УДК 004.056.53

М.О. Мельник, В.О. Клєвець, О.В. Столовський

Одеській національний політехнічний університет, Одеса

СТВОРЕННЯ ВДОСКОНАЛЕНОГО ПЛАГІНА ЗАХИСТУ АДМІНІСТРАТИВНОЇ ПАНЕЛІ ДЛЯ ІНТЕРНЕТ – МАГАЗИНУ НА ПЛАТФОРМІ WORD PRESS

В роботі шляхом аналізу найбільш використовуємих платформ для створення інтернет – магазинів була вибрана найпоширеніша. Аналіз найпоширенішої платформи проводився за наступними факторами, такими як популярність, розмір співтовариства користувачів і розробників, зручність адміністрування, технічна підтримка. Був проведений аналіз існуючих засобів для організації захисту інформації даних розглядаємої платформи. Проведений аналіз недоліків пропонуємих засобів. Розроблений скомпільований програмний модуль для захисту даних в інтернет - магазинах, створених на обраній платформі.

Ключові слова: *інтернет – магазин, програмний модуль, плагін, Word Press (WP), концепція безпеки в електронних магазинах, система управління вмістом (CMS).*

Вступ

Поширення з великою швидкістю інтернет – магазинів (електронних магазинів) в наш час являється невід`ємною частиною суспільства. Одною із складових електронної комерції є технічні рішення, тобто системи управління сайтом. Їх можна розділити на системи управління вмістом (CMS) і програми для просування, ведення, моніторингу та аналізу статистики [1]. Ринок технічних рішень для електронної комерції досить різноманітний, тому в роботі ми спробували сконцентруватися на основних функціональних можливостях існуючих платформ, які необхідні, на сьогоднішній день, для ефективного ведення процесів, пов'язаних з технічною стороною захисту інформації.

Проблеми безпеки електронних магазинів не втрачають своєї актуальності. З кожним роком відкривається тисячі електронних магазинів, але 85% існують менше року. [1] Така статистика пов`язана не тільки зі складним економічним становищем, а з питаннями безпеки інформації. На сьогоднішній день більшість сайтів представляють собою набір запчастин, пов'язано це з низьким рівнем стандартної розробки, відсутністю єдиної концепції безпеки, використанням декількох акаунтів для одного користувача та ін.

Необхідно звернути увагу, на те, що при зміні стандартних налаштувань JS додаткові розширення можуть не працювати. Такі проблеми можуть виникнути, якщо підключити JS скрипт у файлі шаблону, а потім використовувати плагін, якому потрібен цей же скрипт. Таким чином порушується логіка підключення і плагін не буде функціонувати. Найчастіше таке відбувається з JavaScript бібліотеками, наприклад з підключенням jQuery.

Не слід забувати, що у більшості випадків розробники плагінів не мають доступу до файлів шаблону, створеного на платформі WP. Разом з тим розробники повинні гарантувати можливість підключення необхідних скриптів. Тому для розробників одним з кращих варіантом буде використання функція wp_enqueue_script. Ця функція підключає JS файл, якщо він не був підключений раніше, тобто можна викликати її кілька разів для одного і того ж скрипта і, при цьому, скрипт буде вставлений тільки один раз.

Метою статті є аналіз рівня інформаційної безпеки сучасних CMS для електронного магазину, аналіз існуючих засобів захисту та організація захисту адміністративної панелі в електронному магазині, виявлення недоліків та запропонування розробки вдосконаленого захисту на базі існуючих.

Основна частина

Для досягнення поставленої мети необхідно вирішити наступні задачі:

1. Провести аналіз найбільш використовуємих платформ для створення інтернет-магазинів. Вибрати найпоширенішу за наступними факторами: популярність, зручність адміністрування, технічна підтримка.

2. Провести аналіз існуючих засобів для організації захисту адміністративної панелі, розглядаємої платформи для створення інтернет-магазинів. Аналіз недоліків пропонуємих засобів.

3. Розробка скомпільованого програмного модуля для захисту даних в інтернет-магазинах, створених на обраній платформі.

Аналіз найбільш використовуємих платформ для створення інтернет-магазинів показав, що Word Press є найпоширенішою. Подальші дослідження в роботі будуть пов'язані з платформою Word Press у зв'язку з її популярністю, зручністю адміністрування, великим співтовариством користувачів і розробників. Так само одним з вагомих переваг є відмінна адапта-

ція до пошукових алгоритмів, що є важливим для подальшого просування електронного магазину [2].

В ході аналізу було отримано наступне твердження:

Твердження 1. Своєчасно оновлювані версії CMS знижують ризик появи проблем із захистом інформації в середньому в два рази [4].

Аналіз існуючих скомпельованих програмних модулів (плагінів) для захисту зображень і текстового контенту показав, що до недоліків можна віднести наступне [4]: розширений функціонал пропонується у більшості плагінів тільки в платних версіях; більшість плагінів несумісні з новою версією WP.

Існує велика кількість плагінів, що обмежують кількість авторизацій, визначають IP хакера чи бота, та блокують його. Але це не єдині способи захисту адміністративної панелі. Файл .htaccess містить в собі настройки для хостинг-серверів на базі linux. Багато хто не замислюється про важливість правильної конфігурації файлу .htaccess для сайту. Але ж від цього залежить безпека вашого сайту і багато інших аспектів його роботи.

Саме тому нами було вирішено створити повністю безкоштовний плагін для правильного налаштування файла .htaccess. Було прийнято дати йому наступну назву Плагін Setting-htaccess.

Плагін можемо встановити двома способами. Для першого треба використовувати адміністративну панель магазину. У другому випадку установка відбувається за допомогою FTP клієнта: завантажуємо плагін у таку папку:

0:/www/ваш_сайт/wp-content/plugins/ (рис. 1).

Після того, як ми завантажили плагін, його необхідно активувати. Заходимо у меню «Плагіни», знаходимо встановлений плагін та активуємо його (рис. 2).

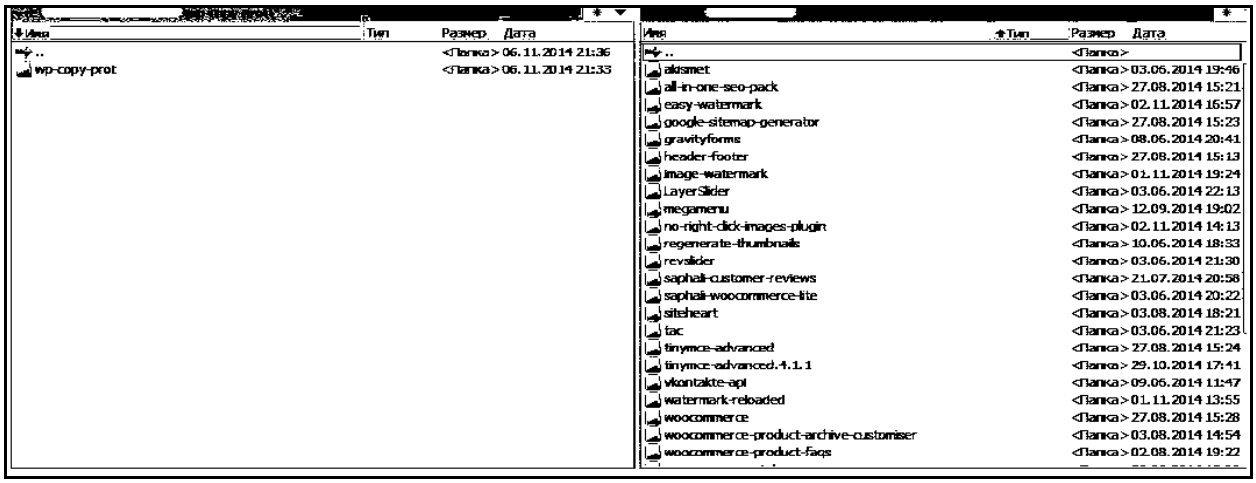

Рис. 1. Початок завантаження плагіна

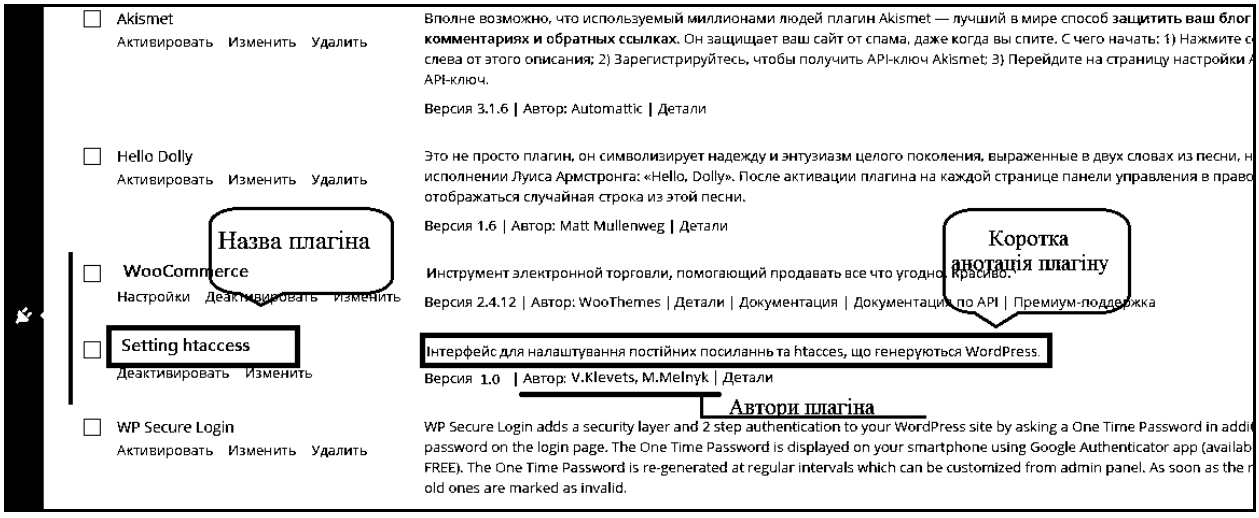

Рис. 2. Активація плагіна

Наступним кроком після активації, переходимо до його налаштувань. Для цього заходимо в меню адміністратора панелі «Налаштування» і вибираємо плагін Setting-htaccess.

Переходимо безпосередньо до налаштувань самого плагіна, що зображені на рис. 3.

Найпоширеніший вид атаки, так званий "брутфорс" – злом облікового запису шляхом перебору.

Одним з найпростіших, але досить ефективним способом захисту адміністративної консолі WP, є зміна адреси адміністративної консолі з відомого всім / wp-admin на щось більш складне і відоме лише адміністраторам. Звичайно, можна взагалі надати доступ до адміністративної консолі тільки з певних IP, але це не завжди зручно [5].

Перше налаштування у нашому списку саме змінює посилання для входу в адміністративну панель (рис. 4).

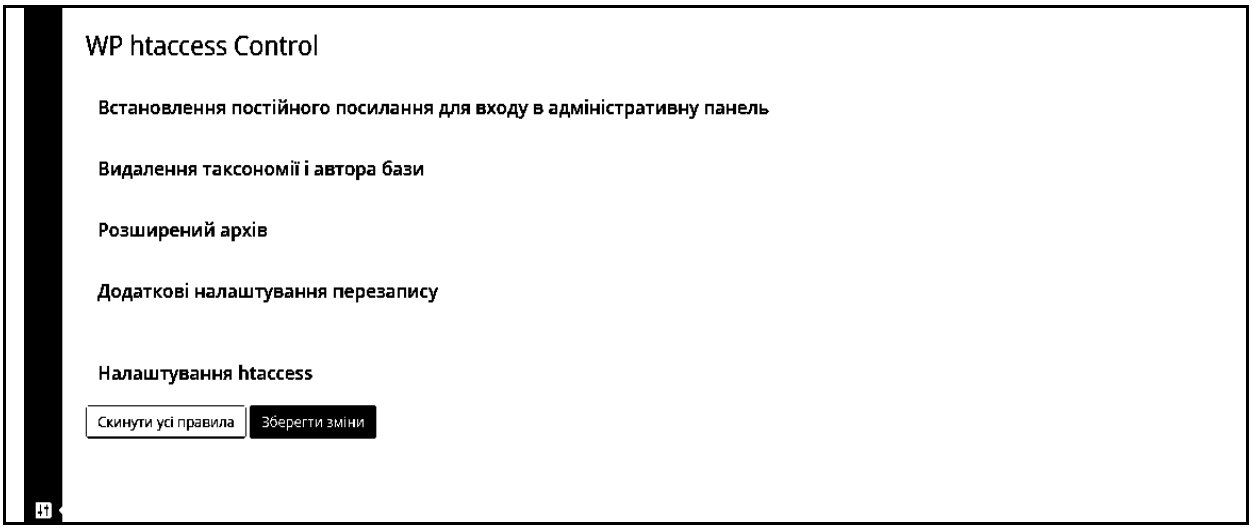

Рис. 3. Налаштування плагіна

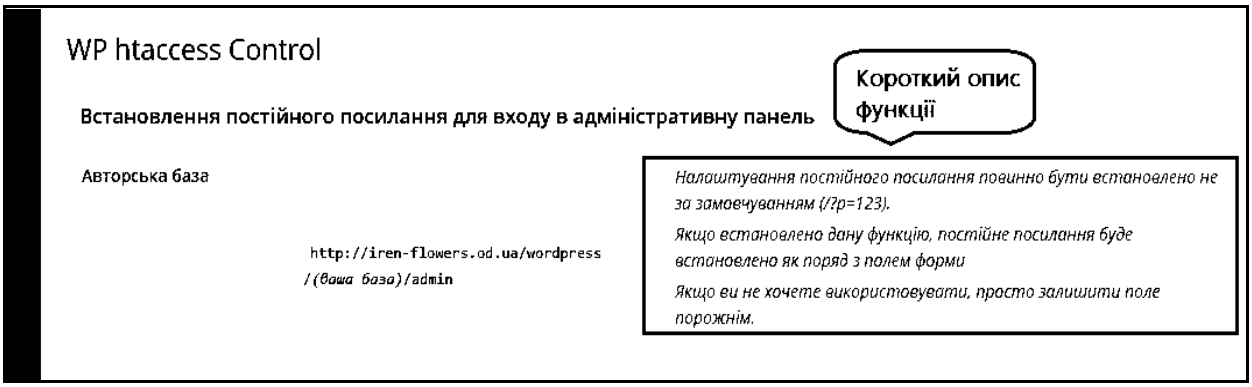

Рис. 4. Встановлення постійного посилання для входу в адміністративну панель

Перейдемо безпосередньо до налаштування файлу .htaccess. Конфігураційний файл WordPress wp-config.php містить в собі деякі налаштування сайту та інформацію для доступу до бази даних, паролі та логіни. Також там інші налаштування, що стосуються безпеки. Якщо хто-небудь отримає доступ до файлу wp-config.php, то він зможе отримати доступ до Ваших даних. Тому потрібно закрити доступ до цього файлу звідки б то не було. Це робиться за допомогою внесення відповідного коду в файл .htaccess.

У цьому випадку зовнішній доступ до файлу wp-config.php буде виключений. Тому рекомендую закривати доступ до файлу wp-config.php увімкнувши дану опцію (рис. 5).

Якщо за допомогою .htaccess можна змінювати таку кількість налаштувань, то безумовно, необхідно захищати і цей файл. Сховати цей файл можно за допомогою опції на рис. 6.

Найчастіше спам-боти звертаються безпосередньо до файлу коментарів, наприклад до wp-comments-post.php, не заходячи на сторінки записів вашого блогу. Функція на рис. 7 дозволяє заблокувати коментарі, відправлені користувачами, які прийшли «з нізвідки», дозволяючи коментувати тільки тим читачам, які перейшли на сторінку вашого блогу з яких-небудь інших сторінок (наприклад, результатів пошуку Google).

Gzip та deflate – це два модуля стискання інформації. Обидва не є модулями за замовчуванням, тому не обов'язково можуть бути присутніми у вашого провайдера. Модуль Gzip вміє працювати з масками, що безсумнівно великий плюс. Та й синтаксис у нього куди більш гнучкий ніж у попереднього. Але використовують його куди рідше аніж deflate. Також у файлі .htaccess можна вказати максимальний розмір файлів, що завантажуються. У полі на рис. 9 необхідно ввести межу розміру у МБ.

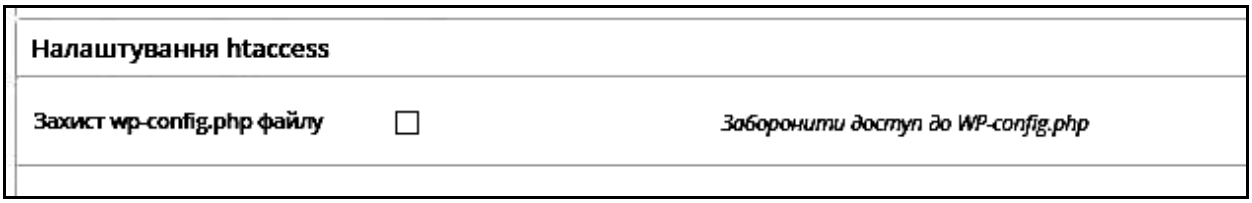

Рис. 5. Опція захисту файлу wp-config.php

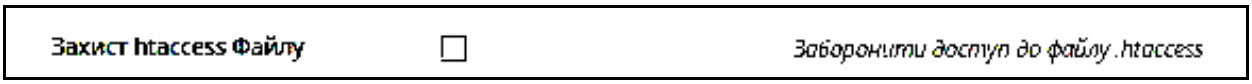

Рис. 6. Опція захисту файлу .htaccess

Рис. 7. Опція захисту comments.php

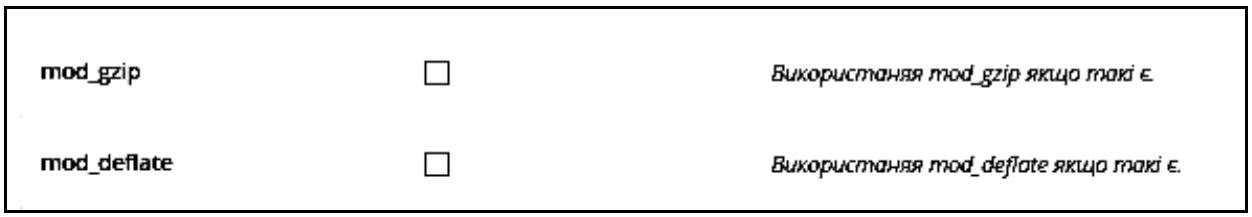

Рис. 8. Модулі стискання

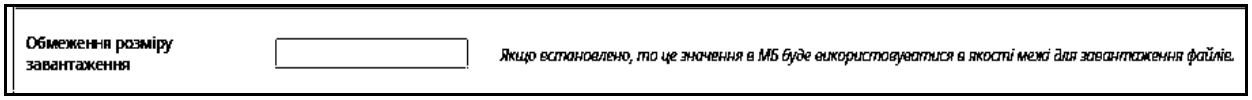

Рис. 9. Опція обмеження розміру завантаження

Хотлінк (Hotlink) – вставка прямих посилань зображень і файлів з одного сайту на інші.

Цей прийом використовується досить часто, наприклад, у вас на сервері не вистачає місця для зберігання картинок і ви користуєтеся яким-небудь безкоштовним сервісом для зберігання файлів зображень, тобто завантажуєте картинку, отримуєте URL і вставляєте його на свій сайт. У результаті: ви зберігаєте місце для вашого сайту і використовуєте пропускну спроможність хостингу для картинок. Але от як бути, якщо хтось вирішив, що ваш сайт можна використовувати як подібний сервіс.

Як не стати безкоштовним постачальником зображень і файлів?

Щоб заборонити іншим сайтам користуватися вашим трафіком і / або просто вказувати прямі посилання на ваші файли (картинки), необхідно просто заповнити поля на рис. 10.

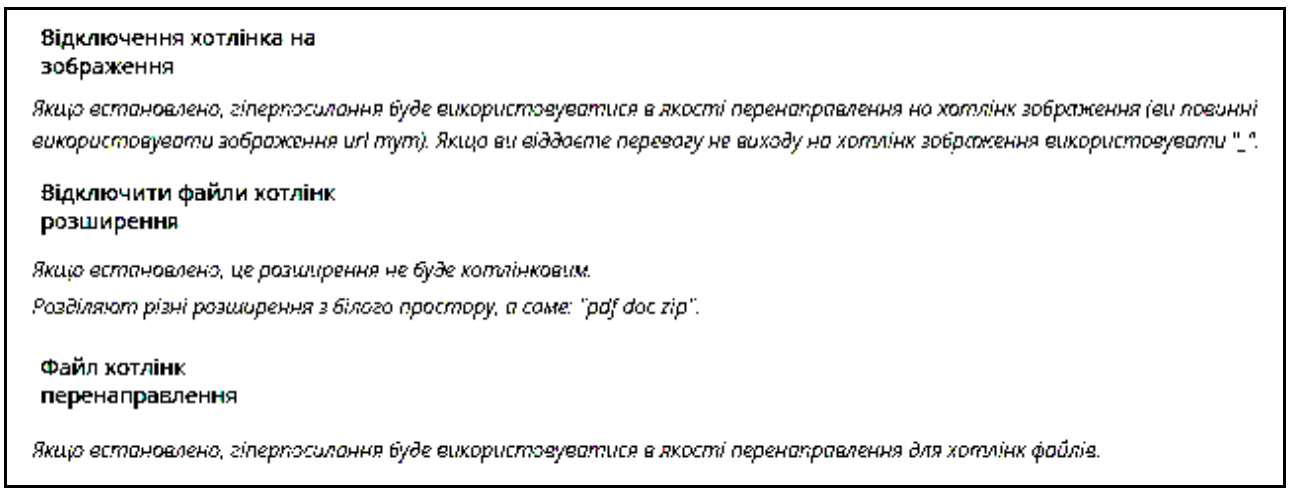

Рис. 10. Опції налаштування хотлінка

Після вірного налаштування, плагін використовує усі заявлені функціональні можливості.

Висновки

В результаті роботи було зроблено наступне:

1. Проведений аналіз найбільш використовуємих платформ для створення інтернет-магазинів. Вибрана найпоширенішу за такими факторами:

популярність,

зручність адміністрування,

технічна підтримка.

2. Проведений аналіз існуючих засобів для організації захисту адміністративної панелі, розглядаємої платформи для створення інтернет-магазинів. Зроблений аналіз недоліків пропонуємих засобів.

3. Розроблено плагін для захисту адміністративної панелі в інтернет-магазинах, створених на обраній платформі.

Перевага розробленого плагіна наступна: він включає всі функції розроблених раніше розширень, але на відміну від них плагін синхронізований до нової версії WP. Даний плагін був протестований на двох інтернет-магазинах. Робота плагіна відповідає заявленим потребам захисту інформації в інтернет-магазині. Всі заявлені функції підключені та працюють.

Передумовою для роботи плагіну має бути включений JavaScript в браузерах користувачів. Таким чином при відключеному JavaScript сайт не повинен працювати взагалі, наприклад за допомогою блоку: <noscript> <style> body{display:none;} </style> </noscript>.

Ще раз звернемо увагу, на те, що при зміні стандартних налаштувань JS додаткові розширення можуть не працювати. Найчастіше таке відбувається з JavaScript бібліотеками, наприклад з підключенням jQuery. Актуальність підключення бібліотек до оновлених версій WP являється безумовною.

Розв`язання цього питання буде обов`язково розглянуто в наступних роботах.

Список літератури

1. Орлов Л.В. Как создать электронный магазин в Интернет; 2-е изд. / Л.В. Орлов. – М: Бук пресс, 2006. – 384 с.

2. Мельник М.А. Цикл поисковой оптимизации как основа поисковой оптимизации электронных магазинов / М.А. Мельник, А.С. Ганенко // Інфокомунікації – сучасність та майбутнє: матеріали четвертої міжнародної наук.-пр. конф. м. Одеса 30-31 жовт. 2014р. – Ч. 4. – Одеса: ОНАЗ, 2014. – С. 116-117.

3. Алексунин В. Электронная Коммерция и маркетинг в Интернете / В. Алексунин, В. Родигин. – М.: Дашков и Ко, 2009. – 216 с.

4. Мельник М.А. Створення вдосконаленого плагіна захисту інформації для інтернет-магазину на платформі WordPress / М.А. Мельник, А.Р. Агадженян, Я.Г. Маховська // Інформатика та математичні методи в моделюванні. – 2015. – Т.1, №1. – С. 65-70.

5. [Електронний ресурс]. – Режим доступу до ресурсу: http:// wordpress.org.

Надійшла до редколегії 15.01.2016

Рецензент: д-р техн. наук, проф. В.В. Скачков, Військова академія, Одеса.

СОЗДАНИЕ УСОВЕРШЕНСТВОВАННОГО ПЛАГИНА ЗАЩИТЫ АДМИНИСТРАТИВНОЙ ПАНЕЛИ ДЛЯ ИНТЕРНЕТ-МАГАЗИН НА ПЛАТФОРМЕ WORD PRESS

М.А. Мельник, В.А. Клевец, О.В. Столовский

В работе путем анализа наиболее используемых платформ для создания интернет-магазинов, была выбрана одна из самих распространённых. Анализ самих распространённых проводился по следующим факторам, такими как популярность, размер сообщества пользователей и разработчиков, удобство администрирования, техническая поддержка. Был проведен анализ существующих средств для организации защиты информации данных рассматриваемой платформы. Проведен анализ недостатков предлагаемых средств. Разработан и скомпилирован программный модуль для защиты данных в интернет-магазинах, созданных на выбранной платформе.

Ключевые слова: *интернет-магазин, программный модуль, плагин, Word Press, концепция безопасности в электронных магазинах, система управления содержимым (CMS).*

AN IMPROVED PLUGIN OF PROTECTION THE ADMINISTRATIVE PANEL FOR INTERNET – SHOP BASED ON THE PLATFORM WORD PRESS

M.O. Melnyk, V.O. Klevec, O.V. Stolovskiy

Analysis the most used platform for building online - shops, was chosen as one of themselves common. The analysis itself was performed on the following common factors such as the popularity of the size of the community of users and developers, ease of administration, technical support. An analysis was made of the existing resources for the organization of information security data of the platform. The analysis of the shortcomings of the proposed funds. Developed and compiled program module for data protection in the Internet - shop created on the selected platform.

Keywords: *internet - shop software module, plug-in, Word Press, the concept of security in e-shops, content management system (CMS).*