**Урок 3. All In One WP Security – плагин безопасности для WordPress**

**Цель:**

Установить и настроить плагин

**Задачи:**

• Научиться устанавливать плагин  
• Изучить плагин  
• Настроить плагин

**Установка плагина**

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

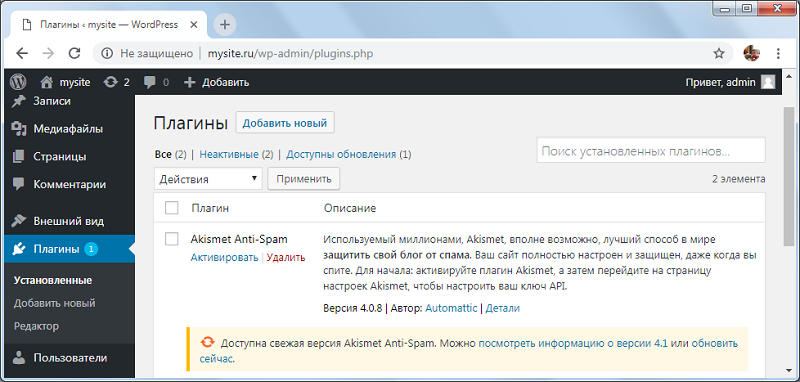


Рисунок 1 - Добавить новый плагин

**Активация плагина**

2. Ищем плагин **All In One WP Security** через поиск, после чего нажимаем **Установить** (рисунок 2).

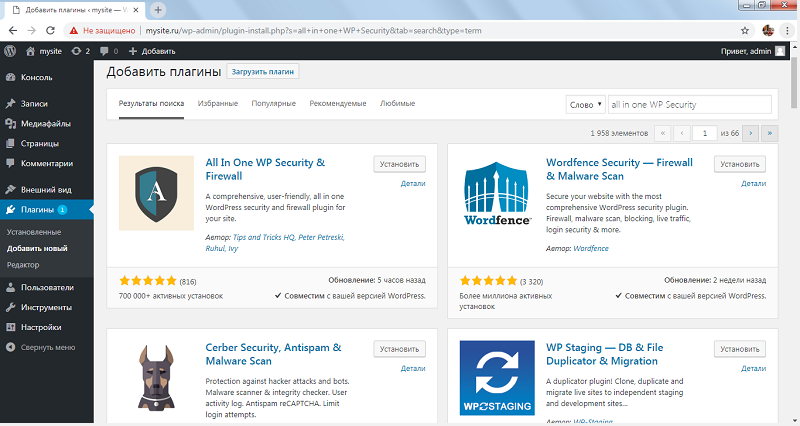


Рисунок 2 - Установка плагина

3. После установки будет информация, изображенная на рисунке 3. Нажимаем**Активировать плагин**

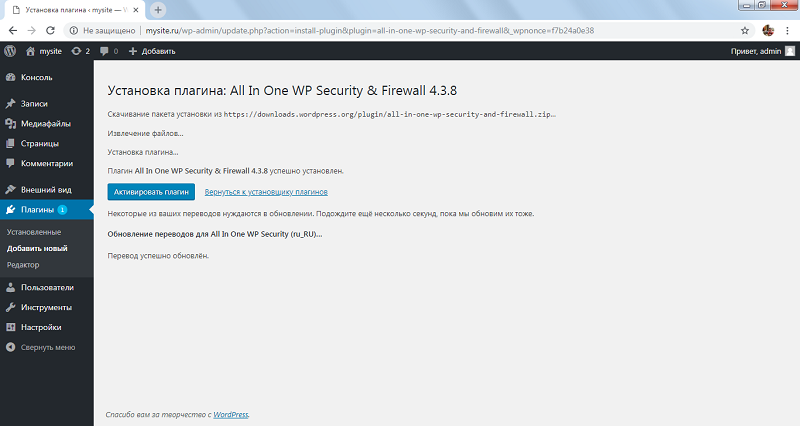


Рисунок 3 - Активация плагина

4. После активации плагина **All In One WP Security**, нам доступна его настройка через панель администратора (рисунок 4).

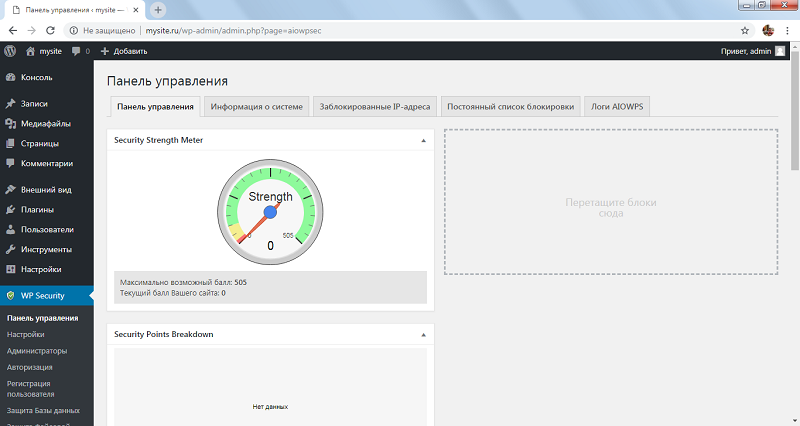


Рисунок 4 - Установка плагина

Также из рисунка 4 мы видим блок **Security Strength Meter** показывающий текущий балл безопасности сайта. На данном этапе балл равен 0, корректируя настройки безопасности в данном плагине, балл будет повышаться.

**Резервное копирование**

Обязательно делаем бэкап (резервную копию) перед началом работы (на всякий случай) следующих файлов:  
база данных;  
файл wp-config;  
файл htaccess.  
Резервные копии этих трех файлов будем делать прямо в данном же плагине, для этого в **WP Security**, открываем - **Настройки** (рисунок 5).

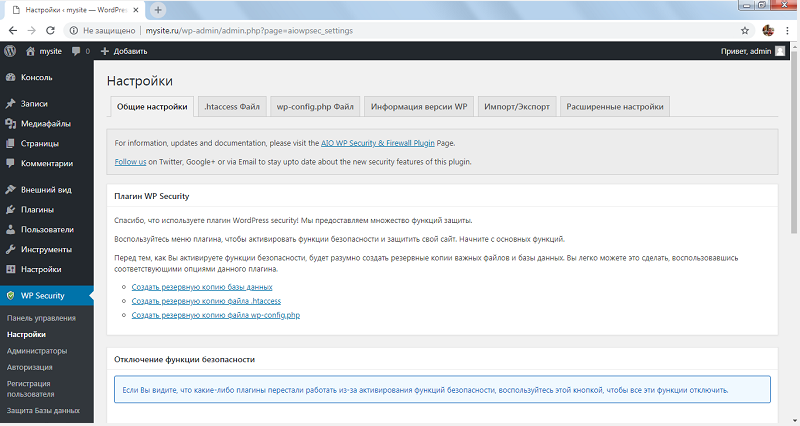


Рисунок 5 - Резервная копия

Переходим в создание резервной копии **Создать резервную копию базы данных**, открывается новое меню настроек (рисунок 6).  
В разделе **Создание резервной копии базы данных вручную** нажимаем **Создать бэкап базы данных сейчас.** Далее в разделе **Автоматическое создание резервных копий** устанавливаем флажок **Включить автоматическое создание бэкапов** и нажимаем **Сохранить настройки.**

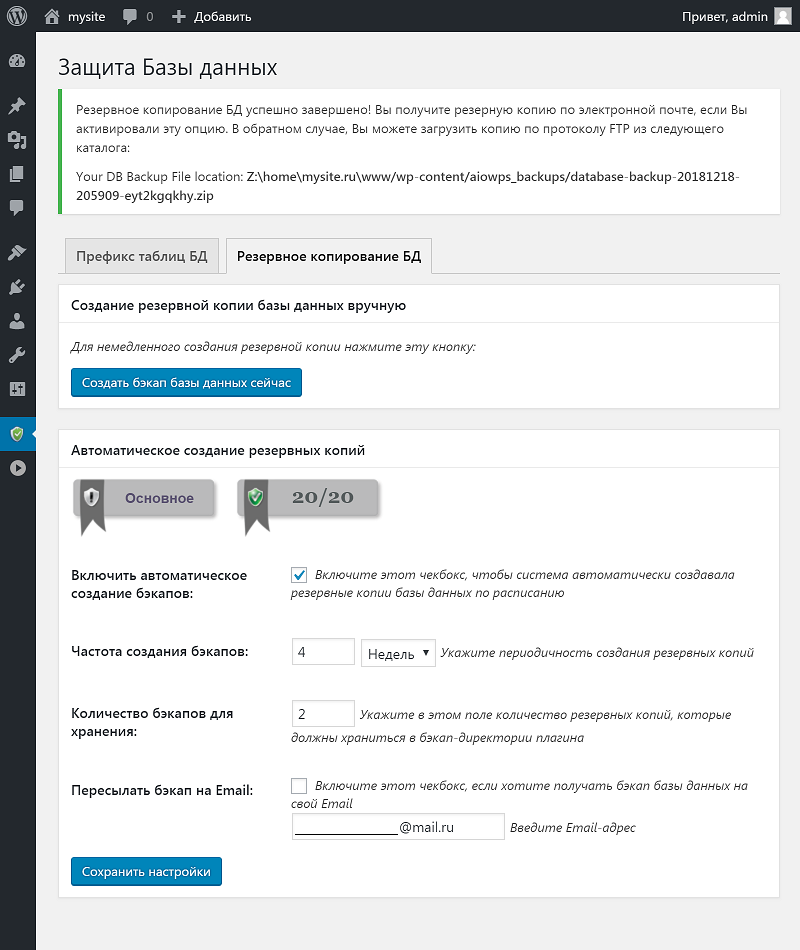


Рисунок 6 - Резервная копия "Создать резервную копию базы данных"

Аналогично делаем резервную копию файла **.htaccess** (рисунок 7). При успешном создании копии будет информация: **Резервная копия файла .htaccess успешно создана!**  
Также на данной странице нам доступна информация о файле **htaccess**.

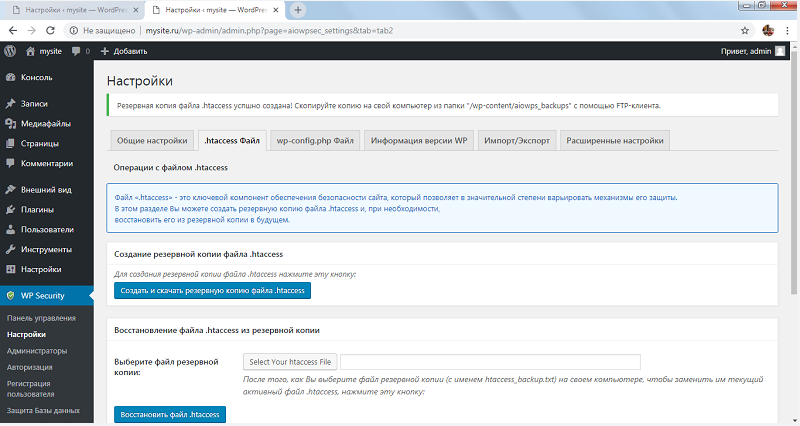


Рисунок 7 - Резервная копия файла .htaccess

Далее делаем третью резервную копию, в этот раз файла **wp-config.php** (рисунок 8). При успешном создании копии будет скачан файл.  
Аналогично **.htaccess**, на странице доступна информация о файле**wp-config.php.**

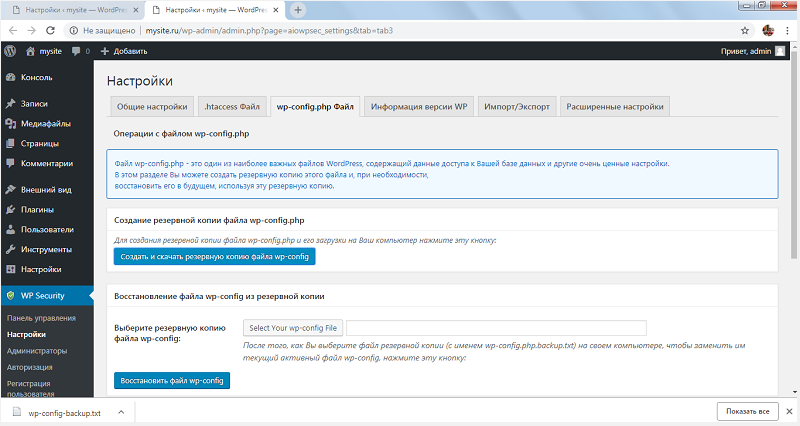


Рисунок 8 - Резервная копия файла wp-config.php

После простых маннипуляций балл безопасности, возрос на 20 баллов (рисунок 9).

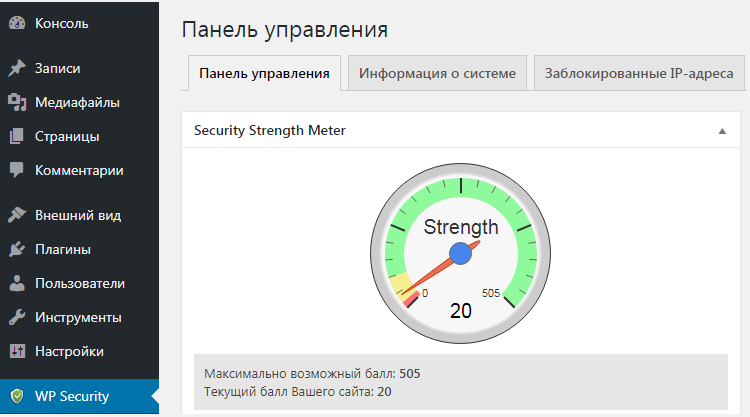


Рисунок 9 - Баллы безопасности

Этот показатель поможет контролировать и понимать, что еще нужно сделать для улучшения безопасности. Не рекомендуется делать все, ради достижения максимальных баллов. Могут быть плохие последствия, сайт может упасть или ошибочно функционировать.

**Раздел "Администраторы"**

При установке WordPress автоматически присваивает администратору имя пользователя **admin** (если Вы вручную не измените его).  
Многие хакеры пытаются воспользоваться этой информацией, применяя для нападения «Брутфорс-атаку», когда они систематично подбирают пароль, используя слово «admin» в качестве имени пользователя.  
По соображениям безопасности, одна из первых и наиболее разумных вещей, которую Вы должны сделать на своем сайте, это изменить имя пользователя **admin**, установленное по умолчанию.  
Раздел **Администраторы** предназначен для изменения имени пользователя **admin** на более безопасное, по Вашему выбору (рисунок 10).

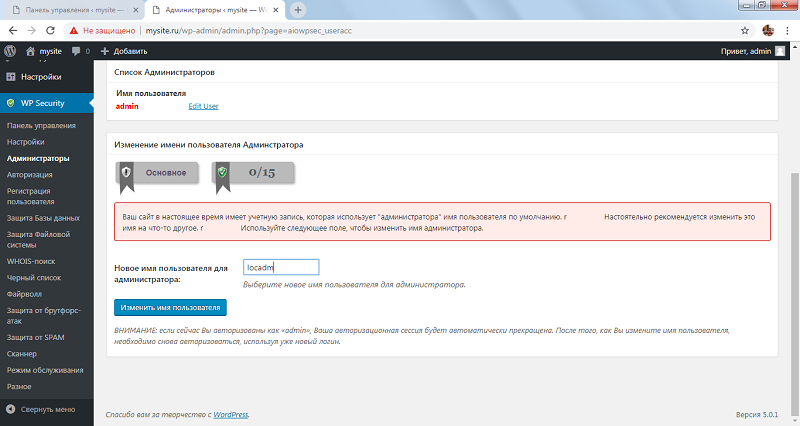


Рисунок 10 - Раздел "Администраторы"

Меняем имя на **locadm** и нажимаем **Изменить имя пользователя.**  
Мы попадаем в меню авторизации, где нам сообщают, что: **Ваша авторизационная сессия была прекращена, так как Вы только что изменили имя пользователя admin. Для продолжения авторизуйтесь снова.**  
Вводим новые учётные данные (рисунок 11).

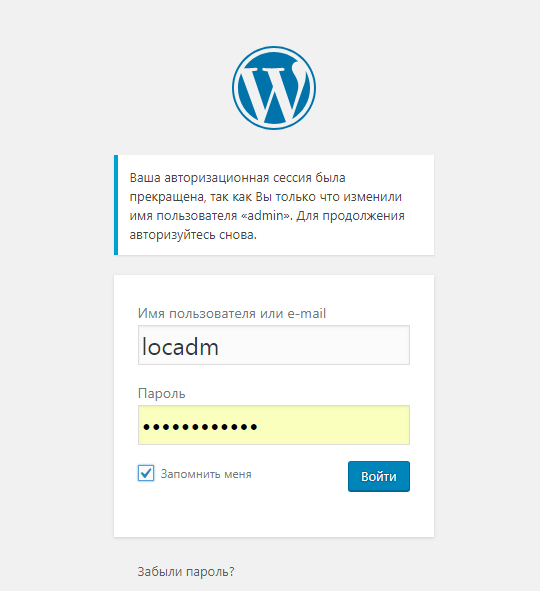


Рисунок 11 - Меню авторизации

Далее нам сообщают что в разделе **Администраторы**, действий не требуется, рейтинг данного меню 15/15 (рисунок 12).

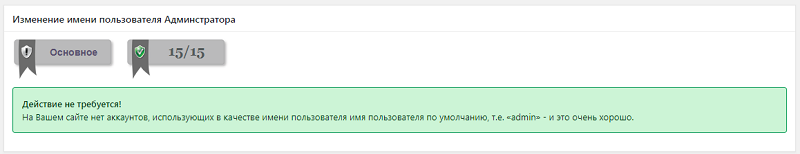


Рисунок 12 - Меню "Администраторы"

**Пароль**

В меню **Администраторы** имеются вкладки, переходим на вкладку **Пароль**.

Плохой пароль - это наиболее распространенная уязвимость на большинстве сайтов, и, как правило, первое, что будет делать хакер, чтобы проникнуть на сайт - попытается подобрать пароль.  
Многие люди сами себе ставят ловушку, используя в качестве пароля простое слово или ряд цифр. На подбор такого предсказуемого пароля у опытного хакера уйдет всего несколько минут, так как для этого используются специальные программы с большими базами наиболее распространенных сочетаний букв, слов и цифр.  
Чем длиннее и сложнее пароль, тем тяжелее будет хакеру его подобрать, потому что это требует гораздо больше вычислительных мощностей и времени.  
Здесь Вы можете проверить свой пароль на надежность. Мы вводим пароль: **Tcctynerb17**, нажимаем **Enter** (рисунок 13).

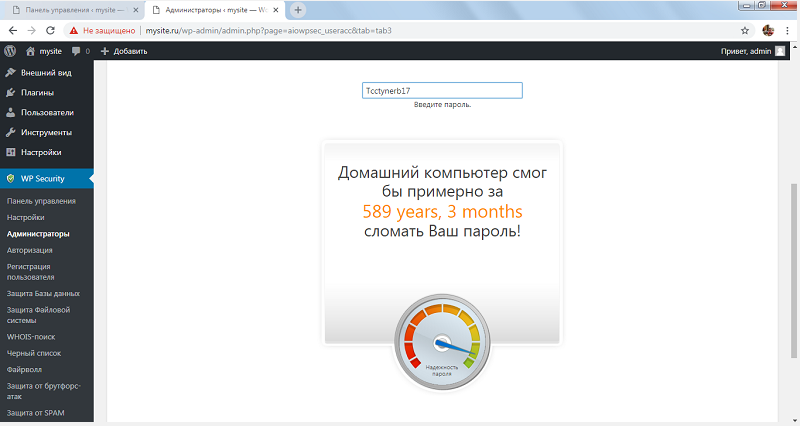


Рисунок 13 - Изменение пароля

После ввода нового пароля, уровень безопасности увеличился. Также нам сообщают, что данный пароль домашний компьютер смог бы примерно за 589 лет и 3 месяца сломать Наш пароль!

Записываем этот пароль и переходим в админ-панели в раздел **Пользователи**, что бы применить его для учётной записи **locadm** (рисунок 14).

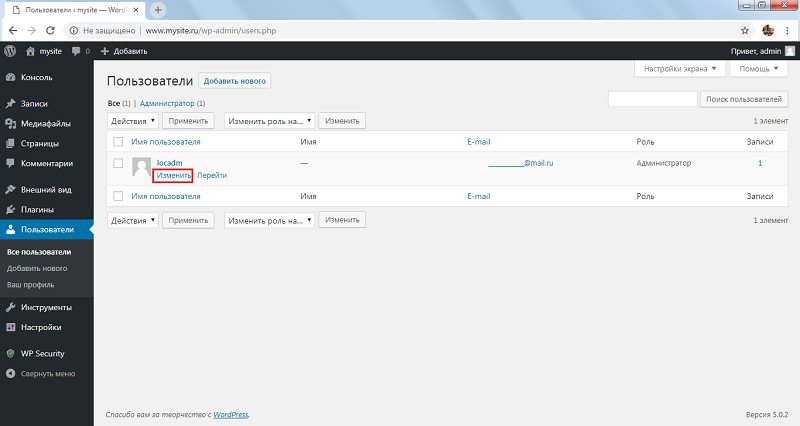


Рисунок 14 - Пользователи

Нажимаем **Изменить**, откроется новое окно, в котором вводим новый пароль: **Tcctynerb17**. После нажимаем **Обновить профиль** (рисунок 15).

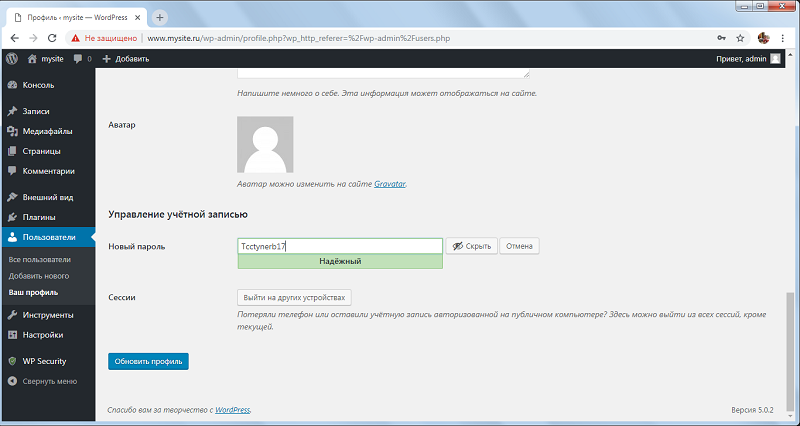


Рисунок 15 - Смена пароля

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

**Защита базы данных**

Ваша база данных - это наиболее ценная часть Вашего сайта, так как в ней находится весь контент и настройки.  
База данных также является мишенью для хакеров, пытающихся получить контроль над определенными таблицами методом SQL-инъекций и внедрением вредоносного кода. Одним из способов усилить защиту от таких атак является изменение префикса таблиц базы данных с устанавливаемого по умолчанию **wp\_** на какой-нибудь другой, который было бы тяжело угадать.  
Эти опции позволяют легко изменить префикс БД на любое введенное Вами значение или на сгенерированное плагином.  
При переходе в раздел **Защита базы данных** (рисунок 16) нам предлагают перед изменением префикса создать DB Backup базы данных. Данный пункт мы выполняли не так давно, но во вкладке "Префикс таблиц БД" следует быть аккуратным и прежде чем поставить галочку, обязательно повторяем создание резервную копию своей базы данных (там же увидите ссылку на создание бэкапа своей БД).

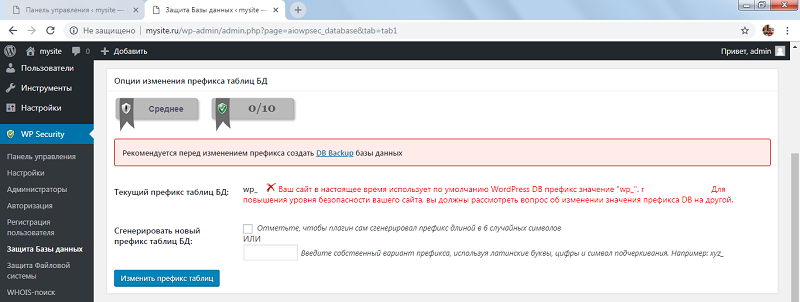


Рисунок 16 - Раздел "Защита базы данных"

После создания резервной копии, прописываем новый префикс таблиц БД: **wordpr** и нажимаем **Изменить префикс таблицы** (рисунок 17).

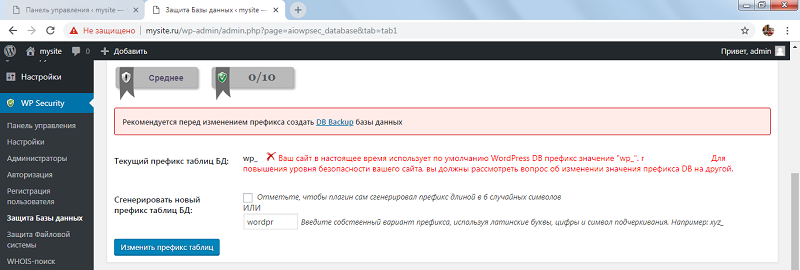


Рисунок 17 - Изменение префикса таблицы

В результате изменения префикса таблицы, будут выполнены процессы, результат которых отобразится в этом же окне, снизу (рисунок 18).

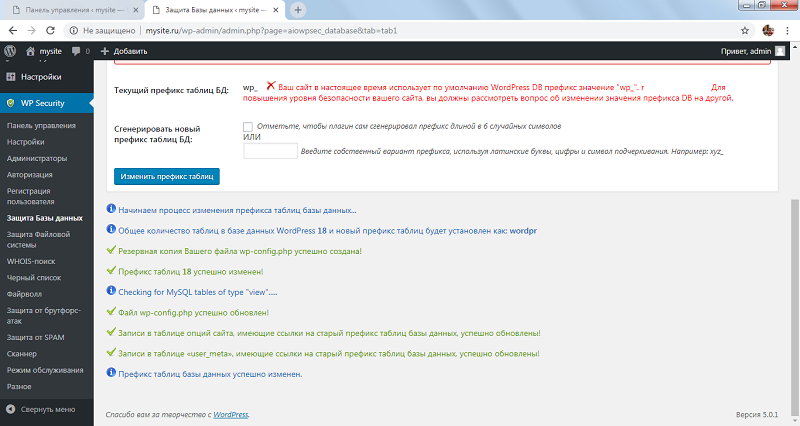


Рисунок 18 - Результат изменения префикса таблицы

**Защита файловой системы**

1. Редактирование файлов PHP

По умолчанию из панели администрирования WordPress позволяется редактировать PHP-файлы плагинов и тем.  
Данный функционал позволяет хакеру в случаи взлома выполнить любой код на Вашем сервере из панели администратора.

В плагине **WP Security** имеется возможность отключить редактирование файлов из панели администратора, для этого выполняем следующие действия:  
1) открываем раздел **Защита Файловой системы;**  
2) переходим во вкладку **Редактирование файлов PHP;**  
3) устанавливаем галочку **Отметьте этот чекбокс, чтобы запретить редактирование PHP-файлов из админ-панели WordPress;**  
4) нажимаем **Сохранить настройки.**  
Выполнение выше указынных действий указано на рисунке 19.

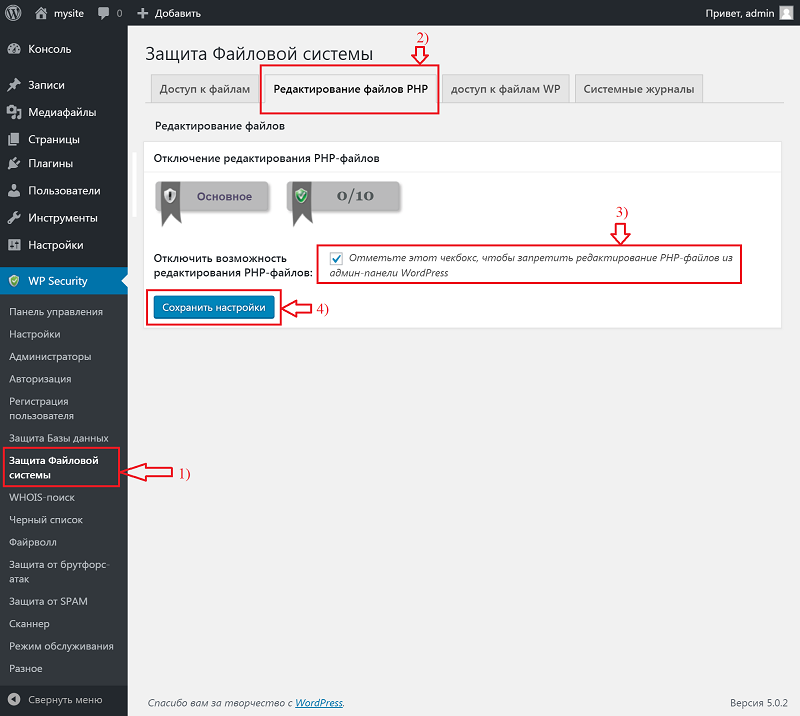


Рисунок 19 - Отключение редактирования PHP-файлов

2. Установка запрета доступа к файлам WordPress

Данная опция запретит доступ к таким файлам как **readme.html**, **license.txt** и **wp-config-sample.php**, которые создаются во время установки WordPress и не несут в себе системной нагрузки, но ограничение доступа к этим файлам позволит Вам скрыть от хакеров важную информацию (такую как версия WordPress).

Для этого в плагине **WP Security** выполняем следующие действия:  
1) открываем раздел **Защита Файловой системы;**  
2) переходим во вкладку **Доступ к файлам WP;**  
3) устанавливаем галочку **Отметьте этот чекбокс, чтобы запретить доступ к файлам readme.html, license.txt и wp-config-sample.php.;**  
4) нажимаем **Сохранить настройки.**  
Выполнение выше указынных действий указано на рисунке 20.

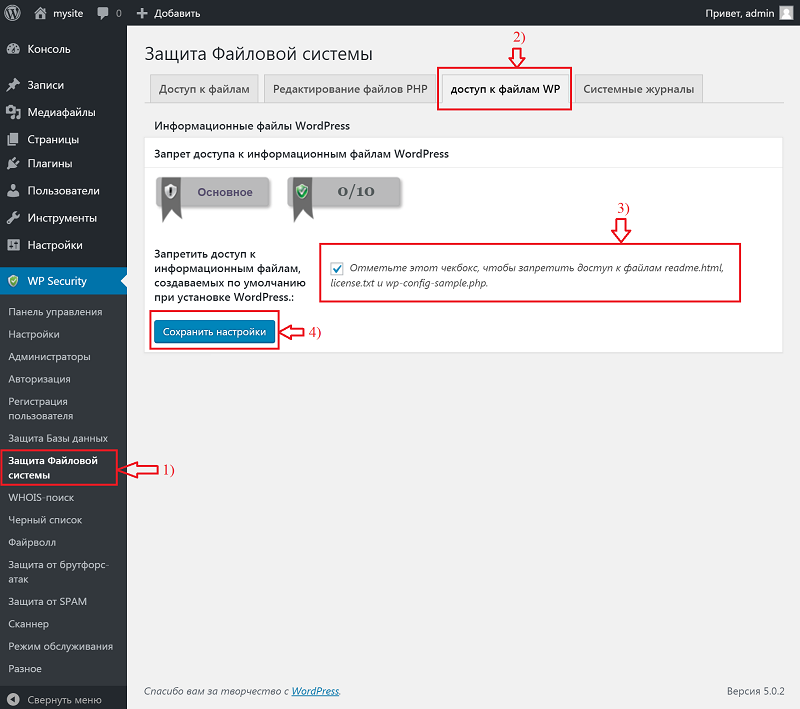


Рисунок 20 - Запрет доступа к файлам

**Файрволл**

Опции в этой вкладке позволяют применить некоторые базовые правила защиты для Вашего сайта.  
Данная функциональность брандмауэра достигается методом добавления в Ваш файл **.htaccess** некоторых специальных директив.  
Активация этих опций не должна иметь никакого влияния на общую функциональность сайта  
1) Настраиваем **Базовые параметры файрвола** WordPress

**Активировать основные функции брандмауэра**: ставим галочку  
**Запретить доступ к файлу debug.log:** ставим галочку  
Функционал установленных параметров также расписан на рисунке 21

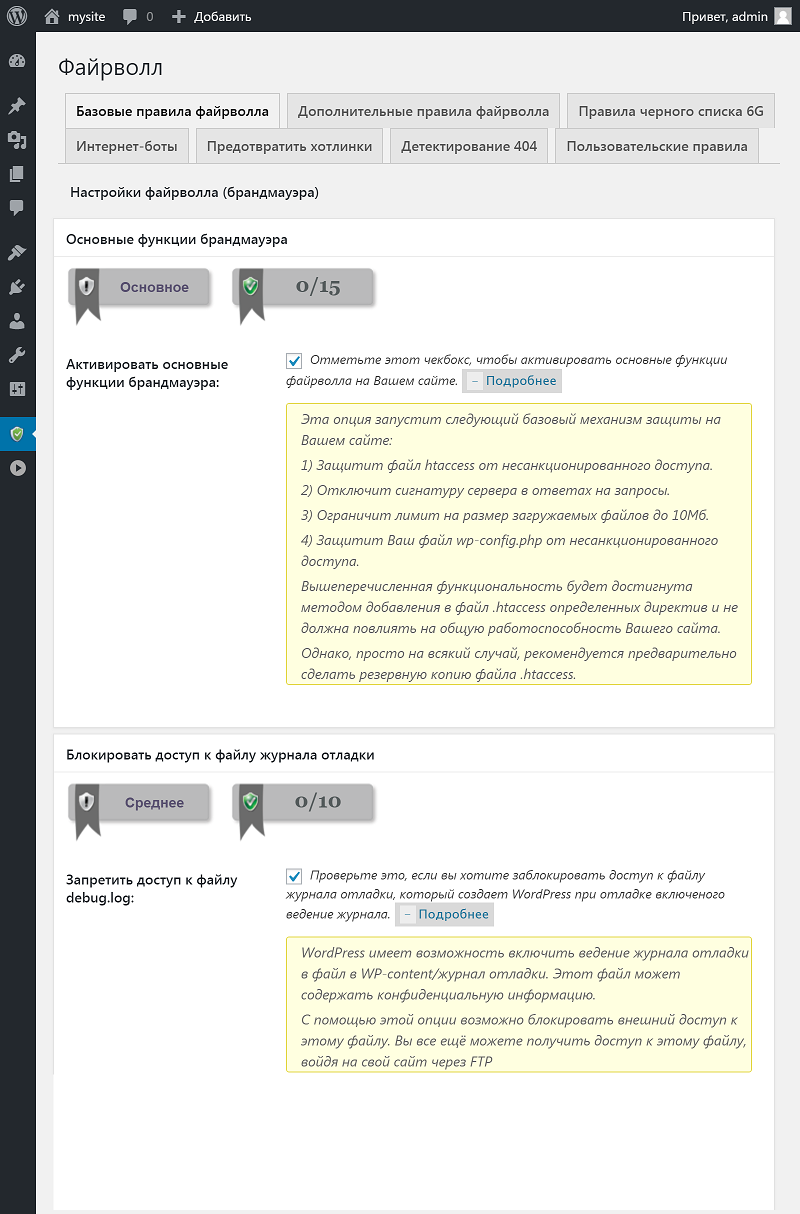


Рисунок 21 - Базовые настройки файрволл

2) Настройки черного списка/фаерволла 6G

6G-брандмауэр (файрволл) - это простая и гибкая защита, помогающая уменьшить количество вредоносных запросов, добавляемых в URL Вашего сайта.  
Дополнительным преимуществом 5G-защиты является тот факт, что она была тщательно протестирована и подтверждена профессионалами из PerishablePress.com, как наименее разрушительный набор директив безопасности для файла .htaccess, на сайтах, работающих на сервере Apache или аналогичных.  
Следовательно, данная защита не должна иметь никакого влияния на общую функциональность Вашего сайта  
Устанавливаем галочки на параметрах:  
- **включить защиту фаерволла 6G;**  
- **включить старую защиту фаерволлом 5G**

Функционал установленных параметров также расписан на рисунке 22.

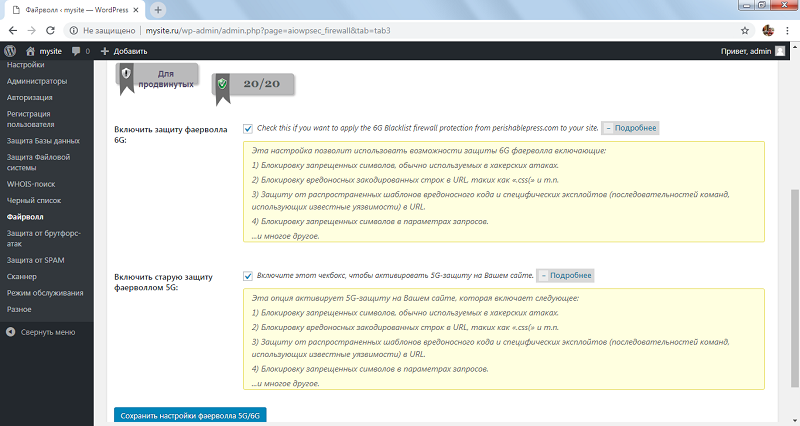


Рисунок 22 - 6G-брандмауэр

**Итоги**

После завершения всех этих настроек, вновь переходим в **Панель управления** и смотрим показатель уровня безопасности.  
В итоге уровень должен быть приравнен показателю изображенному на рисунке 23.

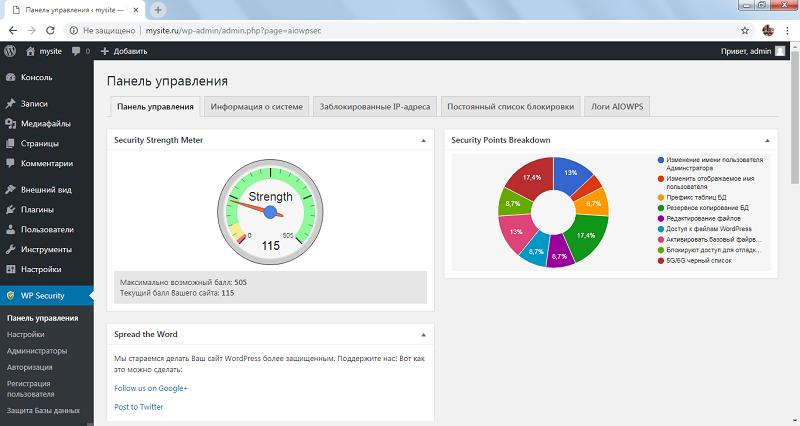


Рисунок 23 - Показатели безопасности

**Вопросы для самоконтроля**

1. Что показывает Security Strength Meter в плагине All In One WP Securite?  
2. Файл "\_\_\_\_\_\_\_\_" - это ключевой компонент безопасности сайта.  
3. Файл "\_\_\_\_\_\_\_\_" содержит данные доступа к базе данных  
4. Редактирование файлов PHP требуется \_\_\_\_\_\_  
5. Для безопасности сайта, требуется \_\_\_\_\_\_\_ файрволл