By results of program complex working, reports of the established type are forming, it is used in different control, analysis levels, also in levels of tariffs approval on producing and transfer of heat power. It was also taking into account, that in the framework of **PT-Q-1** program complex have to be formed special program procedures, which provides the possibilities of providing the wide range calculation experiments with different initial data. It gives the possibility of widespread using of the complex during task solving of prognosis and training.

1. Semenov V.G. Heating in current market conditions. Nadezhnost i bezopasnost ehnergetiki [Reliability and safety of power engineering], 2012. V. 2, pp. 4–11. (in Russian)
2. Bogdanov A.B. The history of the ups and downs of the heating system in Russia. Ehnergoberezhnie [Energy saving], 2009. V. 3, pp. 2–9. (in Russian)
3. Order of the Federal Tariff Service dated June 13, 2013 N 760-e "On Approval of Methodological Guidelines for the Calculation of Regulated Prices (Tariffs) in the Sphere of Heat Supply (as amended on May 27, 2015)". (in Russian)
4. Arunyants G.G., Voronin T.A., Ayrapetov S.A. The concept and features of the PT-Q-1 software package for the automated formation of tariffs in the field of heat supply. Nauka i biznes: puti razvitiya [Science and business: the way of development], 2016. V. 3 (57), pp. 66-73. (in Russian)
5. Arunyants G.G., Voronin T.A. On the accounting of heat losses in the automated formation of tariffs in the system of regulation of the heat supplying complex in the Kaliningrad Region. Sovremennaya nauka: aktualnyie problemyi teorii i praktiki. Seriya «Estestvennyie i tehicheskie nauki» [Modern science: actual problems of theory and practice. Series "Natural and technical sciences"], 2016. V. 8, pp. 56-63. (in Russian)
6. Denisov D.V. Prospects for the development of cloud computing. Prikladnaya informatika [Applied Informatics], 2009. V. 5(23), pp. 52-58. (in Russian)
7. SaaS model - in the world and in Russia. BYTE Rossiya. Upravlenie IT-infrastruktur [BYTE Russia. IT infrastructure management], 2008. V. 10(119), pp. 122-134. (in Russian)
8. Hartl, M. Ruby on Rails Tutorial. 3rd ed. Addison-Wesley. 2015. 664 p.
9. Vaswani V. Zend Framework, A Beginner's Guide. 2010. 445 p. (Russ. ed.: Vaswani V. Zend Framework. Zend Framework. Razrabotka veb-prilozheniy na PHP. St. Petersburg, Peter, 2012. 432 p.).
10. Shasankar K. Zend Framework 2.0 by Example: Beginner's Guide. 2013. 228 p. (Russ. ed.: Shasankar K. Zend Framework 2.0. Razrabotka veb-prilozheniy. St. Petersburg, Peter, 2014. 208 p.).

Грушкина К.А.

Анализ DOS уязвимостей в системе управления контентом Joomla!

*Северо-Кавказский Федеральный университет
(Россия, Пятигорск)*

doi: 10.18411/sr-10-04-2018-47

idsp: 000001:sr-10-04-2018-47

Аннотация

В статье приводится описание Content Management Software (CMS), которая благополучно вытесняет традиционные технологии разработки web-сайтов. Пример одной из таких систем - Joomla!, которая является достаточно популярной в наше время. Приводится краткое описание возможностей данной системы, а также с точки зрения системы безопасности. В качестве иллюстрации одной из уязвимостей Joomla! приводится DOS-атаки, которые приводят к недоступности сервера, а для пользователя – недоступности web-сайтов.

Ключевые слова: Content Management Software, CMS, уязвимости, DOS-атака.

В современном мире большинство организаций имеют web-сайт в сети Интернет. Вследствие чего стали востребованы средства, обеспечивающие автоматизированное создание, поддержание и развитие web-сайтов. Традиционные статистические технологии сайтов для каких-либо изменений требуют привлечения программистов, что, конечно же, является не удобным.

Content Management Software (CMS) благополучно помогает отказаться от традиционных технологий в разработке web-сайтов. CMS является программным комплексом, который автоматизирует процессы управления сайтом, как в целом, так и его отдельными составляющими. CMS не требует специальных знаний в разработке сайтов, все что нужно это навыки оформления текста, которыми обладает практически каждый пользователь текстового редактора. При вызове страницы происходит запрос в базу данных и выгрузка необходимой информации, на основе которой генерируется web-страница.

Вопреки своим многим достоинствам, CMS часто являются причиной несанкционированного доступа к данным. Существует целый ряд уязвимостей CMS, который ставит под угрозу безопасность всего сервера.

В данном исследовании хочется рассмотреть популярную систему управления контентом Joomla!, обращая особое внимание на DOS-уязвимости данной системы.

Joomla! достаточно популярная система управления контентом, за свое недолгое существование она соревнуется с CMS Drupal, достаточно успешно. За все годы своего существования Joomla! не выходила из тройки лидеров. Разбираясь, можно говорить, то Joomla! – это набор скриптов, которые написаны на языке программирования PHP, с использованием MySQL. Во всех веб-приложениях есть две части разработки и выполнения кода: серверная и клиентская. Для использования серверной части Joomla! необходима установка локального сервера DENWER.

Joomla! является программным средством с открытым исходным кодом, который может просмотреть любой желающий. У этого есть ряд недостатков, которые связаны с системой безопасности. Такой код полностью просматривается, и злоумышленник может найти уязвимости и производить атаки по ним на всех сайтах Joomla! . Однако, Joomla! является большим сообществом, в котором система безопасности представляет собой непосредственное обновление и доработку ошибок самой CMS системы. Если были обновления безопасности, значит были найдены уязвимости, о которых стало известно соответственно в скором времени ими кто-то воспользуется. Для предотвращения этого, необходимо своевременно обновлять Joomla! до последней версии, что является основой защиты Joomla!.

Целью DOS-атаки является доведение до отказа вычислительной системы, создание таких условий, при которых пользователи не могут получить доступ к серверам, вследствие чего доступ к сайту, либо доступ будет затруднен. DOS-атаки являются опасным видом, которые связаны с ограниченными мощностями сервера, на котором размещен сайт. Суть данной атаки состоит в отправлении на сайт одновременно большого количества запросов, достаточное для того, чтобы сервер перестал справляться с их обработкой, вследствие чего сайт станет недоступным для обычных посетителей. Естественно, такие атаки не могут быть постоянными, а длятся некоторое время, и часто продолжительное.

Существует еще один вид DOS-атак на Joomla! сайтах, который заключается в желании человека создать копию какого-либо сайта для личных целей. Этот человек может даже не иметь представления, как работает данный сайт. Он находит программу, которая «обещает» скачать сайт целиком. Он ее устанавливает, запускает и указывает нужный для копирования сайт. Данная программа работает как индексирующие роботы поисковых систем: заходит на главную страницу нужного сайта, скачивает ее, после чего переходит по всем внутренним ссылкам на другие страницы, скачивает и их тоже, с этих страниц переходит на следующие и скачивает их и т.д. При этом получается подобие

DOS-атаки, при котором большое количество запросов идет с одного адреса. Так было с сайтом wedal.ru. Для защиты сайта от такого вида атак необходимо посчитать количество запросов с одного и того же IP-адреса за определенное время, если оно будет превышать допустимое значение необходимо заблокировать этот адрес.

На сегодняшний день у Joomla! есть ряд уязвимостей, но, несмотря на это она является самой передовой и стабильной из ведущих систем управления контентом. Производители Joomla! уделяют достаточно большое внимание защите данных пользователя и администратора. В большинстве случаев пользователям Joomla! для того, чтобы себя обезопасить, достаточно обновить систему. Пользователи могут сообщить и найденных уязвимостях, потому что исходный код является открытым, что помогает разработчикам Joomla! своевременно исправлять их.

1. Савельева Н. Системы управления контентом (рус.) // Открытые системы. 2004. №4.
2. Колисниченко Д.И. Движок для вашего сайта. – СПб.: БХВ-Петербург, 2008. – 368 с.
3. Плагины и расширения для Joomla! [Электронный ресурс]. URL: <http://extensions.joomla.org/extensions/ads-a-affiliates/jobs-a-recruitment/7550>
4. Joomla!: Документация [Электронный ресурс] / Режим доступа: <http://www.joomla.ru/documentation.html>

Мельниченко В.Н.

Что такое корпоративная система управления проектами и плюсы от её внедрения

*Российский университет транспорта (РУТ (МИИТ))
(Россия, Москва)*

doi: 10.18411/sr-10-04-2018-48

idsp: 000001:sr-10-04-2018-48

Аннотация

В данной статье рассмотрено понятие корпоративной системы управления и основные её элементы, а так же плюсы и эффективность от внедрения КСУП.

Ключевые слова: КСУП, корпоративная система управления проектами, управление проектами.

Abstract

In this article, we will review the concept of the corporate project management system and its elements, as well as the advantages and effective implementation.

Key words: project management, project management system.

В двадцать первом веке управление проектами является не нововведением как в двадцатом, а хорошо действующим подходом управления предприятием. В настоящее время современные компании имеют большое количество различных задач и становится всё труднее принимать обоснованное решение о выполнении того или иного проекта, а так же контролировать его выполнение и планировать распределение ресурсов. С решением данных проблем хорошо зарекомендовала себя корпоративная система управления проектами (КСУП).

Корпоративная система управления проектами (КСУП) – комплекс организационных, методических и информационных средств, поддерживающих процессы управления проектами в организации.

Основными элементами КСУП являются: методология, специализированная структура, информационная система управления проектами (ИСУП), обучение персонала.