

МОДЕЛЬ ДОСТУПА К ВЕБ-ПОРТАЛУ НА СОВРЕМЕННОМ ПРЕДПРИЯТИИ

© 2011 А.Н. Подобрый

ФНПЦ ОАО “НПО “Марс”, г. Ульяновск

Поступила в редакцию 12.05.2011

В статье рассматриваются проблема выбора системы управления веб-порталом на современном предприятии, а также предлагается модель доступа к portalу для решения поставленной проблемы. Статья предназначена для специалистов, занимающихся внедрением автоматизированных систем управления предприятием, а также для специалистов занимающихся вопросами интеграции данных. Ключевые слова: система управления, веб-портал, предприятие, модель доступа.

Одними из основных задач предприятий являются задачи повышения эффективности производства и качества выпускаемой продукции, а также обеспечения нового качества управляемости за счет создания единого информационного пространства предприятия (ЕИПП). Этого можно достичь, лишь обладая всей достоверной оперативной информацией от всех объектов производства. Реальным инструментом для достижения поставленной цели является комплексная интеграция отдельных подсистем всего предприятия.

Передовой мировой опыт доказывает, что повышение эффективности деятельности современного предприятия возможно только при наличии единой системы, объединяющей управление финансами, персоналом, снабжением, сбытом и собственно производством. Такие системы рассматриваются как средство достижения основных целей бизнеса: улучшения качества выпускаемой продукции, снижения издержек и увеличения объема производства, занятия устойчивых позиций и получения существенных конкурентных преимуществ на рынке.

Ядром любой современной единой информационной системы является веб-портал.

Портальная технология обеспечивает единую точку входа, знакомый для пользователей и удобный в работе web-интерфейс.

“Система управления сайтом”, или CMS – последнее время один из самых распространенных способов администрирования Web портала. Современный рынок предлагает создание сайтов на различных CMS, но далеко не все предложения могут удовлетворить потребности даже среднего бизнеса [1].

Критерии выбора системы основываются на основных характеристиках современных платформ [2]:

1. Интуитивность: легка в понимании и использовании.
2. Гибкость и простота в оформлении и настройках.
3. Возможность усовершенствований посредством плагинов и модулей.
4. Оптимизация для продуктивности и скорости.
5. Безопасность.
6. Документация и сообщества.
7. Стоимость.

Как правило, современные системы управления веб-порталами включают в себя только несколько из приведенных выше характеристик, что приводит к их несовершенству. В связи с этим приходится жертвовать некоторыми характеристиками, что является основной проблемой выбора системы.

Как таковыми, основными минусами современных веб порталов становятся: безопасность, не только в плане взлома системы, но и в плане анализа (внутреннего аудита); детальное разграничение прав доступа; скорость предоставления данных; возможность объединить воедино все информационные объекты современного предприятия.

Одним из оптимальных решений данной проблемы является написание рукописной системы, которая будет удовлетворять требованиям предприятия.

Одна из таких моделей платформы представлена на рис. 1 и сочетает в себе:

- Internet Information Server (web сервер IIS),
- язык программирования *php*, подключенный как модуль ISAPI
- Корпоративная Информационная Система
- SQL сервер.

Основным отличием данной модели от существующих современных систем управления веб-порталом в том, что она основана на использовании sql-сервера не как хранилища данных, а как ядра системы.

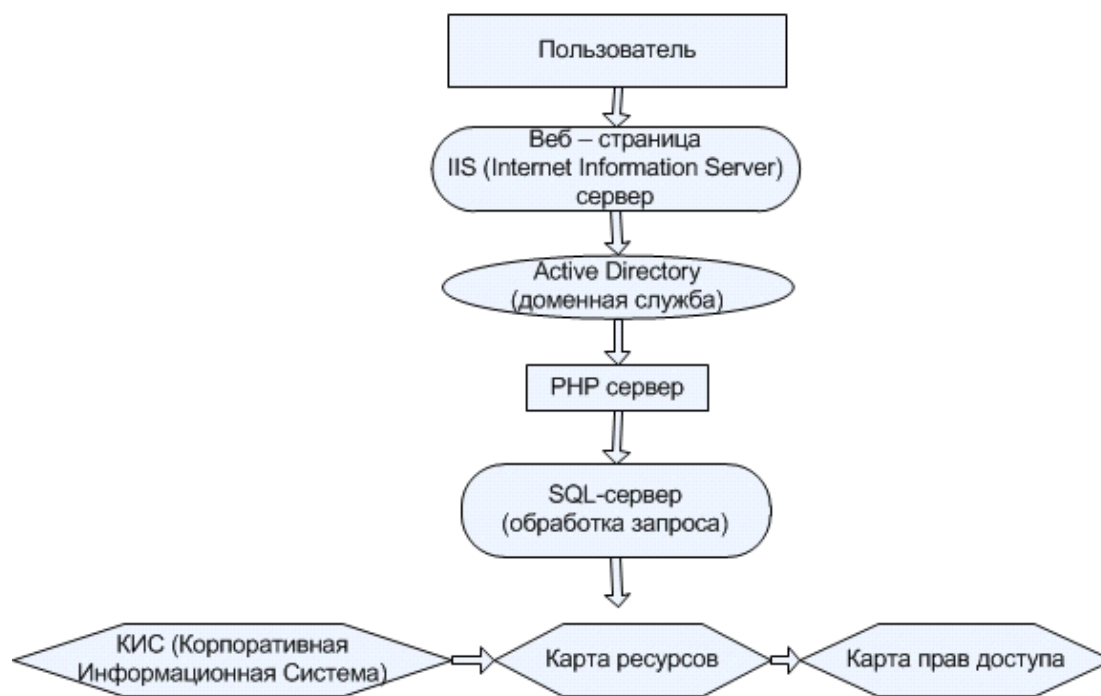


Рис. 1. Схема доступа к веб-порталу

ОПИСАНИЕ МОДЕЛИ ДОСТУПА

Модель доступа к веб-порталу можно описать как:

- 1) Аутентификация пользователя.
- 2) Идентификация пользователя.
- 3) Карта ресурсов.
- 4) Карта прав доступа.

Первый пункт осуществляется за счет связывания Internet Information Server (IIS) и доменной службы Active Directory (AD).

Данный пункт несет в себе не только определение идентификатора пользователя в операционной системе, но и определение прав доступа на «внешнем» уровне. К разграничению прав относятся: область видимости веб-страниц, доступ к каталогам, права на просмотр и редактирование каталогов.

Идентификация пользователя проходит с использованием механизма стыковки доменной службы и Корпоративной информационной системы (КИС).

Под механизмом стыковки AD и КИС понимается определение идентификатора сотрудника (табельный номер) на основании учетной записи пользователя.

Данный механизм можно разделить:

- расписание в базе данных;
- запуск функций реализованных на *vbscript* для получения данных из доменной службы Active Directory;
- запуск функций реализованных на *sql* для анализа полученных данных (учетных записей);
- сохранение необходимых (измененных) данных;

- фиксация в журнале мониторинга измененной информации;
- информирование администратора по электронной почте о результате анализа.

Таким образом, при получении учетной записи, система определяет идентификатор пользователя на уровне *sql* сервера из выверенной таблицы учетных записей, за счет регулярной проверки доменной службы.

Скелетом представленной модели является карта ресурсов, которую можно описать:

- идентификатор ресурса;
- описание ресурса;
- ссылку на место расположения ресурса;
- состояние ресурса.

Каждый ресурс представляет собой самостоятельный объект, имеющий собственное хранилище данных, расположение, списка допущенных пользователей и администраторов.

За счет данной объектной структуры и однозначного определения пользователя, можно создавать группы объектов (ресурсов) как общедоступных, так и индивидуальных. Кроме создаваемых групп существуют и зарезервированные, которые отображаются исходя из прав доступа к ресурсам, входящим в состав данных групп. Таким образом, пользователь имеет возможность самостоятельно формировать отображаемый интерфейс не только в графическом плане, но и в структурном.

Карта прав доступа является основой данной модели, так как она является соединительной частью между ресурсом, пользователем и веб-порталом.

Один из основных плюсов данного пункта это объединение всех сторонних ресурсов, создание иерархии и детальных прав доступа за счет хранения идентификаторов всех связей в базе данных.

Данный механизм состоит из:

- идентификатора ресурса;
- тип таблицы разграничения прав доступа для пользователей;
- идентификатора места хранения таблицы прав доступа пользователей в базе данных;
- тип таблицы разграничения прав доступа для администраторов;
- идентификатора места хранения таблицы прав доступа администраторов в базе данных.

Типы таблиц разграничения прав доступа можно поделить на: общие, табличные и бинарные.

Под общими понимаются зарезервированные таблицы для всех ресурсов, где разграничение прав пользователей выполнено в рамках ресурса.

Табличные типы представляют собой обычные типы данных, за исключением того, что права доступа сотрудников представлены в рамках конкретного ресурса с возможностью разграничения прав в разрезе каких либо параметров.

Бинарный тип также включает в себя разграничение прав доступа в разрезе параметров, только информация храниться в бинарных полях, которые определяются при помощи логического сложения и умножения.

Структура каждой из приведенных таблиц состоит из идентификатора пользователя, которому назначаются права доступа, сами параметры доступа, дата назначения доступа и автор, назначивший эти права.

Кроме таблиц хранения прав, в системе имеется журнал прав доступа, который заполняется вместе с приведенными выше таблицами по средствам триггеров на уровне базы данных. В данном журнале хранится вся хронология назначения прав доступа сотрудников. На основании данного механизма, возможно проводить анализ активности пользователей на любую дату, а также отследить автора, назначившего допуск.

Зарезервированными приложениями системы являются: стартовая страница, административный пул, список ресурсов.

Стартовая страница – единая точка входа для всех пользователей. Содержимое данной страницы формируется на основании прав доступа.

Административный пул – общий интерфейс для администраторов, который имеет ссылки на все страницы администрирования ресурсов, исходя из прав доступа пользователя на данные страницы.

Список ресурсов – доступный всем пользователям интерфейс, который дает детальную информацию (возможности) о каждом объекте

системы, а также возможность обратиться к администратору выбранного ресурса либо по почте, либо через систему мгновенной отсылки сообщения.

Безопасность данной модели достигается трех уровневой структурой:

1) Безопасность на уровне веб – сервера достигается с помощью веб сервера Internet Information server, доменной службы Active Directory и Корпоративной информационной системы.

Данный пункт реализуется путем настройки веб-точек на IIS сервере, а также связывания IIS сервера и AD.

Этот пункт осуществляет аутентификацию и идентификацию пользователей, контроль уровня доступа к веб-точке, контроль уровня доступа пользователей к каталогам, а также ведение журнала активности.

2) Безопасность на уровне *sql* – сервера достигается путем контроля прав доступа выбранного пользователя за счет стыковки AD и КИС, а также базы прав доступа пользователей.

Под механизмом стыковки AD и КИС понимается определение идентификатора сотрудника (табельный номер) на основании учетной записи пользователя. За счет данного механизма, обладая учетной записью получаемой из доменной службы Active Directory можно однозначно определить сотрудника предприятия и тем самым отслеживать поведение пользователя на всех этапах его работы.

3) Анализ данных активности пользователя.

Заключается в сборе всей активности, всех действий пользователя и последующем анализе данных, проводимых для контроля уровня доступа, поиска ошибок, поиска перспективы развития ресурсов.

Данный анализ необходим для регулярного аудита системы, с последующей публикацией и разбора отчета.

Для доступа к данным используется четырехуровневая клиент серверная архитектура, которая состоит из реляционной базы данных, *php* сервера и IIS сервера [4]. Эта структура позволяет не только получать данные в режиме реального времени, но и разграничивать права доступа (рис. 2).

Таким образом, представленная модель доступа к веб порталу удовлетворяет всем критериям выбора современной системы управления веб-порталом.

Она основана на использовании современных, общедоступных языках программирования. Имеет возможность роста и усовершенствования посредством готовых плагинов и модулей, либо рукописного кода. Данная модель включает в

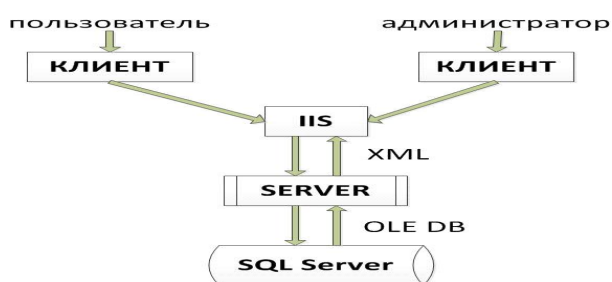


Рис. 2. Четырехуровневая архитектура доступа к данным

себя все основные уровни безопасности, необходимые для контроля прав доступа и анализа активности пользователей. А также возможность оптимизации для продуктивности и скорости за счет разграничения организационной структуры веб портала между веб сервером и сервером базы данных.

Минусом данной системы является содержание в штате предприятия опытного веб программиста, как разработчика и как сопровождающего.

Предложенная модель позволяет объединить

воедино все информационные объекты современного предприятия. Комплексная система безопасности в полной мере защитит персональные данные от утечки и от взлома. Нерывная связь между веб сервером и базы данных позволяет предоставлять информацию в кратчайшее время. Анализ данных проводит полный контроль всей системы, по результату которой можно выявить все недочеты и ошибки.

СПИСОК ЛИТЕРАТУРЫ

1. Официальный сайт журнала Webmasters "Coolwebmasters.com". URL: <http://www.coolwebmasters.com> (дата обращения 15.03.2011)
2. Официальный сайт компании "CMSList.ru". URL: <http://cmslist.ru> (дата обращения 15.03.2011)
3. Официальный сайт компании "Keep-intouch.ru". URL: <http://www.keep-intouch.ru> (дата обращения 17.03.2011)
4. Зеленков Ю.А. Введение в базы данных. Ярославль: Центр Интернет ЯрГУ, 1997. Электронное издание «Архитектура «клиент-сервер»» URL: http://www.mstu.edu.ru/study/materials/zelenkov/ch_7_1.html (дата обращения 17.03.2011)

WEB ACCESS MODEL FOR TODAY'S ENTERPRISE PORTAL

© 2011 A.N. Podobriy

Federal Research-and-Production Center Open Joint-Stock Company
"Research-and-Production Association "Mars", Ulyanovsk

In the article discusses the problem of choosing Web portal management system in modern enterprise and portal access model to solve the problem. Article is intended for professionals involved in the introduction of automated business management systems, as well as for all professionals involved in data integration.

Key words: management systems, web portal, enterprise, portal access model