ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ CMS-СИСТЕМЫ УПРАВЛЕНИЯ ПРОЕКТОМ

студ. В.В. Лебедь, канд. техн. наук, проф. А.М. Филоненко,
Национальный технический университет "Харьковский политехнический институт", г. Харьков.

Сайт или проект – это веб-приложение, работающее на серверном программном обеспечении операционной системы и использующее её сервисные функции. Управление сайтами идет с компьютеров администратора и пользователей, наделенных данной функцией, имеющими свои операционные системы и программы, а, соответственно, и уязвимости.

Безопасность веб-проекта заключается: в безопасности информационной среды, в безопасности системы управления проектом, в безопасности информационной среды администрации и, наконец, в безопасности сторонних веб-приложений. В комплексную безопасность веб-проекта входят такие составляющие обеспечения информационной безопасности, как защищенность информационной среды веб-сервера, средства защиты компьютеров администратора и пользователей управляющими сайтом.

Для безопасности кодов CMS-системы управления проектов используется несколько алгоритмов. Наиболее оптимальный и распространенный, придерживается следующей архитектуры безопасного Web-приложения: одна система входа и авторизации; одинаковый, в сущности, бюджет для каждого пользователя; разноуровневое ограничение прав для доступа; независимая система контроля за доступом от бизнес-логики страниц; обязательное шифрование информации при приеме и передаче; постоянное обновление; ведение журналов отчета; соблюдение политики работы с внешними и переменными данными; применение методики двойного контроля за критически опасными участками кода.

Чтобы уберечь CMS своего сайта от взлома, необходимо придерживаться следующих правил:

– регулярно обновлять CMS;

– скрывать тип и версию установленной CMS и ее плагинов;

– проверять все без исключения данные, которые пользователь может ввести на страницах сайта или передать серверным скриптам при помощи запросов;

– использовать минимум сторонних скриптов, модулей, расширений;

– вебмастера и администраторы должны работать в безопасном окружении и выполнять правила безопасной работы в интернете.