УДК 621.391.037

С.С. Мешечко, В.Я. Певнев, В.А. Погорелов

*Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков*

# МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ CMS WORDPRESS

*WordPress — идеальная платформа для публикации, ориентированная на красоту, поддержку стандартов и удобство использования. На сегодняшний день Wordpress как никогда популярен. Блоги, минисайты, а то и целые порталы — всё это строится на основе такого удобного движка-конструктора как Wordpress. Но за удобностью и лёгкостью освоения кроются, прежде всего, вопросы, связанные с безопасностью вашего сайта. Большая распространённость — большее внимание злоумышленников. В статье проведен анализ методов и способов защиты CMS WordPress. Описаны детальные действия по повышению устойчивости системы к DDos-атакам. Расписаны основные ошибки при администрировании сайта.*

***Ключевые слова:*** *безопасность, защита, надежность, администрирование, пароли, поддержка.*

## Введение

Развитие инфокоммуникационных технологий позволяет резко увеличить скорость обмена информации и ее передаваемый объем. Это приводит к необходимости увеличения затрат на обеспечение информационной безопасности создаваемых сайтов и разнообразных веб-приложений. Обеспечение кибербезопасности, как составляющей информационной безопасности, достаточно сложная задача, включающая в себя решение вопросов конфиденциальности, целостности, доступности. Основную угрозу несет в себе возможность несанкционированного доступа к информации с целью ее модификации или уничтожения. Такой доступ позволяет производить действия с исполнительными устройства вне зависимости от показания соответствующих датчиков, разрушение программного кода и т.п.

Хакерские атаки на всевозможные веб-приложения стали обыденными вещами, но реальных методов защиты не существует. Обеспечение безопасности является одной из основных задач разработчиков и требует не стандартных решений. Одним из таких решений было предложено в системе создания и управления сайтами WordPress. Идея такого решения заключается в том, что при установке нового блога система создает аккаунт администратора с уникальным случайно сгенерированным в реальном времени паролем. То позволяет блокировать всеобщий доступ к настройкам системы, контролируя его с помощью страницы авторизации.

В предлагаемой статье рассмотрены на вопросы усиления безопасности WordPress — как административной панели, так и настроек блога, подразумевая все содержимое папки «wp-admin», которое отображается только после авторизации. Авторами сознательно выделена фраза "после авторизации" — это подчеркивает то, что только пароль отделяет хакера и администратора всего вашего блога или сайта! А защита пароля определяется его размером и символами, которые используются при его наборе.

**Целью статьи** является анализ существующих методов защиты системы создания и управления сайтами WordPress.

## Результаты анализа

**1. Переименуйте папку wordpress.** Начиная с версии 2.6, стало возможным изменять путь к папке wp-content. К сожалению это до сих пор неприменимо к папке wp-admin. Думающие о безопасности блоггеры смирились с этим и стали надеяться, что это станет возможным в будущих версиях. Пока этого не случилось, возможно следующее альтернативное решение проблемы. После распаковки архива с файлами WordPress, создается папка «WordPress». Необходимо переименовать папку (в идеале во что-то непонятное вроде "*wordpress_live_Ts6K"*) и после этого настроить соответственным образом файл wp-config.php, который находится в корневой директории [1]. Что дает это изменение?

- все файлы WordPress не будут смешаны с другими файлами в корне сайта, таким образом повысится ясность корневого уровня;
- множество копий WordPress может быть установлено параллельно в папке с разными именами, исключая их взаимодействие, что делает это идеальным для тестирования;
- административная зона (и весь блог в целом) больше не находится в корневой папке и для проведения каких-либо действий по взлому сначала ее нужно будет найти. Это проблемно для людей, но что касается ботов – вопрос времени.

**Примечание:** Если системные файлы WordPress больше не находятся в корневой директории, и имя папки инсталяции изменено в соответствии с рекомендациями, описанными выше, блог будет все равно доступен по адресу wp-config.ru. Зайдите в раздел «Общие настройки (General settings)» вашего блога и введите в поле «WordPress address (URL)» реальный адрес блога на сервере.

**2. Усовершенствуйте файл wp-config.php.** Конфигурационный файл WordPress wp-config.php

содержит в себе некоторые настройки сайта и информацию для доступа к базе данных. Также там другие настройки, касающиеся безопасности (они представлены в списке ниже). Если таких значений в этом файле нет, или же имеются только установленные по умолчанию, вам необходимо, соответственно, добавить или изменить их: ɾлючи безопасности**:** начиная с версии 2.7, в WordPress есть четыре ключа безопасности, которые должны быть правильно установлены. WordPress спасает вас от необходимости выдумывать эти строки самому, автоматически генерируя правильные ключи с точки зрения безопасности. Вам просто нужно вставить ключи в соответствующие строки файла wp-config.php. Эти ключи являются обязательными для обеспечения безопасности вашего блога [1]. Префикс таблицы заново установленного WordPress блога не должен быть стандартным **«wp_».** Чем больее сложным будет значение префикса, тем менее вероятна возможность несанкционированного доступа к таблицам вашей MySQL базы данных. Плохо**:** *$table_prefix = 'wp_';*. Намного лучше: *$table_prefix = 'wp4FZ52Y_'***.** Если у вас на сервере доступно **SSL** шифрование, рекомендуется включить его для защиты административной зоны. Это можно сделать, добавив следующую команду в файл wp-config. php: *define('FORCE_SSL_ADMIN', true);*

**3. Переместите файл wp-config.php.** Также начиная с версии 2.6, WordPress позволяет перемещать файл wp-config.php на высший уровень. По причине того, что этот файл содержит в себе намного более важную информацию, чем какой либо другой, и потому что всегда намного сложнее получить доступ к корневой папке сервера, имеет смысл хранить его не в той же директории, где и остальные файлы. WortdPress автоматически обратится к высшей папке в поиске файла wp-config.php. Любые попытки пользователей самим настроить путь бесполезны.

**4. Защитите файл wp-config.php.** Не все ISP серверы позволят вам передавать данные на более высокие уровни, чем корневая директория. Другими словами, не у всех хватит прав для осуществления предыдущего шага. Или по другим причинам: например, если у вас несколько блогов, при определенной структуре папок у вас не получится положить в корень все файлы, так как их имена будут совпадать для каждого из блогов. В этом случае мы можем запретить доступ к файлу wp-config.php извне при помощи файла .htaccess [2].

Очень важно убедиться, что файл .htaccess находится в той же директории что и файл wp-config.php. процесс, драйвера, которые он запрашивает, влияние на другие процессы и прочие параметры, которые каждый HIPS реализует по-своему.

**5. Удалите учетную запись администратора.** Во время процесса установки WordPress создает учетную запись администратора с ником «admin» по умолчанию. С одной стороны это вполне логично, с другой — пользователь с известным ником, т.е. ID — 1, обладающий административными правами, является вполне предсказуемой мишенью для хакеров с их программами подбора паролей. Отсюда следует совет: Создайте еще одного пользователя с административными правами и вашим ником. Завершите сеанс работы. Залогиньтесь под новым аккаунтом. Удалите учетную запись "admin".

Если у вас не новый блог и под учетной записью admin вы уже публиковали посты или комментарии, то из предложенных вариантов в момент удаления, выберите пункт «Связать все записи и ссылки с:» и выберите имя нового пользователя: В идеале желательно чтобы логин нового пользователя отличался от отображаемого имени пользователя в постах, чтобы никто не узнал ваш логин.

**6. Выберите сильный пароль.** Вероятность и частота потенциальных атак прямо зависит от популярности блога. И желательно до этого момента быть уверенным, что в вашем сайте не осталось слабых звеньев в цепи безопасности.

Чаще всего именно пароли являются самым слабым звеном в этой цепи. Почему? Способы выбора пароля у большинства пользователей зачастую необдуманны и беспечны. Многие проведенные исследования показали, что большинство паролей — односложные существующие слова, набранные строчными буквами, которые не сложно подобрать. В программах подбора паролей существуют даже списки самых часто используемых паролей. В WordPress реализован интуитивно понятный индикатор стойкости набираемого пароля, который показывает цветом его уровень сложности[3]. Мы рекомендуем использовать как минимум семь символов, комбинировать строчные и прописные и использовать служебные символы, такие как! "? $ % ^ & ( ).

**7. Защитите папку «wp-admin».** Следуя пословице «две головы лучше одной», существует способ вдвое усилить защиту административной зоны. Защита регулируется файлом **.**htaccess**,** который должен находится в папке «wp-admin» вместе с файлом .htpasswd, который хранит логин и пароль пользователя. После обращения к папке, вам нужно будет ввести логин и пароль, но разница в том, что в этом случае авторизация контролируется на стороне сервера, а не силами самого WordPress.

**8. Запретите отображение ошибок на странице авторизации.** Страница авторизации WordPress — это дверь в административную зону вашего блога, которая становится доступна после безошибочного прохождения верификации. У каждого пользователя существует бесконечное количество попыток авторизации, и каждый раз по умолчанию услужливый WordPress указывает, в чем именно была ошибка. То есть, если введенный логин окажется неверным — WordPress так и скажет. Это удобно для пользователя, но также и для хакера[3]. Несложно догадаться, как быстро сокращается вероятность подбора комбинации логина/пароля, когда система указывает что именно введено неверно. Простая строка кода,

поможет решить эту проблему, достаточно добавить её в файл functions.php вашей темы:

**9. Поддерживайте актуальные версии.** Как правило разработчики WordPress очень быстро реагируют, если находят уязвимости в движке. Поэтому следите за обновлениями и обновляйтесь, когда возможно. Благо сам WordPress оповещает о выходе новой версии. Это касается и плагинов — держите их версии актуальными. Запомните: меньше значит лучше, когда это касается любых надстроек и аддонов. Как администратор, вы должны удостовериться, что у вас установлены и активны, только те плагины, которые действительно вам нужны. Каждый плагин — это потенциальный риск и угроза безопасности, так как все они разрабатываются посторонними разработчиками.

**10. Ограничьте количество неудачных попыток авторизации.** WordPress не ведет статистику авторизаций, как удачных, так и нет. Это очень неудобно для администратора, так как у него нет возможности увидеть были ли попытки несанкционированного доступа, чтобы принять какие-либо меры, если они участятся. Предлагаем два решения [3]: плагины Login LockDown и Limit Login Attempts. После установки они не только ведут лог авторизаций, но также ограничивают количество неудавшихся попыток авторизации, блокируя на определенное время IP пытающегося.

**11. Защищаем Wordpress от XSS-инъекций.** Программисты всегда стараются защитить GET- и POST- запросы, однако, иногда этого недостаточно. Необходимо защитить блог от XSS-инъекций и попыток модификации переменных GLOBALS и _REQUEST. Этот код блокирует использование XSS-инъекций и попытки модифицировать переменные GLOBALS и _REQUEST[4]. Вставьте код в ваш файл *.htaccess*, расположенный в корне сайта. (И не забывайте бэкапить этот файл перед внесением любых изменений).

```
Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
RewriteRule ^(.*)$ index.php [F,L]
```

Код позволяет проверять все запросы. Если запрос содержит тег или попытку модифицировать значение переменных GLOBALS и _REQUEST, он блокирует его и выдаёт 403-ю ошибку.

**12. Защита директорий на сервере от просмотра.** Очень многие хостеры позволяют просматривать директории на своих серверах. Поэтому, если ввести в адресную строку www.вашблог.ru/wp-includes, то очень часто можно увидеть всё содержимое этой директории. Безусловно это небезопасно, поэтому лучше это сразу запретитьх[4].

Вы можете либо добавить пустые файлы index.html в папки, просмотр которых хотели бы запретить. Либо дополнить наш *.htaccess* ещё одной строкой: Пустой *index.html* будет выдаваться каждый раз, когда последует запрос к директории. Ну а директива в *.htaccess* просто запрещает апачу выдавать список содержимого директории.

## Выводы

Защита WordPress – вещь сложная, и описанные в этой статье способы не гарантируют на 100%, что ваш сайт будет полностью защищен от каких-либо действий мошенников. Однако, пренебрегать ими не стоит, так как они значительно уменьшат возможность взлома сайта злоумышленниками.

## Список литературы


1. *10 шагов для защиты вашего WordPress блога [Электронный ресурс] – Режим доступа: https://habrahabr.ru/post/62814/ 18.01.17.*
2. *Ещё 10 уловок для защиты Wordpress'a [Электронный ресурс] – Режим доступа: https://habrahabr.ru/post/98083/ 17.01.17.*
3. *17 способов защитить сайт на WordPress [Электронный ресурс] – Режим доступа: https://hostiq.ua/blog/17-ways-to-secure-wordpress/#17 18.01.17*
4. *[Электронный ресурс] – Режим доступа: https://ru.wordpress.org/ 18.01.17.*


*Надійшла до редколегії 3.02.2017*

**Рецензент:** д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

### МЕТОДИ І СПОСОБИ ЗАХИСТУ CMS WORDPRESS

С.С. Мєшечко, В.Я. Пєвнєв, В.А. Погорєлов

*WordPress - ідеальна платформа для публікації, орієнтована на красу, підтримку стандартів і зручність використання. На сьогодніь Wordpress як ніколи популярний. Блоги, міні-сайти, а то й цілі портали - все це будується на основі такого зручного движка-конструктора як Wordpress. Але за зручністю і легкістю освоєння криються, перш за все, питання, пов'язані з безпекою вашого сайту. Авторами проведено аналіз методів і способів захисту CMS WordPress. Описано детальні дії щодо підвищення стійкості системи до DDos-атакам таі основні помилки при адмініструванні сайту.*

***Ключові слова:*** *безпека, захист, надійність, адміністрування, паролі, підтримка.*

### THE METHODS AND WAYS TO PROTECT CMS WORDPRESS

S.S. Meshechko, V.Y. Pevnev, V.A. Pogorelov

*WordPress - an ideal platform for publishing, focused on beauty, standards support, and usability. Today, more than ever popular Wordpress. Blogs, mini-sites, and even entire portals - all this is based on such a convenient engine-designer like Wordpress. But for convenient and ease of development lie, first and foremost, issues related to the security of your site. Most prevalence - more hackers attention. The article analyzes the methods and ways of protection CMS WordPress. We describe the detailed steps to improve the sustainability of the system to DDos-attack. Painted Common Errors in site administration.*

***Keywords****: safety, protection, reliability, administration, passwords, support.*