УДК 004.7

О. Л. Жижимов, А. М. Федотов, Ф. Н. Юданов

Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия

Институт вычислительных технологий СО РАН
пр. Акад. Лаврентьева, 6, Новосибирск, 6630090, Россия

E-mail: zhizhim@sbras.ru, fedotov@nsu.ru, fedwiz@academ.org

МОДЕЛЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ ОРГАНИЗАЦИИ

Статья посвящена изложению основных технологических решений, применяемых при построении системы управления информационными ресурсами организации на примере Новосибирского государственного университета. Указанные решения формулируются в статье на основе подробного анализа задач, связанных с управлением информационными ресурсами НГУ, и подходов, используемых в крупных системах управления, имеющихся на рынке. При этом делается переход от общих принципов работы системы управления информационными ресурсами к решениям, оптимальным для частной задачи управления ресурсами НГУ.

Ключевые слова: управление информационные ресурсами, LDAP, централизованное хранилище данных, настройка прав доступа, информационные ресурсы НГУ.

Введение

Проблема доступа к информационным (в том числе и к вычислительным) ресурсам является одной из основных проблем, возникающих в деятельности научно-образовательного сообщества. В настоящее время наблюдается переход к распределенной схеме создания и поддержания информационных ресурсов, с одной стороны, и стремление к виртуальному единству посредством предоставления свободного доступа к любым ресурсам в сети через ограниченное число «точек доступа» – с другой [1].

Любая крупная организация, как, например, современный вуз типа НГУ, обладает обширным набором разнородных информационных ресурсов, используемых различными подразделениями, службами и персоналом организации. Сюда входят различные информационные системы, используемые в организации, всевозможные сервисы и службы (например, электронная почта, Wi-Fi, VPN и т. д.), а также вычислительные ресурсы, сетевое оборудование, сервера и рабочие станции.

Очевидно, что с ростом числа ресурсов неизменно возникают различные проблемы, связанные с их поддержкой и управлением. В первую очередь эти проблемы обусловлены необходимостью дублирования данных, используемых разными ресурсами. В случае достаточно частого обновления хранимых данных периодически возникают логические противоречия между данными на различных ресурсах, что может стать источником ошибок и сбоев в функционировании ресурсов. Кроме того, сам факт дублирования многократно увеличивает работу системных администраторов, связанную с поддержанием ресурсов. Постоянно действующими факторами при формировании единого (виртуального) информационного пространства организации являются [2]:

- иерархичность информационных систем и ресурсов;
- разнородность ресурсов и программно-технических сред, объединяемых в едином сетевом операционном пространстве;
- распределенность элементов информационной инфраструктуры.

Осознание необходимости интеграции разнородных информационных ресурсов привело к созданию интегрированных (единых) *научных информационных систем* (НИС), которые позволили бы установить связи между разнородными документами, организовывать единые каталоги документов, а также создавать специализированные системы поиска. Основная проблема, связанная с функционированием интегрированных распределенных информационных систем, широко известна – это практически реально нефункционирующая система актуализации информации [3; 4]. Решить эту проблему административными методами практически невозможно. Отметим, что эффективная эксплуатация информационных ресурсов возможна только в том случае, когда они *постоянно поддерживаются авторами*.

По-видимому, единственный путь к решению этой проблемы состоит в интеграции в рамках интегрированной распределенной информационной системы данных локальных информационно-справочных систем, существующих в организации, и придания этим системам функций глобальной (корпоративной) аутентификации и авторизации пользователей по доступу к информационным ресурсам.

Создание и поддержка распределенных информационных систем, интегрирующих разнородные информационно-вычислительные ресурсы и функционирующих в различных программно-аппаратных средах, требует специальных подходов к управлению этими системами [2]. Если управление собственно ресурсами может осуществляться в локальном режиме даже для распределенных систем [2; 5], то задача управления доступом к распределенным ресурсам не может быть решена в рамках локального администрирования. Обоснование последнего тезиса можно увидеть при рассмотрении типичных сценариев работы системы информационного обслуживания, которые мы опишем ниже.

В данной работе на примере информационных ресурсов сети Новосибирского государственного университета, объединяющей более 5 тыс. компьютеров, будут сформулированы требований к системе управления ресурсами, а также описание и обоснование основных решений, применяемых при построении системы. Отметим, что структура использования информационных ресурсов в любой большой организации довольно типична (за исключением, быть может, используемых информационных систем) и разрабатываемые решения в значительной степени применимы и к ним.

Распределенные информационные ресурсы

Развитие информационных ресурсов организации приводит к необходимости создания инфраструктуры для их интеграции в единую информационную систему, обеспечивающую прозрачный доступ к распределенной информации. Распределенность и гетерогенность информационных ресурсов налагает дополнительные требования к информационным системам [3], а именно:

- способность систем функционировать в условиях информационной и реализационной неоднородности, распределенности и автономности информационных ресурсов;
- обеспечение интероперабельности, повторного использования неоднородных информационных ресурсов в разнообразных применениях;
- возможность объединения систем в более сложные, интегрированные образования, основанные на интероперабельном взаимодействии компонентов;
- осуществление миграции унаследованных систем в новые системы, соответствующие новым требованиям и технологиям при сохранении их интероперабельности;
- обеспечение более длительного жизненного цикла систем.

Для удовлетворения перечисленных требований необходимо создание инфраструктуры (информационной службы или центра) для представления и обмена метаданными – структурированной информацией об информационных ресурсах и правилах доступа к ним. В настоящее время многие информационные центры, занимающиеся сбором и распространением метаданных, проявляют активную заинтересованность в организации взаимодействия с целью обмена имеющимися у них фондами. Как правило, в основе такой интеграции фондов лежит выработка стандарта на формат для представления метаданных, одновременно с унификацией массивов нормативно-справочной информации. Отметим, что основу интеграции ресурсов несут на себе технологии работы с метаданными, которые:

- обеспечивают механизмы интеграции информационных ресурсов из разных источников сведениями о свойствах этих ресурсов;
- являются источниками сведений о свойствах и содержании информационных ресурсов для механизмов управления данными в информационных системах;
- являются источником информации, необходимой для осуществления реинжиниринга информационных систем;
- обеспечивают представление сведений о системе, ее информационных и других ресурсах для различных приложений и пользователей системы.

Задача информационных систем – хранение информации и предоставление ее пользователям в удобном для них виде. Как правило, такие системы могут быть организованы на основе различных технологических решений, направленных на реализацию той или иной парадигмы распределенности.

Парадигма распределенности может рассматриваться с точки зрения архитектуры информационных систем. Заметим, что большинство информационных систем сегодня строится по принципу трехзвенной архитектуры с условным делением звеньев на клиенты, серверы приложений и серверы баз данных. Исходя из этого можно выделить три основных группы распределенных систем, реализующих принцип распределенности на соответствующем уровне.

Типичные сценарии работы информационного сервера приложений

Несмотря на разнообразие приложений, предоставляющих доступ к информационным ресурсам, их функционирование происходит по однотипным сценариям. Типичный сценарий акта извлечения информации может быть представлен в следующем виде.

1. Клиент посылает серверу запрос на просмотр информационного ресурса.
2. Сервер принимает запрос и выделяет идентификационные параметры клиента (адрес, имя, пароль, сертификат и т. п.).
3. Сервер проверяет подлинность клиента по предъявленным идентификационным параметрам (аутентификация).
4. Сервер проверяет доступность данному клиенту запрошенного им информационного ресурса (авторизация).
5. Сервер определяет ресурс в хранилище и передает (или предоставляет доступ к нему) его клиенту.

Здесь продемонстрирована последовательность операций с положительным исходом каждой. В реальной ситуации эта последовательность может быть прервана с фиксацией состояния ошибки или включать дополнительные процедуры для уточнения тех или иных параметров запроса клиента.

Таким образом, при обработке запроса на извлечение информационного ресурса из некоторого хранилища сервер вынужден обратиться к трем разнотипным базам данных.

Тип 1 – база данных пользователей, включающая список пользователей и их идентификационные параметры.

Тип 2 – база данных прав пользователей на доступ к информационным ресурсам.

Тип 3 – собственно хранилище информационных ресурсов.

При этом зачастую тип 3 содержит два совершенно различных хранилища:

- хранилище описаний информационных ресурсов – метаданные, каталог ресурсов и т. п.;
- хранилище собственно информационных ресурсов, например, полные тексты, бинарные данные и т. п.

Ситуация еще более усугубляется при организации распределенных информационных систем, в которых целая совокупность разнородных информационных серверов должна использовать единую интегрированную для всех информацию типа 1 и 2. Так возникает естественное желание иметь единую точку доступа к данным типа 1 и 2 для всех сервисов распределенной информационной системы. Это желание не может быть удовлетворено в рамках локальных информационных систем.

LDAP – технологическая основа системы управления доступом к ресурсам

Как следует из вышесказанного, для решения задачи управления доступом к распределенным ресурсам необходимо внедрение технологий, изначально базирующихся на парадигмах «распределенности», с одной стороны, и «интероперабельности», с другой стороны. Для успешного использования различными серверами построение технологии должно быть основано на международных стандартах открытых систем и хорошо поддерживаемых производителями программных продуктах.

В качестве подобной технологии для корпоративного применения может быть использована технология LDAP (Lightweight Directory Access Protocol – облегченный протокол доступа к каталогам) при наличии развитой системы корпоративных каталогов, объединенных в единую корпоративную распределенную справочную систему (КРСС) организации (см., например, [4–6]).

Однако для достижения цели, т. е. создания системы управления доступом к распределенным информационным ресурсам, необходимо в рамках технологий LDAP решить ряд дополнительных задач.

- Создание логической надстройки над КРСС, включающей определения дополнительных схем данных и основных процедур контроля доступа к ресурсам корпоративной распределенной информационной системе (КРИС).
- Создание информационной составляющей системы управления доступом к распределенным информационным ресурсам (СУДРИР) – расширения КРСС, допускающие хранение и обработку исходных данных по контролю доступа к ресурсам.
- Адаптация серверного программного обеспечения, предоставляющего доступ ресурсам (Z39.50, WWW, FTP и т. д.), к возможности работы в соответствии с правилами СУДРИР.
- Создание интерфейсов для управления СУДРИР.

Единая корпоративная распределенная справочная система (КРСС) как базовый элемент СУДРИР должна удовлетворять определенным требованиям.

- Организация информации в КРСС должна обеспечивать ее сегментацию на отдельные административные сегменты.
- Актуальность информации в КРСС должна поддерживаться множеством администраторов независимо в каждом сегменте системы.
- Доступ к КРСС должен быть основан на открытых стандартах.
- КРСС должна обеспечивать возможность хранения информации различного типа с возможностью ее поиска по различным атрибутам.

При использовании технологий LDAP для создания КРСС перечисленные требования могут быть удовлетворены [5]. Наличие КРСС является необходимым условием для успешного построения СУДРИР. Основные требования, которые можно предъявить к системе управления доступом к распределенным информационным ресурсам (СУДРИР) можно сформулировать следующим образом.

- СУДРИР должна быть интегрирована с КРСС.
- Технология СУДРИР должна быть основана на международных стандартах и протоколах.
- СУДРИР должна допускать масштабирование и быть многоплатформенной.
- СУДРИР должна включать демократичные пользовательские интерфейсы.

На рынке существует ряд универсальных решений, основанных на технологии службы каталогов (LDAP), в той или иной степени решающих задачу управления информационными ресурсами. К ним можно отнести:

- IBM Tivoli;
- Microsoft Active Directory;
- HP OpenView;
- Sun Service Desk.

Фактически указанные решения (кроме Tivoli) только частично удовлетворяют сформулированным требованиям и, по сути, являются системами управления ресурсами корпора-

тивной компьютерной сети. Они весьма сложны в конфигурировании и внедрении, при этом обладают крайне высокой ценой.

Но самым серьезным препятствием при применении данных систем является отсутствие учета специфики ресурсов конкретной организации. В первую очередь речь идет об информационных системах (ниже в статье они перечислены на примере НГУ и описаны подробно), которые в данном случае являются краеугольным камнем, поскольку служат основным источником и хранилищем данных, связанных с организацией (вузом).

На основе анализа требований и технологических решений мы приходим к необходимости внедрения системы решающей следующие основные задачи.

1. Организация единообразного авторизованного доступа к ресурсам. Будучи однажды заведенным в системе, пользователь получает набор идентификационных параметров (имя пользователя и пароль), которые затем используются для получения доступа к любым ресурсам, будь то рабочий компьютер или FTP-сервер.
2. Управление правами доступа пользователей. Ввиду того, что для доступа ко всем ресурсам используется один набор идентификационных данных, необходима реализация механизма разграничения доступа к ресурсам, поскольку, очевидно, существуют ресурсы, доступ к которым должен иметь ограниченный круг пользователей, а также в пределах одного ресурса существуют задачи, право на выполнение которых не может быть предоставлено любому пользователю.
3. Введение дисциплины имен на множестве ресурсов. Данный пункт подразумевает присвоение каждому ресурсу своего уникального имени, которое сформировано по заранее определённым правилам, а также наличие процедуры автоматической генерации имен для новых ресурсов.
4. Поддержание централизованного хранилища данных, разделяемых между ресурсами. Использование подобного хранилища в значительной степени решает проблему дублирования данных, описанную в начале статьи, в то же время это хранилище может являться инструментом решения задач, сформулированных в предыдущих пунктах.

Модели функционирования системы управления доступом к ресурсам

Выбор технологии LDAP для построения СУДРИР оставляет открытыми вопросы реализации механизмов контроля управления доступом к распределенным информационным ресурсам. Эта реализация зависит от выбора модели СУДРИР.

Если выделить основные функциональные элементы СУДРИР –

1. функция идентификации клиента КРИС (аутентификация),
2. функция задания правил доступа к ресурсам для различных категорий клиентов,
3. функция определения прав конкретного клиента КРИС (авторизация),
4. функция обеспечения соответствия прав клиента КРИС уровню предлагаемого сервиса КРИС,
5. функция учета используемых ресурсов (биллинга), –

то только элемент 1 (аутентификация клиента) может быть реализован в технологиях LDAP без каких-либо дополнительных построений над КРСС. Реализация других элементов зависит от выбранной модели контроля доступа к распределенным информационным ресурсам. В зависимости от степени «распределенности» перечисленных выше элементов можно выделить следующие модели.

1. Простая модель, в которой КРСС используется только для аутентификации клиента встроенными средствами LDAP-серверов, другие элементы СУДРИР реализованы локально для каждого сервиса и ресурса КРИС. Положительные качества модели – простота реализации единого пространства имен и паролей для клиентов КРИС, недостаток – отсутствие возможности поддержки единых политик доступа к распределенным ресурсам. Однако даже в этой простой модели на основе LDAP решается задача ведения единого реестра пользователей КРИС, их паролей и цифровых ключей на основе поддержки КРСС. Пример реализации

этой модели продемонстрирован на рис. 1 для двух серверов – Web-сервера Apache и FTP-сервера ProFTPD.

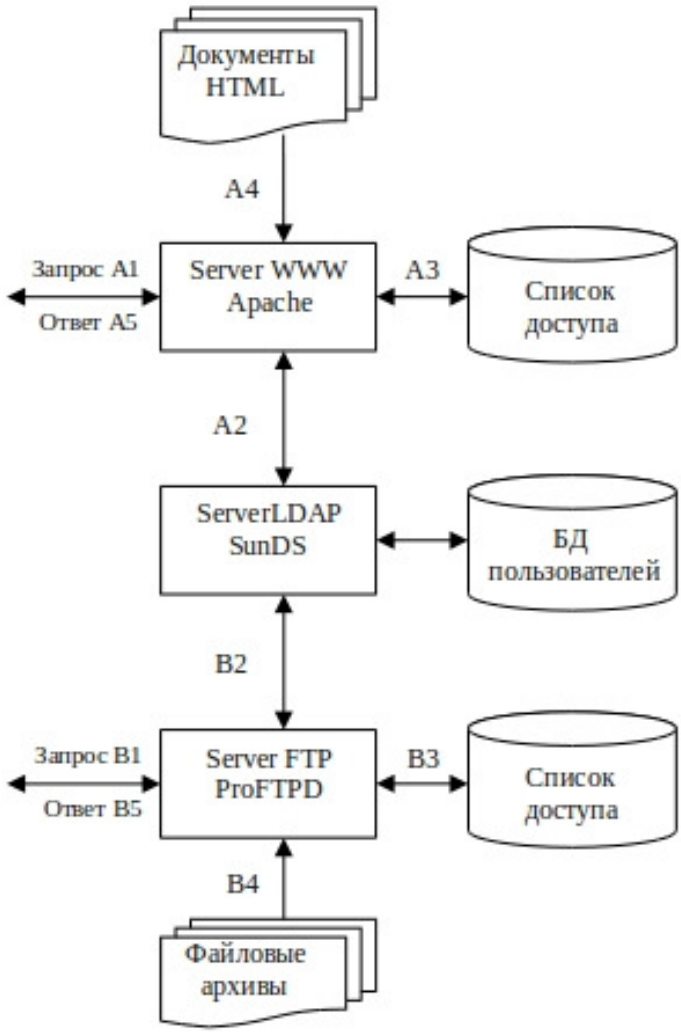

Рис. 1. Иллюстрация модели 1: A2, B2 – запросы на аутентификацию; A3, B3 – запросы на авторизацию; A4, B4 – извлечение данных

2. Модель, в которой формулирование, проверка и реализация прав клиента происходит на основе технологий LDAP, т. е. в КРСС, допускает различные вариации, вплоть до выдачи сертификатов в модели X.509. Поскольку сегодня принято осуществлять контроль доступа к различным информационным объектам, основываясь на списках доступа (ACL – Access Control List), то эти вариации могут отличаться как способом хранения ACL, так и способом привязки информационных объектов к ACL:

а) в наиболее простом варианте ACL формулируются на основе встроенных механизмов LDAP-серверов как наборы штатных серверных инструкций (ACI – Access Control Instructions) по управлению доступом к элементам дерева КРСС. Положительное качество этого способа – простота реализации при условии наличия в каталоге КРСС элемента описания соответствующего информационного объекта. Проверка прав клиента на доступ к информационному объекту при этом сводится к проверке этих прав на доступ к соответствующему описанию объекта в каталоге КРСС. В ситуации, когда необходим различный уровень доступа к первичным и вторичным (описаниям) информационным объектам, этот способ не может быть использован;

б) более сложным представляется вариант, когда ACL формулируются на основе специальной схемы данных – набора объектов и атрибутов каталога КРСС. При этом описания ин-

формационных объектов КРИС должны обязательно присутствовать в КРСС и содержать атрибуты, определяющие правила доступа к собственно объектам, а не к их описаниям, доступ к которым определяется ACI (см. выше). Каждый информационный сервер при этом должен проверять права доступа клиентов к ресурсам, обращаясь к серверу КРСС и анализируя соответствующие атрибуты описания запрошенного ресурса. Этот способ более сложный и затратный, чем предыдущий, но позволяет реализовать полный контроль над доступом к информационным ресурсам в соответствии с определенными выше требованиями.

Оба варианта модели 2 требуют, чтобы, с одной стороны, в каталоге КРСС (корпоративном LDAP-каталоге) существовали объекты определенного класса – описания информационных ресурсов, интегрированных в КРИС, а с другой – чтобы информационные серверы КРИС (WWW, FTP, Z39.50 и т. п.) при предоставлении доступа к ресурсу всегда обращались к соответствующим описаниям. На основе анализа кодов возврата (вариант а) или значения некоторых атрибутов (вариант б) информационный сервер должен принять решение о соответствии прав клиента КРИС уровню предлагаемого сервиса КРИС.

Пример реализации модели 2 продемонстрирован на рис. 2 для двух серверов – Web-сервера Apache и FTP-сервера ProFTPD.

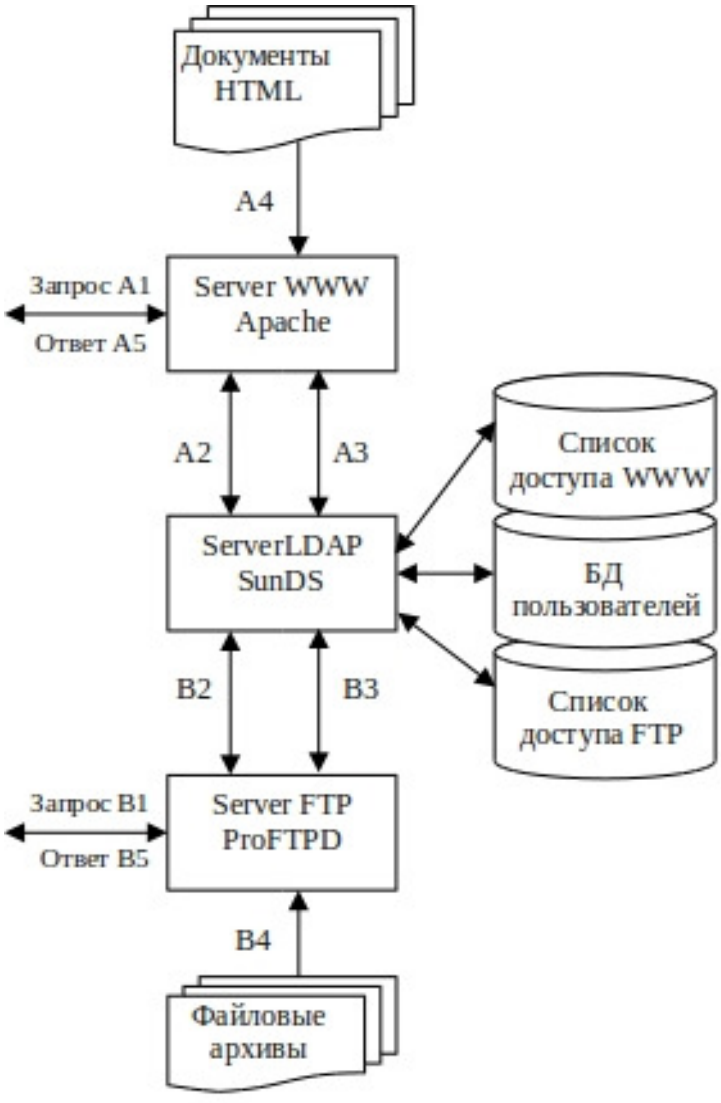

Рис. 2. Иллюстрация модели 2: A2, B2 – запросы на аутентификацию; A3, B3 – запросы на авторизацию; A4, B4 – извлечение данных

Информационные ресурсы НГУ

Эффективность применения той или иной модели контроля доступа к распределенным информационным ресурсам может быть определена только для определенной информационной системы с конкретной топологией и информационными ресурсами

Рассмотрим подробнее список информационных ресурсов НГУ и сформулируем задачи управления, связанные с каждым ресурсом.

1. Информационные системы

- Университетская информационная система (УИС) – комплекс интегрированных программных продуктов, разработанный в Центре новых информационных технологий НГУ (ЦНИТ НГУ), включающий в себя такие компоненты, как электронный документооборот вуза, система автоматизации приемной кампании, система формирования учебных планов, подсистема «Деканат», позволяющая хранить и отслеживать данные о студентах, в том числе их успеваемость, и т. д. [7].

В основном пользователями УИС в НГУ являются сотрудники деканатов и кафедр университета. На текущий момент УИС содержит наиболее полные данные о студентах и преподавателях НГУ, а также о его организационной структуре, кроме того, эти данные своевременно обновляются. Таким образом, УИС может и должна быть использована в качестве основного источника данных для системы управления информационными ресурсами при первичном заполнении данными последней. На более поздних этапах также потребуется регулярная синхронизация данных между двумя системами.

- Система 1С используется в бухгалтерии и в отделе кадров НГУ [8]. На данный момент большая часть данных, касающихся студенческого и преподавательского состава НГУ, а также структуры университета продублирована в 1С и УИС, при этом часть данных периодически импортируется из УИС в формате XML.

На сегодняшний день актуальны следующие задачи:

а) синхронизация данных о персонах и структуре организации между системами;

б) гибкая настройка прав пользователей 1С в системе;

- Библиотечная информационная система «Руслан» используется для хранения и поиска информации о ресурсах библиотеки НГУ.

На сегодняшний день актуальны следующие задачи:

а) своевременное обновлений списков студентов в БИС «Руслан»;

б) разграничение доступа пользователей к ресурсам системы;

- ИС 2-го отдела (отдела воинского учета). На сегодняшний день актуальна задача своевременного обновления списков студентов в системе и передача данных о студентах.

2. Информационные сервисы

- Сервис электронной почты, включающий в себя как IMAP/POP3, так и SMTP сервера. В качестве отдельного информационного ресурса также следует рассматривать каждый почтовый ящик пользователя.

На сегодняшний день актуальны следующие задачи:

а) автоматическое создание и удаление ящиков для всех пользователей по мере их появления в вузе и ухода из него;

б) введение дисциплины именования почтовых ящик, т. е. введение стандартного правила генерации имени ящика в зависимости от ФИО, даты рождения, учебной группы студента или подразделения сотрудника;

в) обеспечение учета альтернативных названий (алиасов) почтовых ящиков. Это требование обусловлено необходимостью учета пользователей, занимающих несколько должностей в университете, а также необходимость сохранения названий адресов, существующих до внедрения системы управления ресурсами.

- Сервис Wi-Fi. В здании НГУ расположено множество точек доступа Wi-Fi, которыми пользуются студенты и сотрудники. На сегодняшний день доступ к этим точкам является открытым и анонимным. Требуется обеспечить авторизованный доступ к сервису, совместимый с доступом к другим информационным ресурсам.

- Сервис VPN. Используется для предоставления пользователям сети высокоскоростного платного доступа в Интернет. Сервис управляется биллинговой системой СмартАСР, хранящей в себе идентификационные данные пользователей VPN, а также состояние их личного счета.

Система управления ресурсами НГУ может обеспечить автоматическую авторизацию пользователей и администраторов в системе, хранение данных о состоянии их счета, который также может быть счетом и для других видов услуг сети.

- HTTP Proxy сервера. В НГУ существует несколько прокси-серверов, как публичных, так и с ограниченным доступом; механизм доступа к последним должен быть унифицирован.

3. Сеть IP-телефонов Cisco. Сотрудники НГУ используют развернутую сеть IP-телефонов. При этом стоит задача привязки имени сотрудника к номеру его служебного телефона, т. е. фактически создания электронного телефонного справочника НГУ, при этом данные справочника необходимо также отображать на дисплеях самих телефонных аппаратов.

4. Web-ресурсы и web-сервисы. В НГУ существует множество web-ресурсов, начиная от сайта университета и заканчивая личными страницами студентов и сотрудников. Актуальными задачами являются:

а) организация авторизованного доступа к web-ресурсам;

б) автоматическое создание шаблонов личных web-страниц пользователей в момент их заведения в системе;

в) введение дисциплины именования личных web-страниц, а также сайтов подразделений (кафедр, факультетов и т. д.).

5. Компьютеры, используемые в НГУ. Сюда следует отнести:

- машины в терминальных классах университета;
- рабочие компьютеры сотрудников;
- компьютеры, используемые в качестве различных серверов (в том числе web-серверов, серверов баз данных, UNIX серверов, используемых в учебном процессе и т. д.).

Актуальными задачами являются:

а) организация единообразного авторизованного доступа к любому компьютеру в университете с возможностью корректной настройки прав доступа администратором:

б) учет и поименование каждого компьютера, хранение данных о компьютерах университета и их конфигурации;

в) хранение профиля пользователя, который содержит настройки и файлы данного пользователя и может быть автоматически загружен по сети на любой компьютер.

Субъекты в системе

Разрабатываемая система поддерживает два основных типа субъектов: персоны и группы персон.

Персоной является любой человек, имеющий отношение к деятельности университета. Можно выделить два основных класса персон: студенты и сотрудники. Большинство персон в той или иной форме являются пользователями информационных ресурсов НГУ.

Группой персон является множество персон, обладающих некоторыми сходными функциями при взаимодействии с информационными ресурсами. Часто группа персон может быть ассоциирована с организационной единицей в вузе, например, с кафедрой, факультетом или студенческой группой.

При организации управления субъектами разрабатываемой системы требуется учитывать ряд особенностей:

1. Значительное количество персон, большинство из которых является студентами (~5 000 человек для НГУ, свыше 20 000 для более крупных вузов).

2. Постоянное изменение множества активных персон, связанное с изменением студенческого и кадрового состава. Студенческий состав изменяется наиболее часто в связи с ежегодным окончанием вуза одними студентами и поступлением в вуз других.

3. Часть функций персоны при взаимодействии с ресурсами обусловлена должностью персоны в вузе и при смене лица, занимающего ту или иную должность, происходит передача соответствующих функций. В то же время существуют ресурсы, относящиеся к данной персоне непосредственно, например, личная web-страница, которая остается закрепленной за персоной, независимо от смены статуса последней.

Исходя их вышеперечисленных особенностей при управлении субъектами используются следующие принципы:

1. Ролевая модель управления доступом. Каждый субъект обладает набором ролей в системе, который обусловлен его статусом в вузе. Каждая роль в свою очередь содержит в себе набор привилегий, предоставляющих доступ к тем или иным ресурсам. Например, можно выделить такие роли, как «сотрудник деканата», «сотрудник приемной кампании», «администратор системы управления».

2. Персона, принадлежащая к некоторой группе, наследует множество ролей этой группы, т. е. каждая роль, присвоенная группе персон, становится ролью всех членов группы.

3. Использование элементов иерархической модели управления доступом. Фактически использование этого принципа обозначает децентрализацию управления пользователями, т. е. наличие в системе множества администраторов (персон, выставляющих роли пользователям) различного уровня. Администратор системы может делегировать часть своих полномочий администраторам более низкого уровня. Такой подход позволяет, например, перенести ответственность за управление правами студентов на сотрудников деканатов, сняв тем самым нагрузку со службы поддержки системы, при этом сами сотрудники деканатов ограничены в возможностях выставления прав настолько, насколько это необходимо.

4. Значительная часть ролей персоны однозначно определяется ее должностью, либо принадлежностью персоны к той или иной группе. Доступ к компьютеру главного бухгалтера всегда имеет главный бухгалтер, независимо от того, кто именно занимает эту должность. Таким образом, при изменении информации о должности персоны в университете, персоне должны автоматически присваиваться (или же, наоборот, удаляться) те или иные роли.

5. Настройка прав доступа отделена от настроек каждого из ресурсов. Иными словами, компонент системы, предоставляющий администратору интерфейс редактирования прав доступа, никак не зависит от логики работы ресурсов, в том числе не зависит и от самого набора ресурсов. Аналогично, сами ресурсы напрямую не зависят от логики работы системы управления доступом, обращение к которой сводится лишь к периодическим запросам на подтверждение наличия у текущего пользователя той или иной привилегии.

Структура системы управления ресурсами

Центральной частью системы управления ресурсами является хранилище данных на основе службы каталогов LDAP. Данное хранилище исполняет роль промежуточного слоя между информационными ресурсами. Хранилище – это единственный компонент системы, с которым напрямую сообщается каждый из ресурсов, при этом сообщение осуществляется целиком по протоколу LDAP.

Хранилище данных используется ресурсами для следующих целей.

1. Осуществление процедуры авторизации пользователя на ресурсе путем проверки корректности идентификационных параметров.

2. Проверка наличия у пользователя необходимых для исполнения той или иной операции привилегий.

3. Получение необходимых данных из хранилища. В хранилище следует помещать такие данные, которые используются более чем одним ресурсом.

4. Обновление некоторых данных в хранилище и, таким образом, осуществление обмена данными с другими ресурсами. Фактически, это единственный способ обмена данными, который должен быть использован в процессе работы ресурсов.

Еще одним важным компонентом системы является управляющий сервер, который предоставляет администратору системы следующие возможности.

1. Управление пользователями системы: создание, удаление пользователей, управление их правами доступа.
2. Редактирование разделяемых данных в хранилище.
3. Управление импортом данных в хранилище и экспортом из хранилища с использованием внешних форматов.

Хотя управляющий сервер имеет функциональность, специализированную под задачи системы управления, с точки зрения процедуры взаимодействия с хранилищем он не отличается от любого другого информационного ресурса и, таким образом, в модели системы выделять его среди других ресурсов необходимости нет.

Схематически структура системы управления информационными ресурсами изображена на рис. 3.

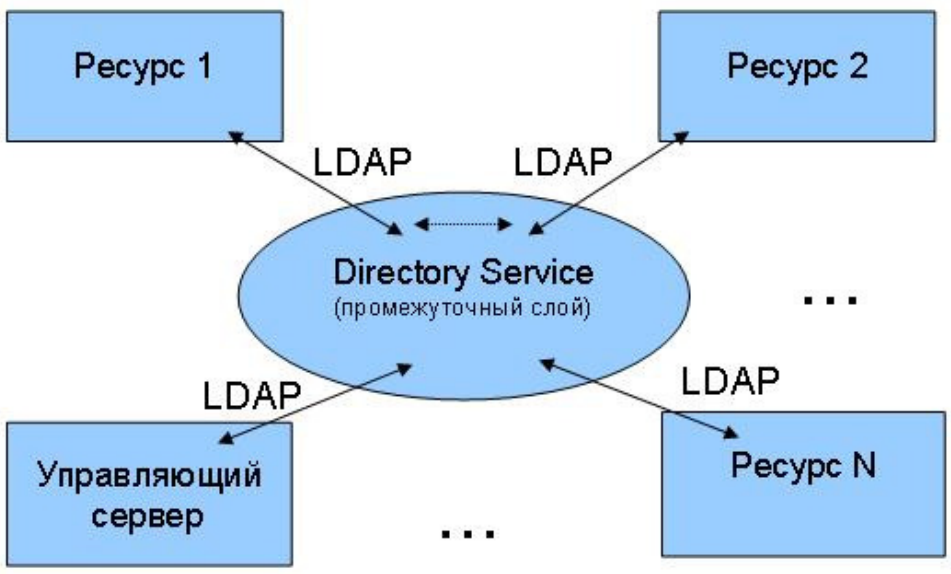

Рис. 3. Верхнеуровневая структура системы

Концепция личного кабинета пользователя

Развитием идеи об организации единообразного доступа ко всем информационным ресурсам является концепция личного кабинета пользователя, как единой точки доступа к этим ресурсам.

Личный кабинет пользователя – это набор интерфейсов, позволяющий пользователю управлять настройками, касающимися его пользования ресурсами сети. Личный кабинет является точкой входа в сеть НГУ, т. е. ввод идентификационных данных осуществляется пользователем для получения доступа к личному кабинету, после чего авторизация на остальных ресурсах производится уже автоматически, не требуя от пользователя дополнительных действий.

Личный кабинет дает следующие основные возможности.

1. Управление платными услугами. Пользователь может просматривать состояние своего счета, контролировать свои расходы, мгновенно подключать или отключать те или иные услуги.

2. Интеграция с системой тестирования студентов, использующейся в НГУ; в личном кабинете студенты могут получать доступ к прохождению тестов, просматривать результаты и статистику по тестированию.

3. Интеграция с личным кабинетом портала НГУ. Портал НГУ – система, внедренная в университете в 2010 году, предоставляющая публичный доступ к данным УИС (т. е. к той части данных, к которой возможен публичный доступ) и одновременно являющаяся социальной сетью для студентов и преподавателей НГУ. Личный кабинет портала НГУ дает возможность преподавателям переписываться со студентами, публиковать описания своих курсов и учебные материалы по ним. Студенты средствами портала могут просматривать свою успеваемость, историю приказов, общаться с одногруппниками.

Разумным решением может быть построение личного кабинета пользователя ресурсами сети на основе личного кабинета в портале НГУ и объединение их функциональности.

Создание единой точки доступа ко всем ресурсами сети автоматически повышает надежность авторизационных параметров в том смысле, что можно быть уверенным, что те или иные операции с ресурсами производятся именно тем пользователем, который был авторизован, поскольку добровольная передача пароля другим лицам, которая была бы возможна, если бы пароль открывал доступ, к примеру, только к точке доступа Wi-Fi, теперь маловероятна, поскольку пароль от личного кабинета является ключом ко многим настройкам, касающимся пользователя лично, в том числе связанным с платными услугами.

Примеры бизнес-процессов в системе

Рассмотрим несколько процессов, иллюстрирующих функциональность описываемой системы (рис. 4, 5, 6, 7, 8).

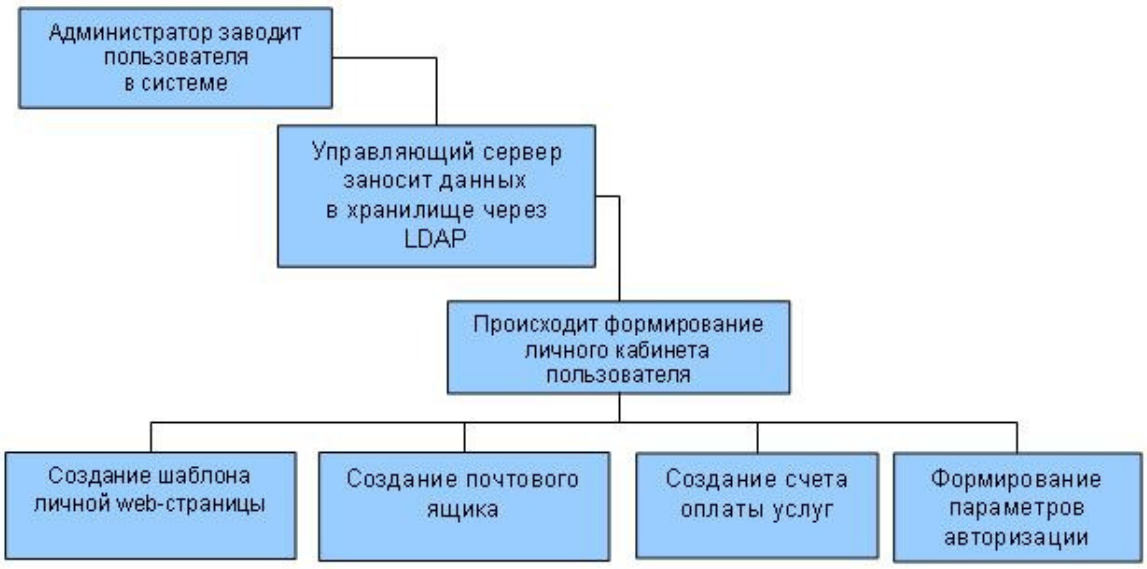

Рис. 4. Процесс создания нового пользователя информационными ресурсами

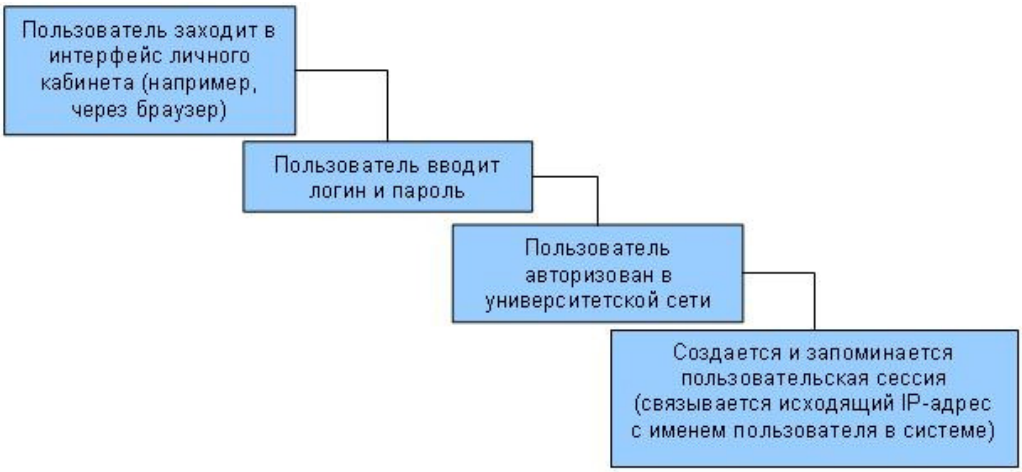

Рис. 5. Процесс авторизации пользователя в системе

Рис. 6. Процесс получения авторизованного доступа к ресурсу

Рис. 7. Процесс модификации прав доступа пользователя

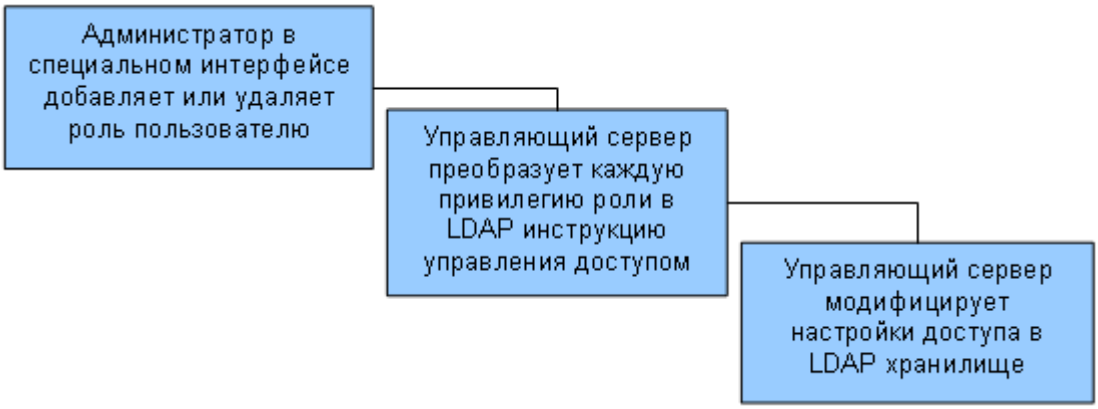

Рис. 8. Процесс модификации необходимых привилегий для доступа к ресурсу

Заключение

В данной статье на примере Новосибирского государственного университета были сформулированы основные задачи, касающиеся управления информационными ресурсами организации, указаны объекты и субъекты управления, приведены их специфичные свойства.

На основе анализа этих задач и особенностей предметной области, а также анализа принципов работы крупных систем управления, имеющихся на рынке, сформулированы основные технологические решения, применяемые при построении системы: централизованное хранилище данных, сообщение по протоколу LDAP, совмещение ролевой и иерархической модели доступа к данным, концепция личного кабинета пользователя как единой точки доступа к ресурсам. Построена верхнеуровневая схема структуры системы и приведены схемы основных бизнес-процессов, происходящих при использовании системы.

Список литературы

1. *Федотов А. М.* Информационная безопасность в корпоративной сети // Проблемы безопасности и чрезвычайных ситуаций / ВИНИТИ. М.: ВИНИТИ, 2008. № 2. С. 88–101.

2. *Жижимов О. Л., Федотов А. М.* Модели управления доступом к распределенным информационным ресурсам // Электронные библиотеки: перспективные методы и технологии, электронные коллекции. Труды Девятой Всероссийской научной конференции RCDL'2007 (Переславль-Залесский, Россия, 15–18 октября 2007 г.). Переславль-Залесский: Изд-во «Университет города Переславля», 2007. С. 301–304.

3. *Шокин Ю. И., Федотов А. М.* К вопросу о развитии информационной инфраструктуры СО РАН // Вычислительные технологии. 2009. Т. 6, № 6. С. 127–137.

4. *Созыкин А. В., Масич Г. Ф., Масич А.Г., Бездушный А. Н.* Вопросы интеграции информационных и сетевых служб. Варианты использования LDAP каталогов // Тр. VI Всерос. науч. конф. «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» – RCDL2004. Пущино, Россия, 2004.

5. *Жижимов О. Л., Турпанов А. А., Федотов А. М.* Корпоративный каталог СО РАН // Электронные библиотеки: перспективные методы и технологии, электронные коллекции: Тр. VIII Всерос. науч. конф. (RCDL'2006) Суздаль, 17–19 окт. 2006 г. Ярославль, 2006. С. 226–230.

6. *Барахнин В. Б., Жижимов О. Л., Степанов Ю. Ю., Федотов А. М.* LDAP-каталог организации как ядро корпоративной распределенной информационной системы // Инновационные недра Кузбасса. IT-технологии: Сб. науч. тр. Кемерово: ИНТ, 2008. С. 226–232.

7. *Адаманский А. В., Денисов А. Л., Кочеев А. А.* Опыт автоматизации вуза. Система УИС // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2006. Т. 4, вып. 1. С. 2–6.

8. *Демиш В. О., Пищик Б. Н., Козьменко Г. Г.* Проблемы автоматизации управления образовательным учреждением // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2009. Т. 7, вып. 3. С. 95–102.

Материал поступил в редколлегию 23.10.2010

O. L. Zhizhimov, A. M. Fedotov, F. N. Yudanov

ORGANIZATIONAL INFORMATION RESOURCES CONTROL MODEL

The article covers some basic solutions used in organizational information resources control system building process by the example of Novosibirsk state university information resources. These solutions are result of the deep analysis of actual problems connected with information resources control in NSU and on other hand the most common approaches used in major control systems available. The common work principles of information resources control system are used to formulate fundamental decisions for particular problems of NSU information resources control.

Keywords: information resources control, LDAP, centralized data store, user access control, information resources of NSU.