковыми именами и паролями, одна из которых является учетной записью в одном из доменов AD (stud.vvsu.ru или empl.vvsu.ru) в зависимости категории пользователя. Учетная запись располагается в группе пользователей, которая соответствует подразделению, где работает сотрудник или учится студент. Другая учетная запись располагается в базе данных зарегистрированных пользователей веб-ресурсов вуза. Для внешних пользователей создается одна учетная запись в базе данных зарегистрированных пользователей веб-ресурсов вуза.
2. На файловых серверах студентов и сотрудников автоматически создаются каталоги в соответствии с оргструктурой вуза, доступ к которым определяется местом работы сотрудника и его должностью или местом учебы студента.
3. Для зарегистрированных пользователей на файловых серверах сотрудников и студентов

автоматически создаются личные папки в каталогах тех подразделений, где они работают или учатся.

4. Система поддерживает актуальность прав зарегистрированных пользователей и отслеживает все изменения, связанные с отчислением, увольнением, переходом в другое подразделение, изменением статуса внутреннего пользователя вуза. Кроме того, отслеживаются и изменения организационной структуры вуза, что позволяет автоматически вносить изменения в учетные записи AD, корректировать права пользователей. Увольнение сотрудника и отчисление студента приводит к блокированию учетной записи в AD с последующим удалением. Автоматически удаляются личные каталоги пользователей на корпоративном файловом сервере, после того как архивные копии размещаются в специальном каталоге файлового сервера. Автоматически удаляется и почтовый ящик, созданный пользователем на почтовом сервере вуза.

Система единой регистрации и управления доступом к информационным ресурсам вуза обеспечивает персонифицированную работу зарегистрированных пользователей с двумя категориями сервисов и служб информационной среды вуза:

1. Доступ к различным корпоративным сервисам и службам, включая файловую и почтовую службу, Инернет (с ограничениями по времени и объему трафику, накладываемому на учетную запись).
2. Доступ к информационным ресурсам корпоративного портала (http://it.vvsu.ru), который включает:
   a. образовательную часть информационной среды, представленную интегрированной обучающей средой Аванта (http://avanta.vvsu.ru), системой интерактивного тестирования СИТО (http://cito.vvsu.ru), сайтом цифровых учебно-методических материалов (http://abc.vvsu.ru), системой раздаточных материалов (http://study.vvsu.ru);
   b. информационно-справочную часть среды, содержащую полезную для сотрудников и студентов вуза информацию (расчетные листы, данные по учету труда, различные финансовые и статистические отчеты по кадровому и студенческому составу и т.д.);
   c. корпоративное программное обеспечение (управление оргструктурой, персоналом, учебным процессом);
   d. дополнительные ресурсы и сервисы корпоративного портала вуза (телефонный справочник, регламентирующие документы, системы анкетирования, форум, чат, поддержка коллективной работы пользователей и т.п.);
   e. системы учета и мониторинга использования ресурсов (компьютерная техника, телефония, почтовая служба, Интернет).

Доступ в первой категории основывается исключительно на учетной записи пользователя в AD. Вторая категория поддерживает учетные записи AD, если:

- ресурсы расположены на внутренних web-серверах и используется конфиденциальная информация (финансовая и персональная);
- происходит обращение к образовательному порталу и дополнительным ресурсам, расположенным на внешних серверах.

Архитектура серверной фермы интегрированной информационной среды вуза представляет собой две зоны – внутренняя корпоративная информационная сеть вуза и ДМЗ. В ДМЗ располагаются почтовый сервер, сервер базы данных, часть из которых представляет собой реплицированное подмножество корпоративных данных, а часть содержит информацию по зарегистрированным пользователями веб-ресурсов вуза. Кроме того, на этом сервере содержатся некоторые данные информационных сервисов портала вуза. В ДМЗ включены так же серверы обучающих сред «Аванта», «Сито» и веб -сервер портала ВГУЭС. Во внутренней сети находятся контроллеры доменов с каталогами учетных записей AD, файловые серверы студентов и сотрудников, а так же внутренний веб-сервер, через который разрешен доступ к конфиденциальным данным. Серверы в ДМЗ используют для аутентификации учетные записи зарегистрированных внутренних пользователей веб-сервисов, а внутренние серверы используют учетные записи AD.

В единой системе регистрации и управления доступом к информационным ресурсам вуза блок управления доступом обеспечивает назначение, изменения и запрещение доступа пользователей к информационным ресурсам и сервисам. Поскольку

вуз имеет большой контингент пользователей, то требования к системе управления правами включают обеспечение автоматизации процесса назначения прав.

Данное требование удовлетворяется с помощью двух подходов:

- для учетной записи в AD обеспечивается автоматический перенос пользователя в группу, правила для которой соответствуют текущему статусу пользователя;
- для учетной записи в базе данных зарегистрированных пользователей веб-ресурсов разработана система назначения ролей, которая позволяет давать права пользователям на основе их принадлежности к некоторой группе.

Например, роли в системе могут определяться категорией пользователя: студент вуза, сотрудник вуза или внешний пользователь, принадлежностью сотрудника к некоторому подразделению, принадлежностью сотрудника к определенному типу подразделения (учебные или административные), статусом или ролью сотрудника, связанной с занимаемой должностью или функцией, выполняемой в определенном проекте. Роль пользователя в некоторой системе может определяться любым специфичным для этой системы условием.

На базе системы единой регистрации и управления правами пользователей в настоящее время в интегрированной информационной среде ВГУЭС работает более 15 сред и сервисов.