**Практическая работа CMS Настройка безопасности**

**Ответить на вопросы:**

1. Не рекомендуется использовать стандартную учетную запись, поскольку она облегчит взлом вашей учетной записи.
2. Отправку отчетов об ошибках PHP требуется при разработке свой темы, или редактированию существующей.
3. Добавление кода: "define( 'DISALLOW\_FILE\_EDIT', true )" выключит редактирование php-файлов самого WordPress
4. Файл license.txt рекондуется удалить.
5. Если не актуальная/не используемая тема не удаляется через админ-панель, то необходимо удалить её в папке тем.

## Ответить на вопросы:

1. При установке плагина имеется уведомление: Обновление: 1 месяц назад. Не тестировался с вашей версией WordPress. Стоит ли устанавливать такой плагин?

Не стоит

2. Разрешить вносить изменения в файлы и сохраниться плагину iThemes Securite? Да

3.Функция отслеживание ошибки в iThemes Security позволяет позволяет отслеживать и обрабатывать действия пользователя

4. Режим "Нет на месте в iThemes Security не позволит никому войти в панель администратора, если вы отлучились.

5. Network Brute Force Protection – это защита от атак перебором.

**Цель:**

Настроить безопасность сайта

**Часть 1**

**Задачи:**

• Научиться добавлять безопасную учетную запись

• Научиться редактировать код

• Научиться работать с файловой системой CMS WordPress

**1. Использование нестандартных учетных данных для входа**

Не стоит использовать admin, как имя администратора.  
Стандартная учётная запись упрощаете процесс взлома админ-панели сайта WordPress. Необходимо изменить имя пользователя администратора или создать новую учетную запись администратора с другими данными. Для этого:

1) входим в админ-панель WordPress (рисунок 1);

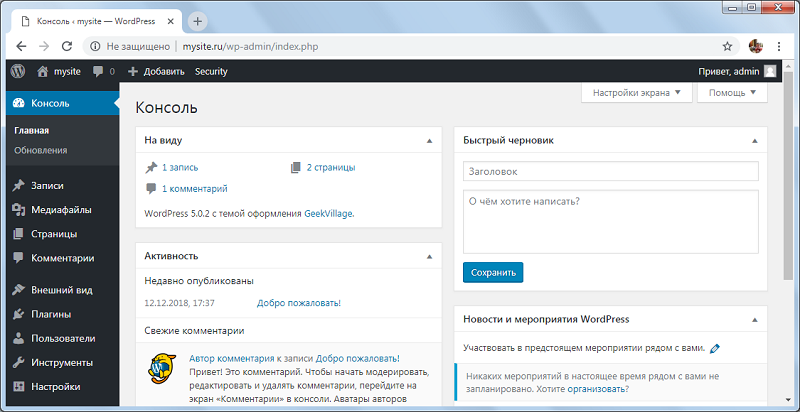


Рисунок 1 - Админ-панель WordPress

2) переходим в раздел **Пользователи** и нажмимаем кнопку **Добавить нового** (рисунок 2);

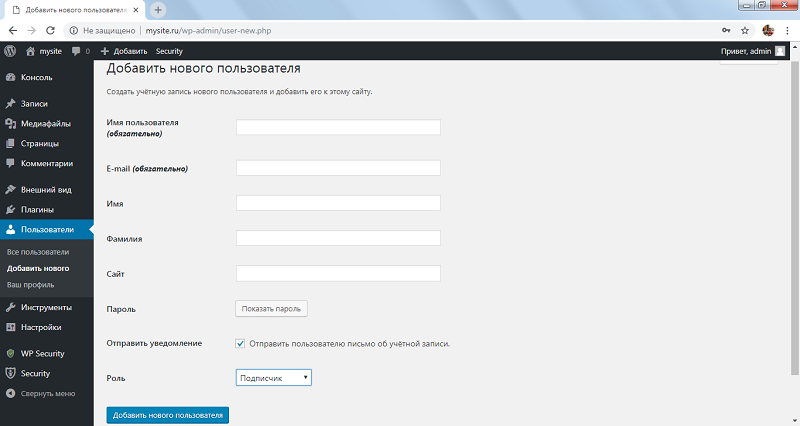


Рисунок 2 - Добавить нового пользователя

3) создаём нового пользователя и назначаем ему права **Администратора**;

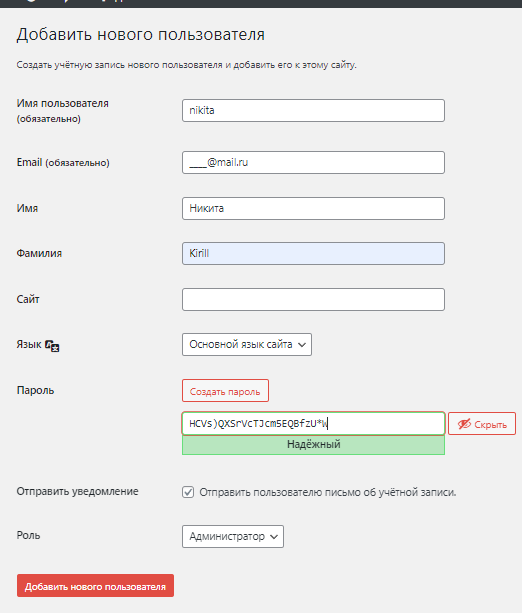


Рисунок 3 - Ввод учётных данных нового пользователя

РЕКОМЕНДАЦИЯ: если Вы указываете Имя пользователя и пароль не единтичный данному пункту, то необходимо его запомнить/записать.  
Восстановление через E-mail не возможно, так как сайт расположен на локальном сервере и соответственно не подключен к почтовому серверу.

4) Перезаходим в WordPress с новыми данными;  
5) возращаемся в раздел **Пользователи** и удаляем стандартную (старую) учетную запись администратора **locadm** (рисунок 3).

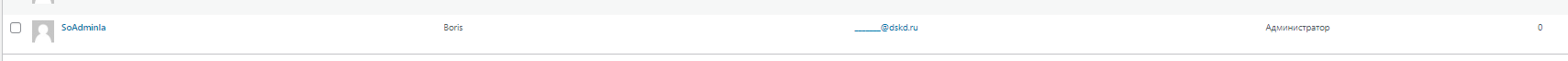


Рисунок 4 - Удаление учётной записи admin

**2. Отключение отправки отчетов об ошибках PHP**

Отчеты об ошибках PHP могут быть довольно полезны, если вы занимаетесь разработкой сайта и хотите удостоверится, что все работает правильно. Однако показывать ошибки всем, это серьезное упущение в безопасности WordPress.

Необходимо это исправить. Для этого редактируем код в файл **wp-config.php.** Данный файл в нашем случаи расположен на локальном хосте **mysite.ru\www** (рисунок 5).

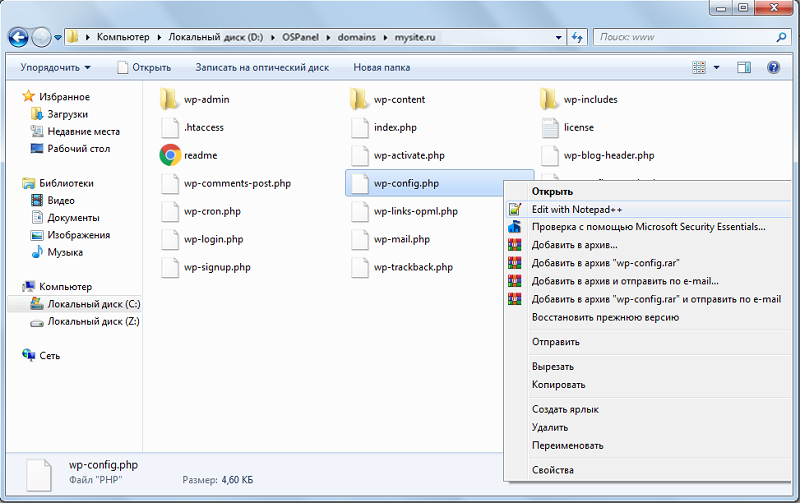


Рисунок 5 - Wp-config.php

Находим строчку:

****

Удаляем её и пишем две новые строчки:

****

В результате должен получиться код, изображенный на рисунке 6. После чего сохраняем изменения.

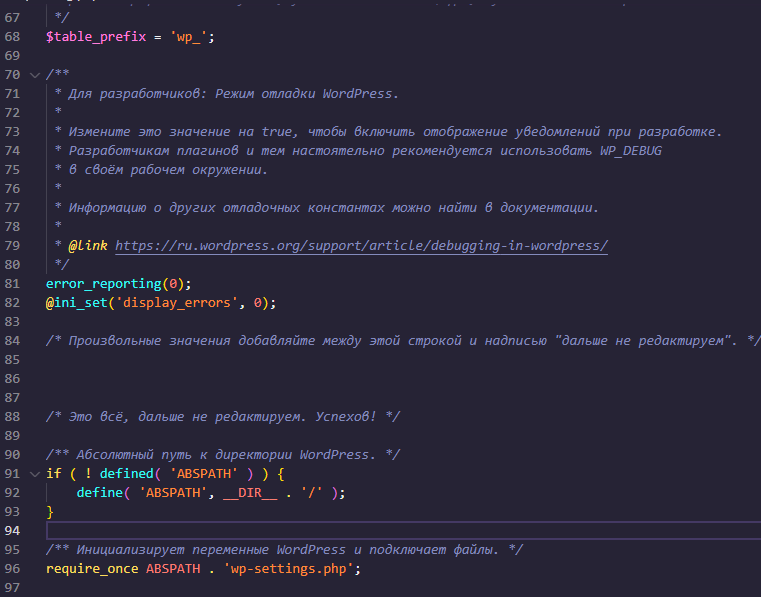


Рисунок 6 - Отключение отправки отчетов об ошибках PHP

**3. Выключение редактирования файлов**

WordPress имеет встроенный редактор, который позволяет редактировать PHP файлы. Эта функция настолько же полезна, насколько она может нанести вред. Если хакеры получат доступ к админ-панели, первая вещь, на которую они обратят внимание, это Редактор Файлов. Некоторые пользователи WordPress предпочитают полностью выключить эту функцию. Она может быть выключена редактированием вновь файла **wp-config.php**, путем добавления туда следующего кода:

****В результате должен получиться код, изображенный на рисунке 7. После чего сохраняем изменения.

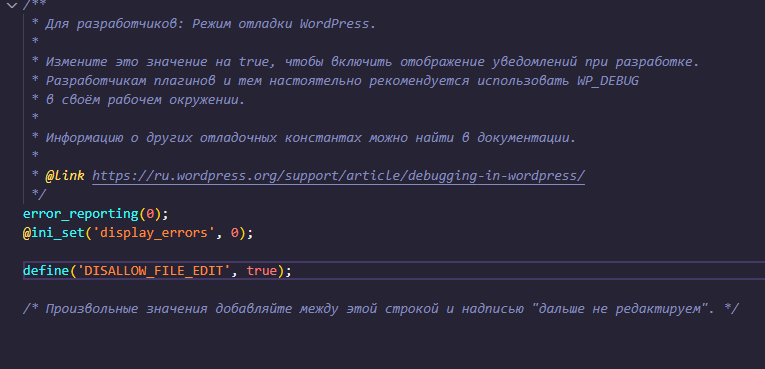


Рисунок 7 - Выключение редактирования файлов

**Удаление readme.html и license.txt**

Файлы **readme.html** и**license.txt** присутствуют в корневой папке любой установки WordPress. Эти файлы не имеют важности для сайта, а хакерам они могут облечить их злодеяния. Например, чтобы выяснить текущую версию вашего WordPress и много чего другого полезного для взлома веб-сайта.

Переходим в каталог с файлами и удаляем файлы (рисунок 8)

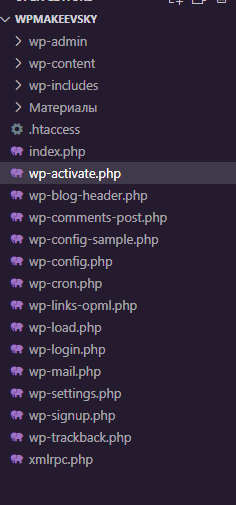


Рисунок 8 - Удаление readme.html и license.txt

**5. Удаление неиспользуемых шаблонов и плагинов**

Сделайте уборку вашего сайта на WordPress и удалите все неиспользуемые шаблоны и плагины. Хакеры часто используют отключенные и устаревшие шаблоны и плагины (даже официальные плагины WordPress) для получения доступа к вашей панели управления, или загрузки вредоносного содержимого на ваш сервер. Удаляя плагины и шаблоны, которые вы перестали использовать (и возможно забыли обновить) давным давно, вы снижаете риски и делаете ваш сайт на WordPress более безопасным.

Переходим в админ-панель и открываем раздел **Внешний вид –Темы** (Рисунок 9)

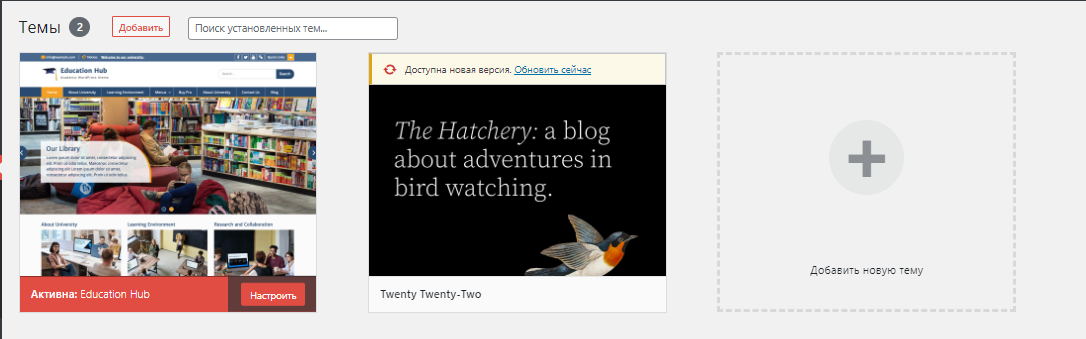


Рисунок 9 - Установленные темы

Наведите курсор мыши на блок с темой, которую требуется удалить. В нашем случаи это все темы, кроме активной (текущей) **GeekVillage.**

При наведении появится кнопка **Информация о теме**, при нажатии на которую открывается тема и доступны дополнительные функции (Рисунок 10)

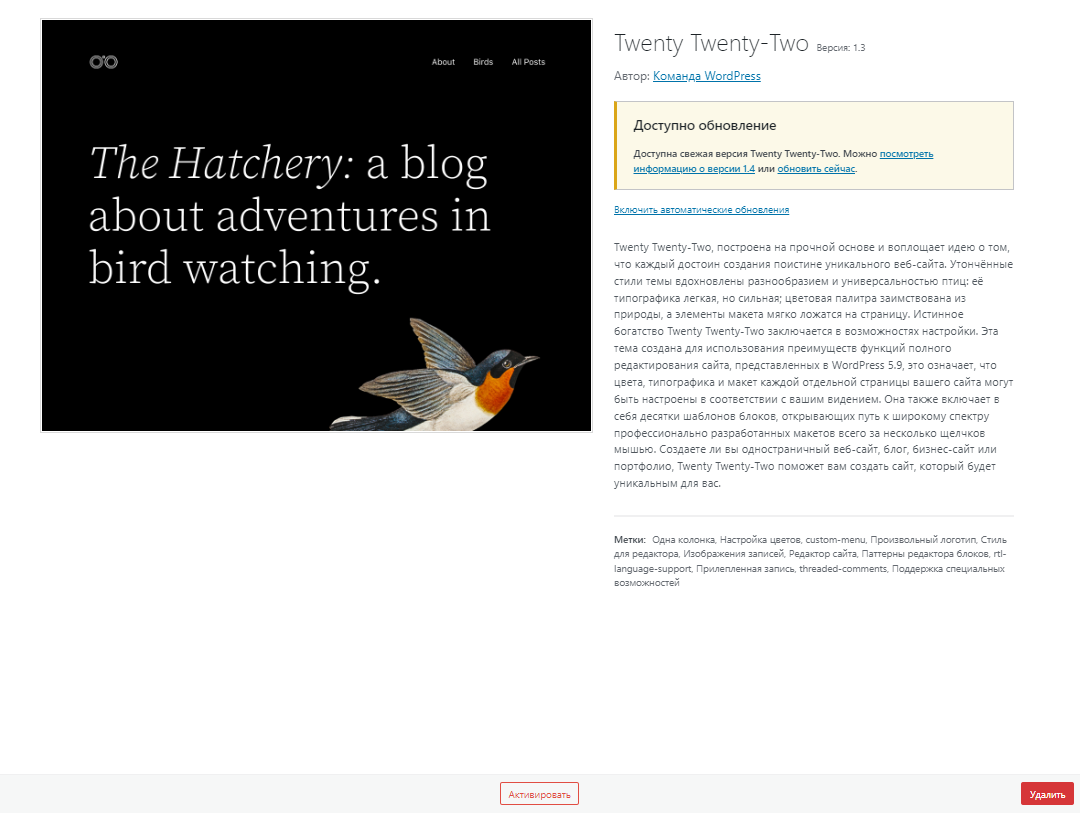


Рисунок 10 - Удаление темы

В появившемся окне помимо кнопок **Активировать** и **Просмотреть** присутствует кнопка **Удалить**. При нажатии появляется запрос на подтверждение действия. Соглашаемся с удалением – выбранный шаблон больше не появится в окне админки с общим перечнем установленных тем, а ее папка удалится на сервере.

Иногда возникают ситуации, когда тему не удается удалить через админку. Возможно, файлы были повреждены при неудачном обновлении либо по другой причине. В этом случае удаление можно осуществить с помощью файлового менеджера. Этот способ также удобно использовать, если вам нужно удалить не одну-две, а большое количество тем.

Для этого:

1) переходим на сервер, где хранится сайт, в нашем случаи это каталог: **mysite.ru**  
2) В каталоге вашего сайта зайдите в папку wp-content и найдите в ней подпапку **themes** (рисунок 11)

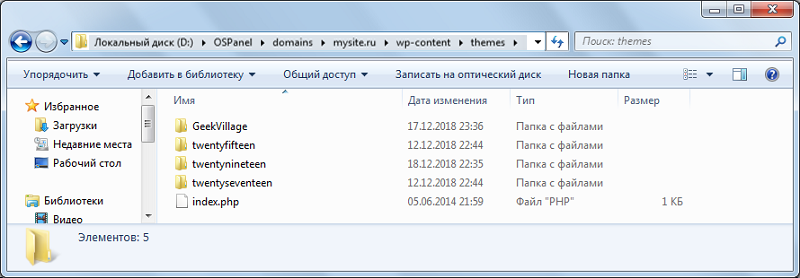


Рисунок 11 - Удаление темы по FTP

3) Внутри папки themes хранятся каталоги со всеми установленными темами. Выберите ненужные темы и удалите папки с их названиями.

## Часть 2.

## Задачи:

• Научиться устанавливать плагин

• Изучить плагин

• Настроить плагин

## Установка плагина

1. Войдите в админ панель WordPress и откройте вкладку **Плагины — Добавить новый** (рис. 1)

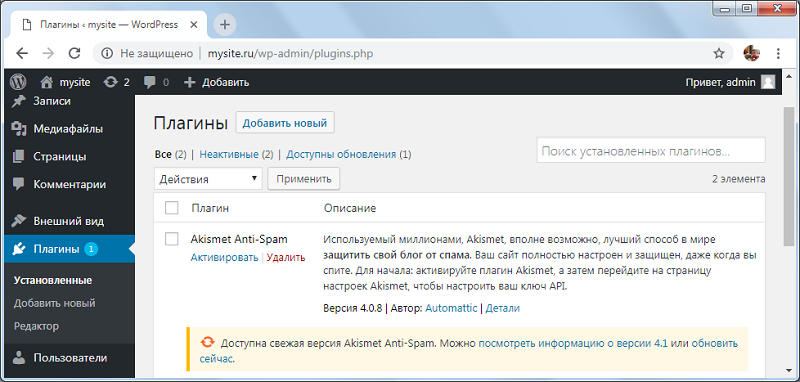


Рисунок 1 - Добавить новый плагин

## Активация плагина

2. Ищем плагин**iThemes Security** через поиск, после чего нажимаем **Установить**. (Рисунок 2)

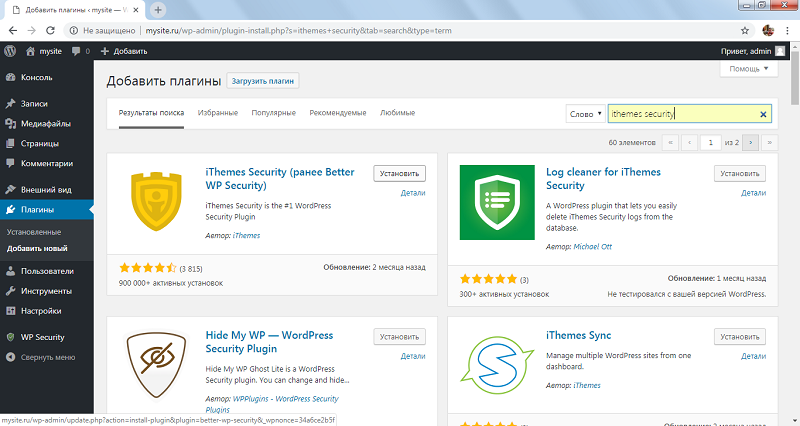


Рисунок 2 - Установка плагина

После установки плагина **iThemes Security,** нажимаем на новую кнопку **Активировать**.(Рисунок 3)

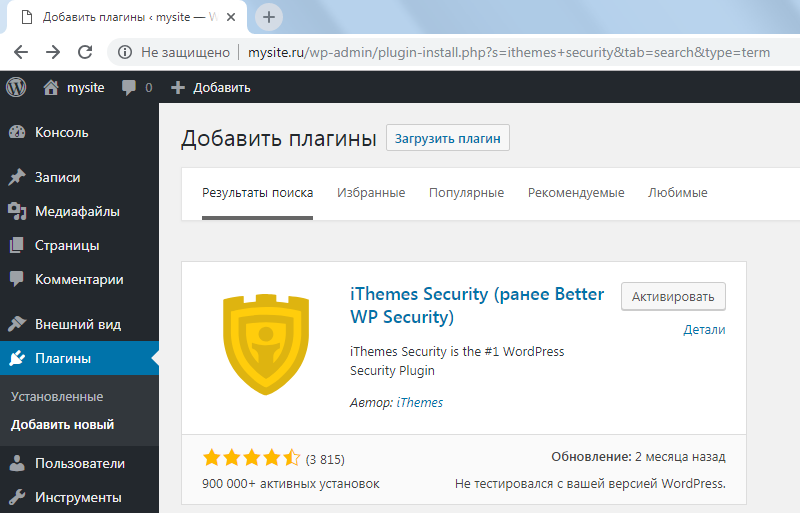


Рисунок 3 - Активировать плагин

## Настройка "Security Check"

Первая вкладка настройки **Security Check** (проверка безопасности) нажимаем**Configure Settings** (Рисунок 4)

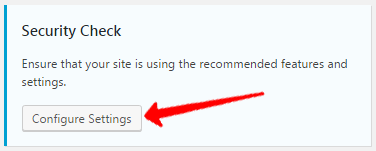
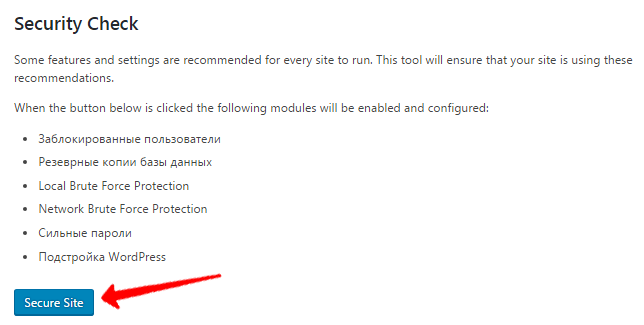


Рисунок 4 - Настройки "Security Check"

Дальше откроется окно настроек. Нажимаем **Secure Site,** плагин установит рекомендуемые настройки безопасности (рисунок 5)

  
Рисунок 5 - Рекомендуемые настройки безопасности

## Настройка "Configure Settings"

Следующая вкладка настройки **Основные настройки**, нажимаем **Configure Settings** (рисунок 6)

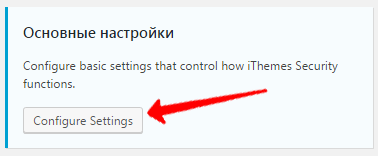
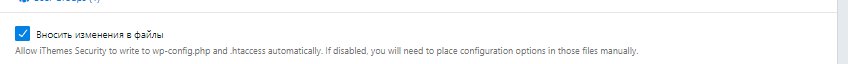


Рисунок 6 - Основные настройки

Здесь обязательно нужно поставить галочку напротив надписи **Вносить изменения в файлы** и сохраниться. Чтобы плагин эффективно функционировал, ему нужен доступ к файлам **wp-config.php** и **.htaccess**. Ставя галочку, предоставляется плагину этот доступ (рисунок 7)



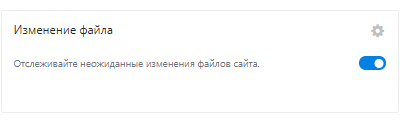
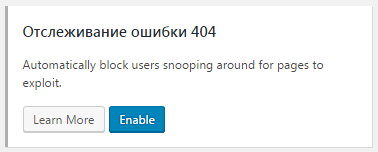


Рисунок 7 - Предоставление доступа

Остальные настройки в этой вкладке оставляем по умолчанию.

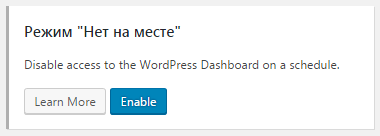
## Опция "Отслеживание ошибки"

Следующая опция это **Отслеживание ошибки.** Что это такое? Представьте ситуацию, когда пользователь на вашем сайте запрашивает большое количество несуществующих страниц. Если это одна или две страницы, тогда нет ничего страшного, но если эта периодичность повторяется, это говорит о том, что злоумышленник пытается найти уязвимости сайта для его взлома, ведь простой посетитель ищет информацию на реальных страницах. Если **iThemes Security** замечает активность подобного рода, пользователь блокируется. Чтобы включить эту опцию, нажимаем **Enable**. (Рисунок 8)

  
Рисунок 8 - Режим "Отслеживание ошибки"

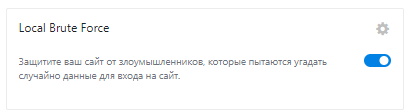
## Режим "Нет на месте"

Следующая настройка это **Режим "Нет на месте".** Если вы отлучаетесь на определенный период, и у вас не будет возможности заходить в административную панель WordPress, можете включить эту опцию, указав в настройках промежуток времени, который вы будете отсутствовать. В это время ни вы, ни кто-то другой не сможет зайти в панель администратора. (Рисунок 9)

  
Рисунок 9 - Режим "Нет на месте"

## Network Brute Force Protection

**Network Brute Force Protection (Сетевая защита от атак перебора)**. Включаем обязательно. Эта опция автоматически запрещает доступ к сайту пользователям, которые совершали попытки взломать вход на другие сайты

  
Рисунок 10 - Режим "Network Brute Force Protection"

iThemes Security настроен. Благодаря гибким настройкам и широкому функционалу ваш сайт максимально защищен от взлома и атак.