

УДК 004.415.25.451.5

ИСПОЛЬЗОВАНИЕ СИСТЕМ УПРАВЛЕНИЯ СОДЕРЖИМЫМ (CMS) ДЛЯ СОЗДАНИЯ, АДМИНИСТРИРОВАНИЯ И ЗАЩИТЫ ИНФОРМАЦИОННО-НОВОСТНОГО ПОРТАЛА**Журба А.С.***Научный руководитель – к.т.н. доц. Иванов В.Г.**Харьковский национальный университет радиоэлектроники г. Харьков**Кафедра системотехники**E-mail: legan4ik@i.ua***Аннотация**

Журба А.С. Использование систем управления содержимым (CMS) для создания, администрирования и защиты информационно-новостного портала. В статье рассматривается проблема выбора, настройки и использования автоматизированной системы управления содержимым (CMS) для облегчения создания, администрирования и защиты информационно-новостного портала о науке и образовании. Особое внимание также уделяется резервированию данных web-ресурса.

Общая постановка проблемы.

В связи с развитием и коммерциализацией Интернет, с каждым годом все большую популярность набирают электронные ресурсы. Веб-сайт – это лицо и одновременно инструмент работы с клиентами для любой компании. Фирма, не имеющая в сети свой портал, просто не может нормально конкурировать с другими организациями. К тому же заметна тенденция к переходу на электронный способ заказа и оплаты покупок. Но создание и администрирование подобного рода ресурсов – задача сложная, а особенно если портал большой, с постоянно обновляющимся и изменяющимся контентом. В случае же выхода его из строя или взломе – фирма может потерять и продажи (например, интернет-магазин), и доверие многих своих клиентов. В связи с этим также возникает необходимость защиты корпоративного веб-ресурса от атак и подмены информации на нем.

Существует несколько способов создания сайта: написать вручную, купить или заказать у фирм, занимающихся этими разработками или же использовать готовые решения (CMS). Первый метод слишком сложен для неподготовленного пользователя, который не имеет знаний по созданию web-проектов, а владеет лишь своей предметной областью. Обращение к сторонней компании – самый затратный метод и чем полнее и доступнее (для освоения) фирма сделает сайт, тем дороже это обойдется. Готовая система управления содержимым CMS может быть как платной, так и бесплатной (которая во многих случаях ничем не уступает коммерческой версии). К тому же некоторые имеют открытый код, который можно изменять на свое усмотрение. По умолчанию обеспечивается базовый уровень защиты контента. С помощью плагинов и модулей система хорошо расширяется и способна выполнить практически любые требования, а интерфейс создан с расчетом на пользователя, не имеющего каких-либо познаний в web-разработке. Таким образом, организации не нужно тратить дополнительные средства на обучение персонала программированию.

Далее компании необходимо модерировать и защищать свой веб-сайт. Вручную администрировать и обеспечивать целостность крупного, динамичного портала пользователю, который вдобавок не имеет глубоких познаний в области информационной безопасности, просто невозможно. Есть несколько решений этой проблемы. Можно выделить два основных: аутсорсинг или защита своими силами. Первый метод заключается в

том, что компания нанимает специалистов в области информационной безопасности, которые и занимаются защитой портала. Некоторую часть работы можно переложить и на хостинг-провайдера. Этот метод обеспечивает высокий уровень защиты, но требует серьезных денежных вложений. К тому же некоторые организации просто не могут пригласить сотрудников извне, так как защищаемая информация может быть строго конфиденциальна.

Второй метод подразумевает обучение своих сотрудников всем тонкостям сетевой безопасности или же использование готовых систем защиты и управления контентом, которые не требуют дополнительной переквалификации персонала. Последнее гораздо предпочтительнее, так как имеется возможность сэкономить время и деньги компании. Таким образом, самым подходящим вариантом будет применение системы управления содержимым.

Также актуальна проблема восстановления информации. Если разработка велась без использования автоматизированных средств, то процесс резервирования сильно усложнится, так как сайт может быть плохо структурирован, а все операции необходимо будет делать вручную. Некоторые хостинг-провайдеры предлагают свои методы решения этой проблемы, но и они имеют ряд недостатков (например, при крупном сбое всего хостинга, все данные будут недоступны). Системы управления содержимым, благодаря различным дополнительным компонентам позволяют практически полностью автоматизировать процесс резервирования данных, который является достаточно рутинным. Это облегчает работу сотрудников фирмы, позволяя им не тратить время и усилия на регулярные операции, а компании помогает сберечь средства и всегда иметь возможность восстановить работу и данные сайта при сбое.

В результате можно сделать вывод, что решением проблемы создания, администрирования, защиты и наполнения содержимым веб-портала является использование и настройка для собственных нужд системы управления контентом.

Постановка задачи исследования.

В настоящее время существует множество CMS, которые отличаются функциональной оснасткой, ориентированных на различные нужды, с открытым и закрытым кодом, бесплатные и платные. Большое распространение получили некоммерческие продукты, которые не уступают, а иногда и превосходят, Shareware-разработки по многим параметрам. В данной работе необходимо было рассмотреть возможность применения таких систем управления контентом, и выбрать такую, которая бы была максимально простой в обслуживании и настройке, но в то же время надежной и хорошо расширяемой с помощью модулей, плагинов, дополнительных компонентов. Простота, предъявленная к системе, обусловлена, прежде всего, тем, что портал рассчитан на людей, не владеющих знаниям в области разработки сайтов и обеспечения их безопасности. Расширяемость системы управления сайтом о науке и образовании необходима для того, чтобы обеспечивать дополнительные сервисы:

- голосование;
- подписка на рассылку;
- статистика посещений;
- поиск по сайту;
- ленты новостей;
- баннеры;
- последние новости.

Также прослеживается тенденция к автоматизации операций защиты и модерирования контента. Особое внимание теперь уделяется безопасности web-ресурсов, в связи с участвовавшими случаями правонарушений в сети. Самые распространенные проблемы с защитой сайтов – это различного рода атаки (SQL инъекция, межсайтовый скриптинг (XSS),

отказ в обслуживании (Denial of Service) и т.д.), а также недостаточная аутентификация и авторизация пользователей.

В данной работе анализировались существующие CMS и возможности их расширения для защиты информационно-новостного портала о науке и образовании, который должен соответствовать следующим условиям:

- многоуровневое разграничения прав доступа для различных пользователей портала;
- защита от SQL и PHP инъекций злоумышленников;
- запрет на многократное дублирование сообщений;
- ведение и отправка почтой логов администратору;
- бесплатное распространение управляющей системы;
- удобное обновление для обеспечения лучшей защиты.

На случай выведения системы из строя должно быть предусмотрено средство быстрого резервного копирования и восстановления. При использовании Joomla без дополнительных компонентов и модулей сделать копии базы данных MySQL и файлов системы придется вручную, а именно:

- отдельно копировать MySQL базы данных;
- возможность игнорировать выбранный пользователем контент (например, кэш и временный данные) при копировании файлов сайта;
- синхронизировать состояния базы и состояния файлов проекта.

К этому можно добавить также, что на площадке, где необходимо выполнить резервирование может не быть доступа по SSH, FTP, инструментов для работы с базами данных.

Таким образом, для рационализации процесса создания резервных копий необходимо чтобы:

- простота эксплуатации и автоматизация рутинных операций;
- лёгкая установка и настройка системы резервного копирования;
- совместное хранение файлов базы и файлов проекта;
- возможность интеграции с админ-панелью Joomla;
- оперативное и легкое восстановления исходного состояния системы.

В итоге должна быть выбрана CMS соответствующая всем требованиям по сервисам и безопасности для данного информационно-новостного портала о науке и образовании.

Решение задачи и результаты исследований.

Для решения поставленной задачи был проведен сравнительный анализ некоторых систем управления контентом, их инструментария и направленности. Наиболее подходящей, учитывая простоту, бесплатность и достаточную ее защищенность, была выбрана CMS Joomla. Ее основные особенности:

- известная и популярная CMS (согласно рейтингами), доказавшая свою пригодность в любых проектах;
- большое количество документации в сети Интернет;
- является свободным программным продуктом;
- имеет хорошую расширяемость, которую обеспечивают дополнительные модули, плагины, компоненты;
- система шаблонов позволяет легко изменять внешний вид сайта;
- имеет дружелюбный (благодаря визуальному редактору WYSIWYG) и гибко настраиваемый интерфейс, поэтому с ним легко работать как новичку, так и профессионалу;
- возможность изменять исходный код для более тонкой настройки системы под разрабатываемый проект;
- возможность локализации.

Что же касается защиты, то Joomla имеет:

- многоуровневая аутентификации пользователей/администраторов, что позволяет ограничить права доступа к определенным разделам сайта;
- большое количество дополнительных модулей и плагинов, которые смогут еще больше повысить безопасность;
- журналирование;
- удобная система обновлений;
- Joomla Security Center – бюллетень безопасности, в котором эксперты в области защиты информации публикуют свежие новости, касающиеся проводимых работ, связанных с обеспечением безопасности Joomla. Там же можно сообщить о найденной ошибке, которая непременно будет исправлена в новых версиях.

Для Joomla необходим Apache в комбинации с PHP и MySQL. Это довольно стандартный и простой набор. К тому же сейчас большинство дешевых хостингов используют именно это решение.

Часть сервисов сайта были обеспечены с помощью стандартных средств Joomla (последние новости, система авторизации, баннеры). Некоторые специфические функции, реализованы благодаря сторонним плагинам и модулями. Например, безопасность. Необходимо было рассмотреть возможность увеличения существующего уровня безопасности с помощью комплекса сторонних компонентов и модулей. Первоначально был использован дополнительный компонент GuardXT. Он по расписанию может делать анализ файловой системы на уязвимости, регулярно отслеживает изменения файлов, показывает новости безопасности. Кроме того, GuardXT:

- проверяет актуальность версий компонентов;
- выполняет контроль безопасности (конфигурации Joomla, параметры настройки PHP и т.д.);
- результаты работы выводит в удобной форме, есть возможность устранить некоторые проблемы прямо из интерфейса компонента.

С помощью него были обнаружены некоторые недочеты (проход защиты тайм-аута, отсутствие проверки для JEXEC и т.д.), которые устранились после обновления Joomla до актуальной версии.

Далее был установлен компонент JDefender. С его помощью можно:

- предотвратить SQL инъекцию;
- избежать PHP инъекции;
- запретить flood-атаку;
- почтой отправлять администратору логи;
- заблокировать IP адреса нарушителей.

Если же злоумышленник повредил контент портала, то для восстановления информации из резервной копии, которую ранее сделал администратор, будет использоваться плагин LazyBackup 2. Его основные особенности:

- автоматически производит резервное копирование MySQL базы данных;
- есть возможность отправки архива БД на e-mail;
- поддержка расписания (планировщик);
- gzip сжатие с защитой паролем;
- легкая установка.

Для более сложных операций с восстановлением и резервированием данных использовался компонент JoomlaPack. Его особенности:

- AJAX-резервное копирование (как сайта, так и базы данных) и AJAX-восстановление;
- возможность выбора папок, файлов сайта и таблиц базы данных для резервирования;
- создание резервной копии базы данных и файлов проекта в один архив;
- сжатие в формате zip, gzip;

- автоматический режим резервного копирования;
- поддержка различных браузеров;
- совместимость с разными версиями MySQL (4.x – 5.x);
- возможность быстро переместить сайт с одного компьютера на другой;
- позволяет управлять резервными копиями, например, удалить или скопировать их на жесткий диск;
- настройки сохраняются в файл конфигурации;
- сохраняет резервную копию в папку сайта.

Компонент JoomlaPack прост в освоении, что позволяет даже неподготовленному пользователю резервировать и восстанавливать данные. К тому же весь процесс наглядно отображается на странице, а аварийные сбои не происходят по причине таймаута сервера, а так же из-за того, что есть ограничение размера памяти для скрипта.

Выводы.

В результате работы, система наполнения содержимым Joomla была применена для создания, администрирования и защиты информационно-новостного портала о науке и образовании. Благодаря тому, что были использованы не только стандартные средства, а и дополнительные модули, в комбинации с тонкой настройкой необходимых элементов, время на разработку сайта было уменьшено, по сравнению с табличной версткой, была обеспечена хорошая локализация и возможность быстро наполнять контентом портал даже людям, не имеющим опыт работы с web-разработками. При этом денежные затраты на реализацию проекта сведены к минимуму, так как сама система управления контентом бесплатна, а переквалификация персонала не потребуется.

Особое внимание было уделено защите. С помощью комплекса плагинов и компонентов, был обеспечен необходимый уровень безопасности. На первом этапе были устранены небольшие бреши в защите портала. Затем безопасность была увеличена средствами стороннего дополнительного компонента JDefender, который запрещал SQL и PHP инъекцию, а также flood-атаку. Встроенные средства авторизации и аутентификации защищают контент и административную панель от несанкционированного доступа. При дальнейшей поддержке портала необходимо логично и четко разграничить доступ к ресурсам и админ-панели сайта, а также следить за обновлениями компонентов, модулей, плагинов, системы Joomla и всегда устанавливать актуальные версии для обеспечения наилучшей защиты.

Для резервирования данных были установлены дополнительные компоненты, которые позволяют автоматизировать эти рутинные операции. Помимо основной функции восстановления информации в случае сбоя или атаки, решаются и дополнительные задачи, такие как дублирование и передача данных на другие рабочие станции.

Список литературы

1. Колисниченко Денис Николаевич Joomla! 1.5. Руководство пользователя. — М.: «Диалектика», 2009. — С. 224.
2. Дэн Рамел Joomla! Самоучитель = Beginning Joomla! From Novice to Professional. — Санкт-Петербург: «БХВ-Петербург, 2008. — С. 448.
3. Хаген Граф Создание веб-сайтов с помощью Joomla! 1.5 = Building Websites with Joomla! 1.5. — М.: «Вильямс», 2009. — С. 304. — ISBN 978-5-8459-1506-1
4. Бэрри Норт Joomla! Практическое руководство = Building a Successful Joomla! Powered Website. — М.: «Символ-Плюс, 2008. — С. 448.