ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ СДО MOODLE

А.В. Гуринович[1], Л.А. Глухова[2]

[1] *Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, altmind@gmail.com*

[2] *Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, glukhova@bsuir.by*

Abstract. Moodle is one of the most popular E-learning solutions in the world. It is architectured as a web-application written in php and usually operates with mysql DBMS in UNIX-like operation system. Public availability of source code, high awareness of security issues in technological stack, insufficient training of technical staff and lack of formal security audit are main reasons of possible security accidents during expluatation of Moodle. This paper describes basic rules necessary to ensure moodle secure usage in correspondence education applications.

Известно, что безопасность систем дистанционного обучения (СДО) является составной характеристикой, зависящей от следующих факторов [1]:

– физической безопасности сервера приложений и каналов данных;
– механизмов обеспечения безопасности уровня операционной системы (ОС);
– механизмов обеспечения безопасности прикладного уровня;
– разделения ролей и прав пользователей, контроль доступа;
– качества процедур сопровождения СДО (резервирования, аудита, обновления);
– политики управления и эксплуатации СДО;
– безопасности канала клиент-сервер и безопасности ЭВМ конечного пользователя.

Физическая безопасность сервера приложений и каналов связи необходима для обеспечения доступности СДО. Использование shared хостинга, хостинга сервера приложений на мощностях эксплуатирующей организации или на неподконтрольных ресурсах создают угрозу безопасности данных и доступности СДО. Надежной практикой является хостинг приложения на ресурсах специализированной организации, обладающей разрешениями на оказание телематических услуг, а так же всеми необходимыми сертификатами для обработки личных данных.

Механизмы безопасности уровня ОС нужны для разграничения доступа различных приложений к обрабатываемым данным и разделяемым ресурсам. При нарушениях в механизме разделения прав уровня ОС возможен неавторизованный доступ и модификация данных СДО. Хорошо показавшей себя практикой является использование виртуализации, которая надежно изолирует сервисы и приложения, работающие в рамках одной вычислительной машины.

Механизмы безопасности прикладного уровня заключаются в корректной настройке сервера приложений СДО и среды исполнения (php, mysql). Общие рекомендации по настройке среды приведены в [2]. Основными пунктами для проверки являются настройки php (параметры register_globals, magic_quotes_gpc, display_errors), а так же настройки в панели управления moodle.

Важным аспектом является четкое разграничение прав доступа для различных категорий пользователей. СДО Moodle позволяет осуществлять гибкую настройку прав и полномочий различных пользователей, однако при неверной настройке к защищенным данным могут получить доступ пользователи без необходимых полномочий.

Критически важным является наличие процессов обслуживания системы. Обслуживание должно производиться регулярно и по постоянному сценарию. Распространенной практикой является использование планировщика задач для выполнения задач резервного копирования, обновления системы и оперативного анализа событий, произошедших в системе за предыдущий период обслуживания.

Политика управления и эксплуатации СДО также является важным аспектом обеспечения безопасности и определяет такие характеристики как [3]:

– требования к именам пользователей и сложность паролей используемых пользователями;

– доступность СДО поисковым системам;

– возможности, содержание и размер загружаемых файлов;

– возможности вставки управляющего содержимого в контент, загружаемый пользователем;

– наличие и доступность публичной зоны сайта.

Безопасность канала клиент-сервер может быть обеспечена использованием протокола HTTPS для передачи всей информации от клиента к серверу. Важным является использование подписи авторизованного центра сертификации для удостоверения сторон, участвующих в обмене информацией.

Для обеспечения безопасности установленной системы, moodle предоставляет специальные технические средства. В стандартной поставке moodle содержится отчет по безопасности (Security Report), который считывает настройки сервера и показывает, какие из настроек могут привести к потенциальным уязвимостям в системе.

Обеспечение безопасности СДО является простой задачей, однако требует системного подхода к определению векторов угроз и обслуживания работающей системы.

Для оценки степени безопасности разворачиваемой системы а также для управления уровнем безопасности могут применяться отраслевые стандарты и другие документы, используемые для оценки безопасности работы собственного ПО и обработки данных. Это могут быть, например, ISO/IEC 27001:2005, US-EU Safe Harbor и технические регламенты, описанные в ФЗ-153 РФ.

В докладе анализируются методы обеспечения безопасности не только СДО moodle, но и информационной системы, в которой работает СДО; подробно рассматриваются основные точки уязвимостей СДО, использующих Moodle, и виды уязвимостей. Выполняется оценка уровней уязвимости СДО при использовании различных методов обеспечения безопасности, даются практические рекомендации по устранению каждого из видов уязвимостей.

Литература

1. OWASP Attack Surface Analysis Cheat Sheet [Электронный ресурс]. Режим доступа: https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet (дата обращения: 31.10.2013).

2. Moodle Security recommendations [Электронный ресурс]. Режим доступа: http://docs.moodle.org/24/en/Security_recommendations (дата обращения: 31.10.2013).

3. Darko Miletic, Moodle Security, Birminham, Packt Publishing, 2011