Курманбек уулу Талант

«КАРАКОЛ» ЭРКИН ЭКОНОМИКАЛЫК ЗОНАСЫНЫН МААЛЫМАТТЫК СИСТЕМАСЫ ҮЧҮН КОЛДОНУУЧУЛАРДЫ ИДЕНТИФИКАЦИЯЛОО

Курманбек уулу Талант

РЕШЕНИЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ СВОБОДНОЙ ЭКОНОМИЧЕСКОЙ ЗОНЫ «КАРАКОЛ»

Kurmanbek uulu Talant

SOLUTION USER AUTHENTICATION FOR THE INFORMATION SYSTEM OF THE FREE ECONOMIC ZONE «KARAKOL»

УДК: 681.5

«Каракол» Эркин Экономикалык зонасынын маалыматтык системасы үчүн колдонуучуларды идентификациялоо маселеси ачык программалык коддор менен чечилет.

Проектируется и создается информационная система для Свободной Экономической зоны «Каракол» и решается проблема авторизации и идентификации пользователей автоматизированной системы. Предлагается единая идентификация, которая сможет предоставить всем пользователям доступ к нужным приложениям.

There is designed and creature information system for "Karakol" free economic zone and is solved the problem of authorization and identification of the users of automated system. There is proposed the single identification, which can submit access to all the users towards the needed applications.

Информатизация государственных или коммерческих структур требует комплексного и системного подхода в выборе программного обеспечения (далее ПО) и технологии организации идентификации пользователей. Выбор ПО зависит от многих факторов, таких, как финансирование, уровень секретности, объем данных, объем передачи данных, радиус действия, технические параметры и т.д. Выбор ПО является сложным и важным этапом информатизации, необходимо выбрать платформу, прикладное программное обеспечение для создания порталов, специализированное программное обеспечение для обеспечения единой аутентификации и обеспечения необходимой безопасности.

Для дирекции СЭЗ «Каракол» (свободная экономическая зона), территориально расположенной в Иссык-кульской области Кыргызской Республики и имеющей статус государственного учреждения, проектируется информационная система, для которой необходимо выбрать решение вопроса по авторизации и идентификации пользователей. С этой целью был проведен анализ программных средств по различным критериям, а также по функциональным требованиям, требованиям информационной безопасности и т.д. В результате анализа было выделено следующее программно-техническое направление: построение единой идентификационной системы с использованием открытых программных средств (с открытыми программными кодами).

Рассмотрим подробно выбранное направление с открытыми кодами. В работах [1] - [5], приведены необходимые сведения по данному вопросу и при дальнейшем изложении используются материалы из этих источников.

Использование систем с открытыми кодами позволяет настроить и доработать комплекс программ идентификационной системы, обеспечить высокий уровень безопасности, исключить наличие «программ-закладок», использовать бесплатное ПО для создания Web-приложений. Для применения открытых программных средств требуются специалисты высокого уровня, способные адаптировать и создать систему Web приложений.

Приведем технологические основы создания и реализации предлагаемой системы. Технология на основе программных продуктов с открытыми кодами включает, как известно, несколько этапов:

- выбор операционной системы для формирования платформы системы аутентификации и идентификации;
- разработка структуры базы данных Open LDAP;
- разработка структуры базы данных пользователей организации и обеспечение совместимости программных средств;
- разработка параметров электронного портала, настройка свойств файла локализации и файла параметров меню портала;
- настройка параметров безопасности данных портала.

Далее встает вопрос выбора архитектуры для идентификации пользователей на открытых программных кодах. В результате исследований и анализа программных средств была сформирована архитектура единой идентификационной системы, на которой можно реализовать программные модули аутентификации и авторизации пользователей и модули адаптации готовых или разработанных web - приложений, используя при этом специализированную систему серверов. Данный портал должен предоставлять единую идентификацию путем запро-

са директории типа LDAP, поддерживаемой базой данных организации. Эта идентификация сможет предоставить всем пользователям доступ к нужным приложениям. Более того, в дальнейшем можно будет, за счет добавления и адаптации программных модудей, создавать новые возможности использования единого информационного пространства. На рис. 1. показана архитектура идентификационной системы. Функциональная архитектура системы состоит из следующих модулей: модули аутентификации и авторизации пользователей;

модули аутентифицированных разработанных и готовых web приложений.

Серверная архитектура системы состоит из следующих серверов: OpenLDAP; Central Authentication Server (CAS); Web Application server (WAS); Microsoft Identity Integration Server (MIIS). Далее рассмотрим более подробнее технические решения по данным серверам системы единой аутентификации.

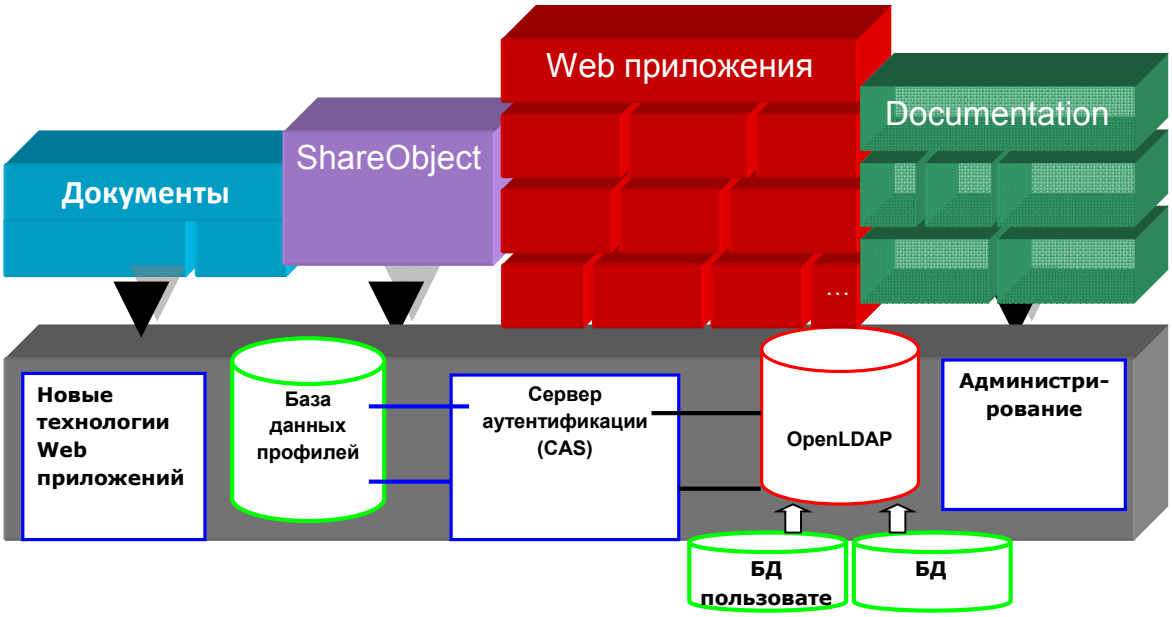

Рис. 1. Архитектура идентификационной системы на открытых кодах.

На сегодняшний день существует несколько реализаций протокола LDAP от различных фирм. Наиболее известные из них: Netscape Directory Service™, Novell Directory Service™ и Microsoft Active Directory™. Из некоммерческих реализаций LDAP наибольшее распространение получил проект OpenLDAP. Стандарт LDAP представляет собой:

- сетевой протокол для доступа к информации в директории;
- информационная модель, определяющая форму и характер информации;
- именное пространство, определяющее ссылки информации, и ее назначение;
- дистрибутивная операционная модель, определяющая, как данные могут быть доставлены.

Как известно, серверы LDAP регистрируют все документы в их порталах, где «фильтры» могут быть использованы для выбора как отдельного человека или нужной группы людей, которые вам нужны, и предоставляют лишь необходимую вам информацию. Такие Web приложения, как почта, форумы и т.д., широко распространились за последние годы, и данные приложения всегда нуждаются в авторизации. Использование директорий LDAP предоставляет единый отчет для пользователей, что, безусловно, является весомым преимуществом. Сервер OpenLDAP, после формирования информации обо всех категориях пользователей, создает иерархическую схему принадлежности пользователей по группам, категориям и присвоение прав доступа этим информационным единицам. Настройки устанавливаются системным администратором, которые предоставляют доступ к базе данных LDAP только определенному кругу лиц, и по выбору сохраняют личные документы. Серверы LDAP обеспечивают службу авторизации, так что Интернет серверы, email могут использовать единый список зарегистрированных пользователей и паролей.

Самым важным преимуществом таких систем является возможность легко и быстро адаптировать Web приложение, программный модуль, готовые программные средства с использованием отработанной технологии идентификации и авторизации и классификации web приложений.

Важный компонент системы аутентификации – это технология однократной регистрации или однократной записи (Single Sing-On). Такая система снимает необходимость многократно вводить пароли (или аутентифицироваться каким-то другим образом) при доступе к различным сервисам информационной системы, интернет – портала или корпоративной сети.

Существуют различные программные продукты, которые позволяют выполнить единую аутентификацию пользователей, но не приложений. Для решения этой нелегкой задачи можно использовать свободно распространяемый программный продукт Central Authentication Server (CAS), который позволяет произвести аутентификацию установления подлинности приложений. Осуществление протокола Single Sign-On, таким образом, гарантировано и только способ местного установления подлинности оставлен на стороне администратора сервера, за которым остается свобода выбора установки из нижеуказанных протоколов сетевой аутентификации установления подлинности.

Коротко остановимся на возможностях CAS. Процесс идентификации централизуется на одной машине, называемой CAS сервером. Эта машина является единственным автором, знающим пароли пользователей. Она играет двойную роль: во-первых, это идентификация пользователей; во-вторых, передача и подтверждение персональных данных идентифицируемых пользователей.

Кроме того, имеется развитая технология CAS – клиент, которая доставляет ресурсы только к тем клиентам, которые предварительно идентифицированы CAS сервером. При этом клиентами CAS являются: библиотеки, соответствующие наиболее широко применяемым языкам web программирования (Perl, Java, JSP, PHP, ASP); модуль Apache, применяемый, в частности, для защиты статических документов; модуль PAM, применяемый для улучшения уровня идентификации системы.

Рассмотрим теперь технологию CAS для идентификации пользователя. На рис. 2. приведен первый вход на сервер CAS через интернет - браузер. Ранее не идентифицированный пользователь (или пользователь, чья идентификация еще находится в процессе ожидания), заходя на CAS сервер, представляет идентификационную форму, в которой его просят ввести netId и пароль.

Рис. 2. Вход на сервер CAS через браузер.

Если netId и пароль подтверждаются, сервер посылает cookie, называемый TGC (Ticket Granting Cookie) браузеру. Таким образом, подтверждается аутентификация CAS. Как известно, TGC – это паспорт пользователя в отношении к CAS серверу. Его период действия (validity) ограничен временем сеанса пользователя. Это способ, которым web браузеры получают tickets (для клиентов CAS) от CAS сервера без необходимости пере-авторизации или пере-идентификации. Такой приватный файл cookie является защищенным и зашифрованным. Он является непрозрачным, т.к. все tickets связаны с CAS, и, следовательно, не содержит информацию о пользователе. Это просто сессионный идентификатор между web браузерами и CAS сервером, что позволяет защитить приложение.

Как мы знаем, для создания информационного электронного портала необходима среда разработки Web-приложений портала (WAS), которые реализуют его функционирование. В качестве программной среды WAS был выбран программный продукт Web Objects. Он, как известно, состоит из двух приложений: Web Objects Developer для разработчиков и Web Objects Deployment для серверов приложений. Для него характерны следующие особенности:

- WebObjects значительно упрощает и ускоряет процесс разработки и внедрения Java серверных приложений и позволяет создавать приложения в виде стандартных web сервисов.

- WebObjects представляет собой идеальный способ разработки, внедрения и расширения мощных web сервисов, предлагая среду для создания стан-

дартных web сервисов без написания специального программного кода.

- Созданные web-сервисы могут взаимодействовать с клиентскими приложениями, написанными на многих языках, включая Java, AppleScript, Perl и .Net, открывая тем самым возможности разработки для программистов.

- Помимо web-сервисов, WebObjects также позволяет быстро создавать приложения на основе СУБД, обладающие HTML, XML, SMIL или Java интерфейсами, в зависимости от потребностей.

Таким образом, создается устойчивый программно-аппаратный фундамент, который предоставляет все преимущества, такие, как многозадачность, поддержка симметричной много процессорности, поддержка сетевых стандартов и стандартов обеспечения безопасности и т.д. Средства удаленного администрирования позволяют производить безопасный мониторинг и администрирование всех служб из любого места ЛВС или через Интернет.

Литература

1. Технология открытых систем / В. К. Баторин, Ю. В. Гуляев, А. Б. Петров и др. – М.: Янус-К, 2004 г. – 288 с.
2. Компания MySQL AB. MySQL: руководство администратора / пер. с англ. – М.: Изд. дом «Вильямс», 2005 г. – 624 с.
3. Компания MySQL AB. MySQL: справочник по языку / пер. с англ. – М.: Диалектика, 2005 г. – 429 с.
4. Джусупова, Г.Г. Практическая реализация системы электронных услуг для ВУЗа // Журнал «Известия ВУЗов» - Бишкек, №1, 2012 г.
5. Бийбосунов Б. И., Джусупова Г. Г. Краткий обзор современных ИКТ для информационной системы вуза //Интернет-журнал ВАК КР - Бишкек, № 2, 2012 г.

Рецензент: к.т.н. Бочкарев А.И.