Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ САЙТА КОМПАНИИ

Выпускная квалификационная работа
по направлению 44.03.04 Профессиональное обучение (по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 501

Екатеринбург 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующий кафедрой ИС
_____И. А. Суслова
«____» _____2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ САЙТА КОМПАНИИ

Исполнитель:
обучающийся группы № ЗИБ–501 М. Б. Ефремов
Руководитель:
кандидат педагогических наук,
доцент Н. С. Власова
Нормоконтролер: С. Ю. Ярина

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из сайта и пояснительной записки на 81 странице, содержащей 65 рисунков, 38 источников литературы.

Ключевые слова: САЙТ, БЕЗОПАСНОСТЬ, WORDPRESS.

Ефремов М. Б. Обеспечение безопасности сайта компании: выпускная квалификационная работа / М. Б. Ефремов; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 83 с.

В работе рассмотрены вопросы разработки и безопасности сайта.

Целью работы является обеспечение безопасности программной и серверной части сайта компании ООО «УралТрейд». Для достижения цели были проанализированы современные методы используемых уязвимостей и атак в распространенных системах управления контентом, способы защиты от уже известных программных и серверных уязвимостей сайта, технологии разработки сайта, выбор оптимального хостинга и возможности локальной разработки. Также был проведен анализ различных источников информации и аналогичных сайтов. Разработан сайт, содержащий информацию о компании, предоставляемых услугах, контактах, вакансиях, и размещенных документах, а также обеспечен комплекс мер для повышения уровня безопасности программной и серверной составляющей части сайта, подготовлен обучающий материал для администратора сайта.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В России появляется всё больше разнообразных компаний, которым необходимо продавать свои товары и услуги. Для этой цели им необходима известность, чтобы как можно больше людей знали о них и о том, что именно они лучше, чем любая другая организация, которая имеет такое же направление. Для этого используют рекламу. Для того, чтобы как можно больше клиентов увидело рекламу, необходимо использовать то, что люди часто используют: телевидение, радио, рекламные щиты. Но в данный момент наибольшую популярность имеет именно интернет.

Интернет в России с каждым годом становится лишь популярнее, и большая доля населения имеет у себя дома или на работе выход к его ресурсам. Благодаря этому люди получили доступ к огромному количеству информации, возможность обучаться или найти ответы на многие интересующие их вопросы, но особенно широко это направление используют именно в рекламных целях. Многие компании создают собственные веб-сайты для информирования клиентов о своей деятельности, контактах. Благодаря чему каждый человек может не только узнать о возможностях выбранной организации, не выходя из дома, но и сделать заказ интересующей его продукции или услуги.

На сегодняшний день наличие корпоративного веб-сайта является необходимостью, даже если деятельность компании не связана с информационными технологиями и интернет-продажами. В некоторых отраслях, таких, как образовательные сайты, для удобства упорядочивают структуру сайта, подбивая под единый шаблон, чтобы пользователи не тратили время при сравнении. В статьях или новостях, публикующихся в сети, обязательно вставляются ссылки на корпоративный сайт упомянутой компании.

Сейчас уже не встает вопрос: нужен сайт или не нужен, но очень актуальна тема создания максимально удобного и информационного сайта, благодаря которому повысится престиж организации.

Использование системы управления контентом (CMS) обусловлено большим прорывом в технологии создания и разработки современных вебсайтов [22]. Нынешние системы управления контентом широко применяются при создании сайтов любой сложности. По сути CMS — это система управления контентом, представляющая собой сбалансированное сочетание различных программных средств, которые предназначены для подготовки, редактирования и публикации информации на сайте. Кроме того, любая современная CMS — включает в себя различные инструменты, необходимые для эффективного управления функциональными возможностями сайта.

Довольно большое распространение при создании своего сайта получили бесплатные CMS [11]. Многие подобные системы имеют хороший функционал и высокую надежность, благодаря чему у них появляется большое преимущество среди платных систем.

Основной отличительной чертой систем управления контентом, которая одновременно являются преимуществом: возможность быстрого, простого и интуитивно-понятного добавления, удаления или изменения контента, что значительно упрощает администрирование сайта и позволяет выполнять эту задачу даже штатному маркетологу, а также позволяет значительно разнообразить общий вид сайта и привлечь интересным контентом новых посетителей. Также стоит отметить, что все системы управления контентом обладают практичной панелью администратора, которая затрагивает все сферы работы сайта.

Объект исследования — исследование методов обеспечения безопасности сайта.

Предмет исследования — процесс организации безопасности программной и серверной составляющей сайта.

Цель работы — обеспечить безопасность программной и серверной части сайта компании ООО «УралТрейд».

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Проанализировать литературные и электронные источники, посвященные сравнительному обзору различных CMS, их уязвимостей, и средства обеспечения защиты сайта, изучить устав компании, учредительные документы.
2. Реализовать сайт средствами выбранной системы управления контентом.
3. Обеспечить безопасность программной составляющей части сайта.
4. Обеспечить безопасность серверной составляющей части сайта.
5. Подготовить обучающий материал для администратора сайта.

1 ПРОБЛЕМЫ БЕЗОПАСНОСТИ ВЕБ-САЙТОВ

1.1 Анализ угроз и атак, применяемых к веб-ресурсам

Один из наиболее важных вопросов в контексте информационной безопасности — безопасность сайтов. Как правило, большинство веб-сайтов, доступных в Интернете, имеют различного рода уязвимости и постоянно подвергаются атакам. Не секрет, что сайты, созданные на CMS WordPress, особенно активно подвергаются стороннему вмешательству. Для периодической проверки защищенности сайта, существует ряд действий, которые принято называть аудитом безопасности сайта WordPress.

Основные проблемы безопасности WordPress: их динамичность и скрытость. Динамичность подразумевает новые варианты взлома сайтов, скрытность — невозможность понять, что сайт взломан без специальных инструментов анализа.

Существует ряд часто используемых и потенциальных уязвимостей WordPress, он включает:

1. SQL Injection (SQLI) — возникает, когда SQL-запросы могут вводиться и выполняться с URL-адреса сайта.
2. Межсайтовый скриптинг (XSS) — хакер может вводить код в сайт, как правило, через поле ввода.
3. Загрузка файлас вредоносным кодом на незащищенный сервер.
4. Подпрограмма запроса на межсайтовый запрос (CSRF) — код или строки вводятся и выполняются с URL-адреса сайта.
5. BruteForce — метод подбора. Постоянные попытки войти в систему, угадывая имя пользователя и пароль учетной записи администратора.
6. Отказ в обслуживании (DoS) — когда сайт падает из-за постоянного потока трафика, исходящего от хакбота.

7. Распределенный отказ в обслуживании (DDoS). Подобно атаке DoS, за исключением того, что hackbot отправляет трафик из нескольких источников, таких как зараженные компьютеры или маршрутизаторы.

8. Open Redirect — внедряется в код, и страница сайта постоянно перенаправляется на другую страницу со спамом или на другой (фишинговый) сайт, установленный злоумышленником.

9. Вредоносное ПО — вредоносный скрипт или программа с целью заражения сайта или операционной системы.

10. Локальное включение файлов (LFI) — злоумышленник может контролировать, какой файл выполняется в запланированное время, установленное CMS или веб-приложением.

11. Обход аутентификации — проблема безопасности, позволяющая злоумышленнику обойти регистрационную форму и получить доступ к сайту.

Перечисленные уязвимости являются наиболее распространенными способами взлома сайта с помощью ботов. Могут быть применены несколько разновидностей атак одновременно [36].

Основные мероприятия, которые нужно включить в аудит безопасности WordPress сайта:

1. Актуальность версии. Необходимо убедиться, что система управления контентом WordPress обновлена до последней версии. Разработчики системы и сообщество WordPress постоянно следят за возникающими проблемами уязвимости и в кратчайшие сроки после выявления уязвимости, выпускают релизы безопасности с её устранением.

2. Префикс базы данных. Этот пункт необходимо выполнять еще во время установки. Префикс базы данных в виде двух букв [wp_] следует сменить и использовать для префикса четыре цифры и/или буквы (можно больше).

3. Простые логины. Следует исключить из пользователей и не допускать регистрации тех, кто в качестве логина использует «administrator» или

«admin», так как подобные логины используются при подборе пароля в первую очередь.

4. Исключить использование простого пароля администратора. Чтобы злоумышленники не могли взломать сайт, необходимо использовать сложные пароли.

5. Актуальность активных и пассивных плагинов сайта. Своевременное обновление плагинов так же повышает безопасность сайта, так как есть вероятность взлома сайта через плагины, которые не имеют актуальных исправлений.

6. Резервное копирование. Важно, чтобы под рукой, всегда была свежая резервная копия файлов сайта и базы данных.

7. Плагин безопасности. Завершить аудит безопасности WordPress сайта можно установкой профильного плагина.

Основным источником угроз информационной безопасности веб-приложения являются внешние нарушители. Внешний нарушитель — лицо, мотивированное, как правило, коммерческим интересом, имеющее возможность доступа к сайту компании, обладающее достаточными знаниями об исследуемой информационной системе, имеющее высокую квалификацию в вопросах обеспечения сетевой безопасности и большой опыт в реализации сетевых атак на различные типы информационных систем.

Если сказать иначе — основная угроза безопасности сайта — хакерская атака, которая может иметь конечную цель, быть целевой атакой, либо носить бессистемный характер.

В первом случае злоумышленник может выявлять максимально возможное количество векторов атаки для составления и реализации потенциально успешных сценариев взлома, во втором — объекты атакуются массово, обычно используя несколько поверхностных уязвимостей.

Основные типы угроз информационной безопасности веб-приложения:

- угрозы конфиденциальности — несанкционированный доступ к данным;

- угрозы целостности — несанкционированное искажение или уничтожение данных;
- угрозы доступности — ограничение или блокирование доступа к данным.

Уязвимости веб-приложений, чаще всего, приводят к выполнению кода на удаленном сервере. Во всех серверах используются данные, которые передаются пользователем при обработке запросов. Часто эти данные используются при составлении команд, применяемых для генерации динамического содержимого. Если при разработке не учитываются требования безопасности, злоумышленник получает возможность модифицировать исполняемые команды. К подобным уязвимостям относятся, например, SQL-injection.

Атаки, направленные на используемые веб-приложением методы проверки идентификатора пользователя, службы или приложения, либо направленные на методы, которые используются веб-сервером для определения того, имеет ли пользователь, служба или приложение необходимые для совершения действия разрешения. К таким атакам относятся — bruteforce, обход авторизации, небезопасное восстановление паролей, предсказуемое значение сессии или её фиксация.

Во время посещения сайта, между пользователем и севером устанавливаются доверительные отношения, как в технологическом, так и в психологическом аспектах. Пользователь предполагает, что сайт предоставит ему необходимую информацию, и не предполагает наличие опасности. Эксплуатируя это доверие, злоумышленник может использовать различные методы для проведения атак на клиентов сервера. Такого рода атаки могут быть задействованы как в сложных сценариях атаки (watering hole, drive by), так и в более привычных — клиент-сайд атаках, например, XSS.

К разглашению информации относится как информация непосредственно о веб-приложении, его компонентах, платформе и составляющих, так и утечка чувствительной информации с сайта, из-за её ненадлежащей защиты. Подразумевается раскрытие информации лицам, доступ к которым им за-

прещен, либо раскрытие информации в результате неверной настройки веб-приложения или веб-сервера.

Также возможны логические атаки, которые направлены на эксплуатацию функций приложения или логики его функционирования. Логика приложения представляет собой ожидаемый процесс функционирования программы при выполнении определенных действий.

В качестве примеров можно привести восстановление паролей, регистрацию учетных записей, транзакции в системах электронной коммерции. Приложение может требовать от пользователя корректного выполнения нескольких последовательных действий для выполнения определенной задачи. Злоумышленник может найти способ обхода или использовать эти механизмы в своих целях.

К подобным атакам относятся и атаки класса отказ в обслуживании, DoS.

Виды атак на веб-приложения

Целевые атаки — это атаки, специально нацеленные на один сайт или их группу, объединенную одним признаком (сайты одной компании, либо сайты, относящиеся к определённой сфере деятельности, либо объединенные рядом признаков). Опасность таких атак заключается именно в «заказном» характере. Исполнителями чаще всего становятся высококвалифицированные в области безопасности веб-приложений злоумышленники.

Цель подобных атак — получение конфиденциальной информации, которую можно использовать для получения прибыли.

Нецелевая атака на сайт — это попытка получения несанкционированного доступа к веб-ресурсу, при которой злоумышленник не ставит целью взломать конкретный сайт, а атакует сразу сотни или тысячи ресурсов, отобранных по какому-то критерию. Например, сайты, работающие на определенной версии системы управления контентом. Такого рода атаки бьют по «площадям», стараясь охватить максимальное количество сайтов при минимуме затрат.

При удачной попытке атаки злоумышленник старается извлечь из этого пользу: закрепиться на сайте, загрузив хакерский скрипт (бэкдор, веб-шелл), добавить еще одного администратора, внедрить вредоносный код или получить необходимую информацию из базы данных.

Целевые атаки — проводятся скрытно, как правило, достигают своей цели. Нецелевые атаки довольно «шумные» и зачастую не достигают поставленных целей, но, тем не менее, могут доставить множество проблем владельцу веб-ресурса.

В первую очередь это несет угрозу работоспособности сайта. Во вторую — сохранность пользовательских данных. Из этих причин вытекает логичное следствие — финансовые и репутационные потери компании.

Хакеры используют сайт для атак на другие ресурсы, в качестве опорного плацдарма, для рассылки спама или проведения DoS атак. В результате сайт блокирует поисковые системы и браузеры, теряются пользователи.

Распространение атак на веб-приложения связаны с двумя основными факторами: халатное отношение к безопасности сайта и низкий порог входа потенциальных злоумышленников.

В большинстве случаев на сайтах не используются специальные средства обнаружения, мониторинга и защиты, нет ответственного персонала и осведомленности об угрозах безопасности сайта. Качеству кода и безопасной настройке веб-приложения или веб-сервера уделяется мало внимания [18].

Безопасность сайта складывается из трех вещей:

- безопасности программной части (CMS, скриптов);
- безопасности сервера (хостинга);
- осведомленности и аккуратности администратора сайта или тех, кто работает с сайтом как администратор.

Если все три составляющих организованы надлежащим образом, то сайт будет неприступным для хакеров и вирусов.

Надежность программной части

Программная часть — это система управления контентом (Joomla, WordPress, Bitrix и др.) или скрипты, на которых работает сайт. Надежность программной части подразумевает отсутствие уязвимостей, позволяющих злоумышленнику получить доступ к базе данных, файловой системе или панели администратора сайта.

Чтобы в программной части не было уязвимостей, необходимо разрабатывать скрипты с оглядкой на безопасность, что выполняется не всегда. Практически в каждой CMS или в скрипте существуют уязвимости. Часть из них опубликована в открытом доступе (публичные уязвимости), другая недоступна широкой аудитории и используется злоумышленниками для целевых атак на сайты. Для того чтобы программная часть сайта была надежна и неприступна, нужно уделять внимание проблеме безопасности.

Если сайт работает на одной из популярных систем управления контентом, нужно следить за обновлениями и патчами, и своевременно обновлять CMS до самой последней доступной версии.

Если сайт работает на скриптах собственной разработки, нужно выполнить сканирование сайта доступными средствами поиска уязвимостей (XSpider’ом, Acunetix Web Vulnerability Scanner’ом, утилитами для поиска SQL инъекций, XSS, RFI и другими), проверить исходный код сайта средствами статического анализа исходного кода (RIPS) и, если обнаружатся уязвимости, исправить их.

Кроме регулярных обновлений скриптов и CMS есть еще один важный момент, усиливающий безопасность и надежность скриптов — это правильная конфигурация сайта. Необходимо:

- грамотно настроить права на файлы и директории;
- закрыть доступ к внутренностям сайта (каталогам с резервными копиями, конфигурационным файлам и пр.);
- запретить выполнение скриптов в директориях загрузки;

- поставить дополнительную защиту на вход в панель администратора и др.

Данные меры позволяют значительно снизить вероятность взлома сайта, даже при наличии уязвимостей в программной части.

Вторым важным моментом, влияющим на безопасность сайта в целом, является хостинг, на котором размещается сайт. Хостинг может быть shared («общий») или dedicated («выделенный»).

Для shared-хостингов ответственность за настройку безопасности сервера лежит на администраторе хостинг-компании. Для dedicated-сервера (VDS/VPS) эта ответственность лежит на владельце сервера.

Как в случае shared-хостинга, так и в случае dedicated-сервера конфигурация должна обеспечивать минимальную свободу действий, не нарушающих работоспособность сайта. То есть на сервере должны быть разрешены только самые необходимые функции, а все остальное — запрещено. Например, если сайт не выполняет внешних подключений к другим серверам, должны быть отключены опции внешних соединений. Кроме того, должна быть ограничена область видимости файловой системы из скриптов и многое другое. Обо всем этом должен позаботиться системный администратор сервера.

Как известно, на одном сервере shared-хостинга размещаются сотни сайтов, и каждому сайту требуются свои функции. Поэтому хостинг-провайдеры максимально лояльно подходят к вопросам настроек сервера, разрешая практически все. Естественно, это сказывается на общем уровне безопасности всех сайтов, размещенных на их серверах. Поэтому владельцам сайтов нужно тщательно подходить к вопросу выбора хостинга: выбирать тот, который позволяет производить настройку веб-сервера и PHP персонально для аккаунта, а не использовать установки по умолчанию.

Настройку dedicated-сервера должен проводить опытный системный администратор, который изолирует сайт от остальной части системы, максимально ограничит свободу скриптов и область их видимости, а также органи-

зует механизмы контроля целостности файловой системы, систему резервного копирования и логирования.

Владельцы сайта, обычно, уделяют мало внимания вопросам безопасности, предполагая, что программная часть безупречна, настройки сервера надежны и безопасны. Хотя собственная беспечность наиболее часто является причиной взлома сайтов и заражения вирусами.

Ниже приведен чеклист, который должен постоянно держать в голове администратор (владелец) сайта:

1. Компьютер, с которого выполняется работа с сайтом, должен быть защищен коммерческим антивирусным программным обеспечением и регулярно им проверяться. Если с сайтом работает несколько человек, данное требование применяется к каждому.
2. Пароли от ftp/ssh/панели администратора нужно менять регулярно, хотя бы раз в месяц.
3. Не хранить пароли в программах (ftp-клиентах, браузере, электронной почте).
4. Ставить сложные пароли.
5. Работать по безопасному протоколу SFTP или SCP.

Чтобы сайт был защищен от вирусов и хакеров, нужно достаточно много внимания уделять проблеме безопасности: поддерживать программное обеспечение в актуальном состоянии, правильно настраивать хостинг и следить за доступами к сайту. Если хотя бы один из трех элементов будет слабым звеном, сайт останется уязвимым [5].

Одним из самых рекомендуемых дополнений, обеспечивающих безопасность сайта, построенного на платформе WordPress, является плагин All In One WP Security. Несмотря на многочисленный функционал, плагин использует минимум ресурсов, что позволяет не нагружать сайт. И при всех возможностях он совершенно бесплатный и весьма прост в использовании. Имеет три степени сложности: простой, промежуточный, продвинутый. Та-

ким образом, правила брандмауэра можно применять постепенно, не нарушая функциональность сайта [16].

Функции плагина:

- делает резервные копии базы данных, файла конфигурации wp-config.php и файла .htaccess;
- смена адреса страницы авторизации;
- скрытие информации о версии WordPress;
- защита административной панели — блокировка при неправильной авторизации;
- защита от роботов и др.

Огромные плюсы плагина All In One WP Security:

- бесплатный;
- простой в настройке;
- русифицированный.

All In One WP Security использует беспрецедентную систему оценки точек безопасности, чтобы определить, насколько хорошо защищен сайт, основываясь на активированных функциях безопасности [32].

1.2 Обзор систем управления контентом и их уязвимостей

Система управления контентом (CMS или Content management system) — программная основа для разработки и редактирования сайта, другими словами — это платформа, которая позволяет создать веб-ресурс и наполнять его статьями, фотографиями, видео и другими данными [23].

Content management system также называют «движками» сайта. Несмотря на многообразие существующих сегодня CMS-систем, нет оптимального решения, которое бы подошло для успешной реализации и сайта-визитки, и интернет-магазина. У каждого движка есть свои достоинства и недостатки [6].

Главной функцией CMS является показ страниц сайта для пользователей, генерируя их содержимое с использованием заранее заданных шаблонов, дизайна и контента, которые хранятся в базе данных. Очень важно понимать, что сайта в целом как набора страниц не существует. Имеются отдельно шаблоны и набор различных материалов (контент): текст, изображение, файлы с архивами и другие материалы. CMS генерирует страницу для пользователя в момент запроса. При этом пользователю может быть предоставлена уникальная информация, которая другим никогда не будет показана. Например, содержимое корзины при заказе в интернет-магазине.

Второй функцией CMS является помощь владельцу сайта без специальных навыков и умений управлять сайтом, публикуя новые страницы или новости, выкладывая видео, размещая ссылки как на внешние, так и на внутренние ресурсы. Для редактирования любой страницы администратору доступен визуальный редактор, позволяющий форматировать текст, добавлять ссылки и изображения, при этом видя все в таком же виде, как это будет отображаться на сайте.

Поскольку создать сайт с помощью CMS можно быстро и без специальных навыков, этот инструмент становится всё более популярным.

Преимущества CMS:

1. Создание сайта при помощи CMS не требует никаких специальных знаний и навыков.
2. CMS несёт в себе достаточно большую функциональность, что позволяет не тратить лишнее время на поиск или написание отдельных скриптов.
3. При создании сайта на CMS экономится время.
4. При выборе популярной CMS можно найти большое число разнообразных шаблонов и дополнительных модулей, расширяющих функциональность, а также получить советы по настройке, установке и решению тех или иных проблем от сообщества разработчиков и пользователей этой CMS.

Недостатки CMS:

1. Чтобы освоить работу с каждой конкретной CMS, требуется какое-то время.

2. Быстрое создание сайта с помощью CMS, может привести к тому, что он будет похож на множество других.

3. Иногда функциональность CMS оказывается недостаточной, либо немножко не такой, как нужно.

4. Для простых сайтов функциональность CMS, как правило, оказывается чрезмерной, из-за чего сайты на данной платформе работают медленнее, занимают больше места на хостинге, в большей мере подвержены сбоям.

5. У многих распространённых CMS, до сих пор не редкость проблемы с безопасностью, из-за чего сайт могут взломать хакеры.

Из всего вышесказанного следует, что существует много разнообразных CMS. Каждая из них имеет свои преимущества и недостатки, не стоит забывать и про личные предпочтения пользователей. Главная задача этого анализа — выбрать наиболее подходящую платформу для создания собственного сайта.

Для решения поставленной задачи было решено просмотреть наиболее популярные платформы, что позволит заметно сократить затраты на время, необходимого для сравнения разных CMS, изучить их достоинства и недостатки.

Благодаря интернет-источникам были найдены данные о популярных CMS, обнародованные в статье «Рейтинг Рунета» 2017 года. Данный рейтинг учитывал тематический индекс цитирования (тИЦ) и посещаемость ресурсов, созданных с помощью разных систем управления контентом (рисунок 1).

В результате для сравнительного анализа были выбраны четыре лидирующие платформы: WordPress, Joomla, Drupal иMODX.

С помощью WordPress можно создавать сайты различного типа: информационные, новостные и т. п. Данная платформа хорошо русифицирована, легко устанавливается: процесс установки занимает менее пяти

минут от начала до конца. Наполнение сайта контентом не требует никаких дополнительных знаний.

#	CMS	Проекты	Балл	Тренд
1	WordPress	5 516	24.59	↗
2	Joomla!	6 453	24.53	—
3	Drupal	3 359	23.86	↘
4	MODX	4 640	17.96	↘

Рисунок 1 — Рейтинг популярных систем управления контентом

WordPress — самая популярная CMS на сегодняшний день [14]. Это видно из «Рейтинга Рунета», так же в этом можно убедиться, если посмотреть рейтинг Google Trends (рисунок 2) за последние пять лет.

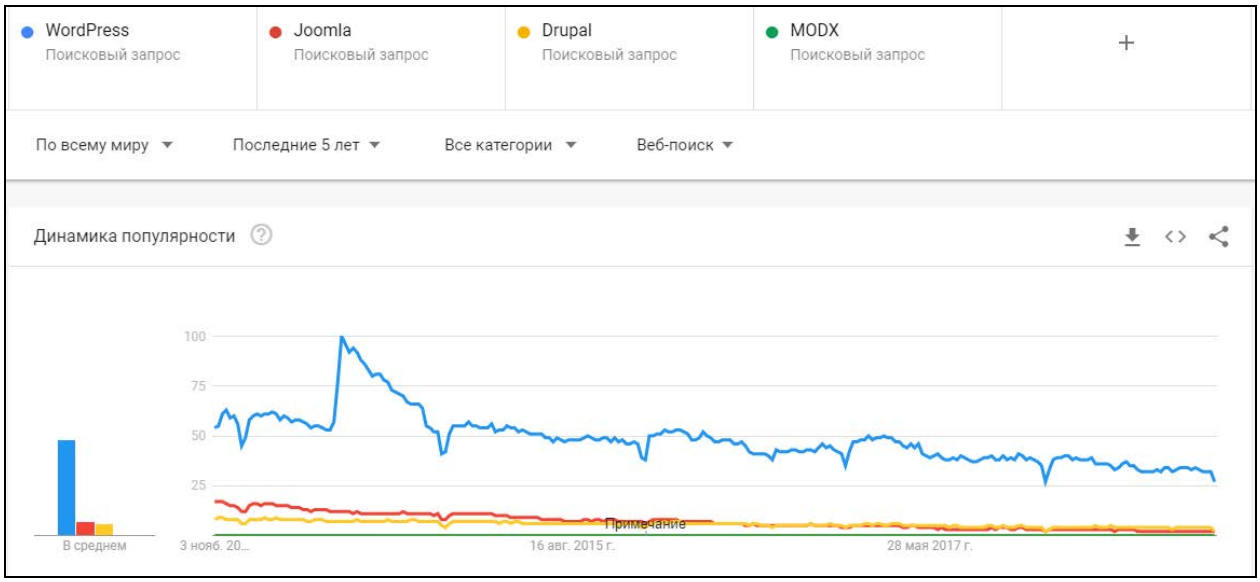

Рисунок 2 — Рейтинг Google Trends

По данным рейтинга можно увидеть, что популярность другого распространенного движка Joomla падает, а желающих воспользоваться WordPress стало незначительно меньше.

Преимущества WordPress:

1. Очень простое создание сайта.
2. Настраиваемые темы для создания уникального дизайна.
3. Плагины для расширения.
4. Большое количество документации.

5. WordPress создана профессиональными разработчиками;

6. Более 50% сайтов, созданных на CMS, используют WordPress.

Недостатки WordPress:

1. Сравнительно ограниченные возможности настроек.

2. Отсутствует сохранение пользовательских изменений исходного кода при обновлении.

3. Высокая уязвимость плагинов.

Возможные уязвимости веб-ресурсов, использующихWordPress:

1. Misconfiguration (ошибочная настройка) — неправильная установка CMS на хостинг, что ведет к возможности получения полного контроля злоумышленником над данным ресурсом в пределах подпапки на сервере или, что гораздо реже, содержимого корневой папки.

2. Injectionflaws — возможность для инъекций вредоносного кода разных видов. Это может произойти при передаче неотфильтрованных данных на сервер SQL (SQL-инъекции), в браузер (XSS) и т. п. Злоумышленник может внедрять таким образом исполнительные команды (скрипты), что позволяет использовать браузеры клиентов для кражи информации.

3. Crosssitescripting (XSS) — довольно частый случай инъекций. Хакер подает веб-приложению на вход код, написанный на языке программирования JavaScript. При случайном обращении к нему пользователем произойдет немедленное выполнение скрипта браузером. Он может быть замаскирован в виде простой фишинговой кнопки или менее приметным образом. На загруженной странице начинает работать сценарий, который, например, может быть использован для отправки cookies злоумышленнику [35].

Joomla — вторая по популярности CMS в мире. Как и WordPress, она бесплатная, невероятно простая, доступная и надежная. По сути, она обладает всеми качествами WP. Главное отличие Joomla от более успешного open-source решения — более сложное управление. Её не так просто установить, настроить и наполнить контентом.

Преимущества Joomla:

1. Множество решений для интернет-магазинов.
2. Возможность оптимизации без дополнительных плагинов.
3. Сразу доступно кеширование.
4. Большое количество документации.
5. Более 2,8% сайтов, созданных на CMS, используют Joomla.

Недостатки Joomla:

1. Немного ограниченные возможности настроек.
2. Недостаточная обработка SQL-запросов и загружаемых файлов.
3. Малое количество плагинов.

Возможные уязвимости веб-ресурсов, использующихJoomla:

1. Компонент SimpleFaq 2.x (com_simplefaq). Уязвимость позволяет удаленному пользователю с помощью специально сформированного запроса выполнить произвольные SQL команды в базе данных приложения. Уязвимость существует из-за недостаточной обработки входных данных в параметре aid в установочном сценарии Joomla -index.php.

2. Компонент ReMOSitory 341RE (com_remository). Уязвимость существует из-за недостаточной обработки загружаемых файлов на сервер, и наличия прямого доступа к ним по умолчанию.

Drupal — это CMS совершенно другого уровня. Если Joomla и WordPress — простые, но ограниченные решения, то Drupal — платформа, которая позволяет воплотить практически любой ваш замысел, но требующая определенных навыков.

Преимущества Drupal:

1. Высокий уровень безопасности.
2. Большая оптимизация.
3. Гибкие настройки прав пользователей.
4. Большое количество готовых бесплатных плагинов.
5. Более 2,2% сайтов, созданных на CMS, используют Drupal.

Недостатки Drupal:

1. Высокая стоимость разработки.
2. Высокая сложность настройки.

Возможные уязвимости веб-ресурсов, использующих Drupal:

1. Уязвимость из-за ошибки, связанной с модулем OpenID. Удаленный пользователь может авторизоваться от имени административного пользователя и захватить контроль над учетной записью.
2. Уязвимость из-за ошибки, связанной с модулем Field UI. Удаленный пользователь может перенаправить произвольного пользователя на произвольный веб-сайт.
3. Уязвимость из-за ошибки, связанной с модулем Overlay. Удаленный пользователь может перенаправить произвольного пользователя на произвольный веб-сайт.
4. Уязвимость из-за ошибки, связанной с обработкой кеша. Удаленный пользователь может получить доступ к важным данным.

MODX — еще одно решение для тех, кто не привык себя ограничивать. Так же как Joomla похожа на WordPress, CMS MODX похожа на Drupal. MODX подойдет для разработки любого сайта: блога, форума, огромного портала, сервиса с онлайн-платежами и т.п.

Преимущества MODX:

1. Много типов контента.
2. Высокий уровень безопасности.
3. Seo без дополнительных модулей и настроек.
4. Возможность создания мультиязычных сайтов.
5. Более 1% сайтов, созданных на CMS, используют MODX.

Недостатки MODX:

1. Высокая стоимость разработки.
2. Ограниченное количество встроенных шаблонов.
3. Ограниченное количество плагинов.
4. Высокая сложность настройки.

Рассмотрев распространенные CMS с открытым исходным кодом, становится ясно, что большим преимуществом обладает CMS WordPress. Так как компания не планирует использовать большое количество плагинов и хочет запретить процессы регистрации, авторизации и публикации комментариев, то вполне подходит для решения поставленной задачи. Кроме того, CMS вполне подходит для структуры сайта компании «УралТрейд» [8].

1.3 Характеристика системы управления контентом WordPress

Платформа WordPress является системой с открытым исходным кодом и может быть изменена и отредактирована любым пользователем в соответствии с его потребностями [33]. Платформа написана на языке PHP, который является серверным языком программирования с открытым исходным кодом. Платформа использует базу данных MySQL для хранения такого контента, как сообщения, комментарии, изображения и т.д. MySQL также является программным обеспечением с открытым исходным кодом и находится в свободном доступе [4].

WordPress — это одна из CMS (Content Management System). Данная аббревиатура означает специальное программное обеспечение для создания и дальнейшего редактирования содержимого сайта, а также управления контентом и регулирования не только его внешних характеристик (дизайна), но и функциональных особенностей.

Главное преимущество такой системы — возможность для владельца ресурса вносить правки в любой момент, не привлекая специалистов. Данная платформа написана и работает на языке программирования PHP, этот скриптовый язык используется для разработки веб-приложений. Для создания динамичных сайтов с различными скриптами, шаблонами и различного рода контентом это наиболее популярный на сегодня инструмент. Проект изначально стал выпускаться под собственной лицензией, несовместимой с универсальной GNU General Public License. WordPress была выпущена под

лицензией GNU, это значит, что программное обеспечение передается автором в общественную собственность. На тот момент это была вторая версия, дававшая право использования также в некоторых библиотеках ПО. Сегодня применяется третья версия лицензии, предоставляющая возможность получения исходного кода тем пользователям, которые работают с ней исключительно через сеть.

В WordPress есть огромное количество плагинов, ознакомиться с ними можно на официальном сайте. Это специальные расширения, создающие дополнительный функционал. Виджеты — модули, с помощью которых необходимая информация помещается в сайдбар ресурса. В свою очередь, сайдбар — та область, где и находятся самые разные виджеты.

При работе с функционалом WordPress пользователи также сталкиваются с таким понятием, как мультисайт. Это один из режимов работы ресурса, когда в панели администратора выбирается управление сразу несколькими сайтами из одной учетной записи.

Слаг или ярлык — ссылка, созданная специально для определенной страницы, записи, рубрики, то есть уникальная по сути.

Информацию можно найти и отредактировать в разделе «Свойства».

Тема — файлы, использующиеся для графического оформления сайта, его функционал.

При этом важно, что в использование термина «Шаблон» неправильно. На данный момент в сети находится огромное количество тем, скачать которые не представляет никакого труда [17].

WordPress разрабатывалась, как система для удобного создания и ведения интернет-дневников. Однако благодаря тому, что «движок» этой системы допускает подключение внешних модулей, её функциональность практически ничем не ограничена, что позволяет использовать WordPress для разработки интернет-ресурсов практически любого типа: от обычных блогов до новостных порталов со сложной структурой [3].

С помощью WordPress можно создавать совершенно разные сайты, например:

1. Интернет-магазин: чтобы это реализовать, нужно установить несколько специальных плагинов. Одними из самых распространенных являются WP Commerce и eShop. Первый применяется в случае создания большого и функционального интернет-магазина, второй — когда нужно реализовать небольшой проект, так называемый «интернет-ларек». Еще одним популярным плагином является WooCommerce, функционал которого предоставляет большие возможности создания полноценных интернет-магазинов. Стоит учитывать, что интернет-магазины, построенные на WordPress, как правило, сильно нагружают серверы, поэтому лучше их устанавливать на проверенные хостинги.

2. Веб-сайт для бизнеса. Сайт для бизнеса на WordPress, это одна из возможностей дать развитие делу, с минимальными затратами времени и денег. Для данной CMS создано довольно много сервисов, скриптов и плагинов, которые в комплексе способны сделать проект многофункциональным и интересным.

3. Портфолио. WordPress идеальное решение для фрилансеров, которые хотят продемонстрировать свою работу.

4. Адаптивный сайт и другие. Одной из главных особенностей WordPress является структура организации базы данных. Гибкость и функциональность связей позволяют создавать и выводить на страницу материал любого вида с любыми параметрами.

Встроенная система «тегирования» создает дополнительные связи для материалов сайта, что при необходимости, позволяет оперировать всеми записями, соответствующими определенным условиям.

В системе управления контентом WordPress предлагается гибкая схема организации структуры сайта на основе таксономии. Таксономия — механизм, позволяющий создавать произвольное количество связей между объек-

тами содержимого сайта и ассоциировать их с «Ключами записей», «Категориями записей» или «Категориями ссылок».

«Категории», «Ключевые слова» и «Ссылки» могут представлять плоские или иерархические списки, либо сложные структуры, где элемент может иметь несколько «родителей» и несколько дочерних элементов. С помощью подобной схемы одними и теми же компонентами системы управления контентом возможна организация различных вариантов структуризации, обработки, редактирования и вывода содержимого.

При выборе системы WordPress для создания сайта, можно выделить следующие преимущества:

1. Систему можно скачать бесплатно. Каждый, кто захотел создать свой собственный блог или сайт, может без лишних затрат и вложений сделать это с помощью WordPress.
2. Простая установка и настройка.
3. Наличие удобного, настраиваемого интерфейса. Все элементы сайта находятся в единой структуре. Например: все меню в разделе меню, все страницы — в страницах, статьи — в статьях, товары — в товарах.
4. Простая в администрировании система управления сайтом. «Визуальный редактор» — потрясающе удобен как для начинающих, так и для продвинутых пользователей, в режиме редактирования сразу виден конечный результат.
5. Хорошее SEO продвижение. Благодаря модульной системе выполнить все рекомендации Яндекс и Google гораздо проще, чем, если использовать другие платформы.
6. Современный и адаптивный дизайн. Большинство сайтов на WordPress создаются в современном стиле с адаптивной вёрсткой, что на данный момент является общепринятым стандартом и позволяет при минимальных усилиях и затратах придать сайту актуальный вид.
7. Контент и дизайн — независимы друг от друга. В любой момент можно изменить дизайн сайта, при этом всё наполнение (страницы, статьи,

товары и прочее) останется на своём месте. Очень важный момент при работе на долгосрочную перспективу.

8. Большой набор различных дополнений и расширений (плагинов). Благодаря плагинам расширяются возможности сайта.

9. Регулярные и бесплатные обновления системы. WordPress очень популярен, поэтому все сбои и ошибки устраняются максимально оперативно: как только пользователи обнаруживают проблему и сообщают о ней разработчикам.

10. Сообщество разработчиков. Дружное коммьюнити разработчиков — это огромная база знаний для программистов.

Также система WordPress имеет следующий ряд возможностей:

1. Шаблонный дизайн графического оформления страниц создает гибкость, простоту редактирования и дает возможность установить стандарт выполнения любых шаблонов для данной системы управления.

2. Создание чистого HTML кода при помощи графического редактора текста.

3. Возможность подключать плагины, с уникально простой системой их взаимодействия с основным кодом.

4. Возможность ограничения доступа к интерфейсу администратора по спискам разрешенных IP адресов.

5. Возможность редактирования непосредственно самого PHP кода.

6. Возможность создания современного динамического многофункционального сайта с ярким внешним видом на любую тему.

7. Поддержка медиа форматов (аудио, видео и изображения), возможность загрузки их на сайт и корректного отображения на его страницах [34].

И это лишь неполный перечень возможностей системы WordPress, а благодаря механизму поддержки дополнительных плагинов этот список практически ничем не ограничен.

2 РЕАЛИЗАЦИЯ САЙТА КОМПАНИИ И ЕГО БЕЗОПАСНОСТИ

2.1 Характеристика компании

Объектом исследования является компания ООО «УралТрейд», которая была создана коллективом единомышленников в 2016 году. За время своей деятельности исследуемая организация выросла в одну из крупнейших компаний по приему лома, а также по закупу и реализации железнодорожного лома Уральского региона.

С компанией ООО «УралТрейд» сотрудничают такие крупные холдинги, как группа компании «Новотранс» г. Москва, АО «СГ-транс» г. Москва, компания «Трансойл» г. Санкт-Петербург и др. Клиентами компании ООО «УралТрейд» являются: ПАО «Магнитогорский металлургический комбинат», Новолипецкий металлургический комбинат (НЛМК), ПАО «Северсталь» г. Череповец и др.

Общество с ограниченной ответственностью «УралТрейд», именуемое в дальнейшем «Общество», образовано 15 февраля 2016 года. Единственным учредителем ООО «УралТрейд» является директор Белик Станислав Леонидович. Общество создано в соответствии с законодательством РФ, и действует на основании Устава и законодательства Российской Федерации. Общество имеет расчётный счёт в банке, круглую печать со своим наименованием, эмблему, штампы, бланки и другие реквизиты. Предприятие имеет самостоятельный баланс.

Юридический адрес: 620026, Свердловская область, г. Екатеринбург, ул. Розы Люксембург 64, оф. 904. Телефон: 8 (343) 310-01-05; e-mail: info@uraltrd.ru [19].

Организационная структура представляет собой совокупность технических, вспомогательных и обслуживающих подразделений. Основной формой

организации труда является технические и обслуживающие отделы, состав и численность которых зависят от направления деятельности.

Цели и виды деятельности

Основными видами деятельности компании является «торговля оптовая металлами и металлическими рудами», «торговля оптовая отходами и ломом». Компания «УралТрейд» предоставляет полный спектр услуг:

- прием цветного лома;
- прием черного лома;
- закуп железнодорожного лома;
- реализация железнодорожного лома;
- разделка вагонов;
- демонтаж и вывоз металлоконструкций [21].

Главная миссия компании: «предлагать настолько качественный сервис, который помогает клиентам компании повышать эффективность своего бизнеса».

Цель компании — стать самой востребованной организацией, которой будет стремиться воспользоваться каждый потенциальный клиент: продать или купить металлолом, продать вагоны в разделку.

Стремление к новому для компании означает:

- постоянно искать, находить и использовать нестандартный подход к решению задач;
- постоянно искать, находить и использовать новые возможности;
- никогда не останавливаться на достигнутом.

Как стать клиентом компании

Для того, чтобы получить максимально возможную цену на металлолом и начать сотрудничать с компанией, клиенту необходимо всего лишь предоставить менеджерам информацию об остатках лома с указанием местонахождения, номенклатуры и его количества, а также свои контактные данные и реквизиты предприятия, отправив информацию на электронный адрес: info@uraltrd.ru или заполнив форму на сайте. В течение одного рабочего дня

менеджер отправит цену покупки и свяжется с клиентом для обсуждения условий, а также подписания договора и спецификации.

2.2 Выбор хостинга и возможность локальной разработки

Перед началом создания веб-сайта необходимо зарегистрировать доменное имя и найти хостинг, на котором будет размещен сам сайт. При выборе домена, нужно учитывать следующее моменты:

- использование правильной доменной зоны;
- не использовать длинное название;
- не использовать название близкое к конкурентам;
- выражение идеи веб-сайта, к которому он привязан.

После выбора доменного имени нужно выбрать надёжного регистратора, а также хостинг провайдера. Любой созданный сайт должен физически размещаться на специальных компьютерах (серверах), которые постоянно подключены к интернету. Компании, предоставляющие услуги по размещению сайтов на своих серверах называют хостинг провайдерами или коротко — хостингом [9].

Обычно в такие услуги включены различные преференции, такие как: предоставление места под почтовый сервер, возможность создания баз данных и их обслуживание, и многое другое. Именно в зависимости от различных предоставляемых условий выбирают хостинг. При выборе стоит найти оптимальный вариант между стоимостью и функциональностью. Многие хостинг провайдеры предоставляют услуги комплексно, предлагая купить хостинг с оплатой на год и получить домен в подарок. Управление хостингом осуществляется через веб-интерфейс. Существует множество систем управления, среди которых широко распространены: cPanel (рисунок 3), ISPmanager (рисунок 4), Plesk (рисунок 5) и другие.

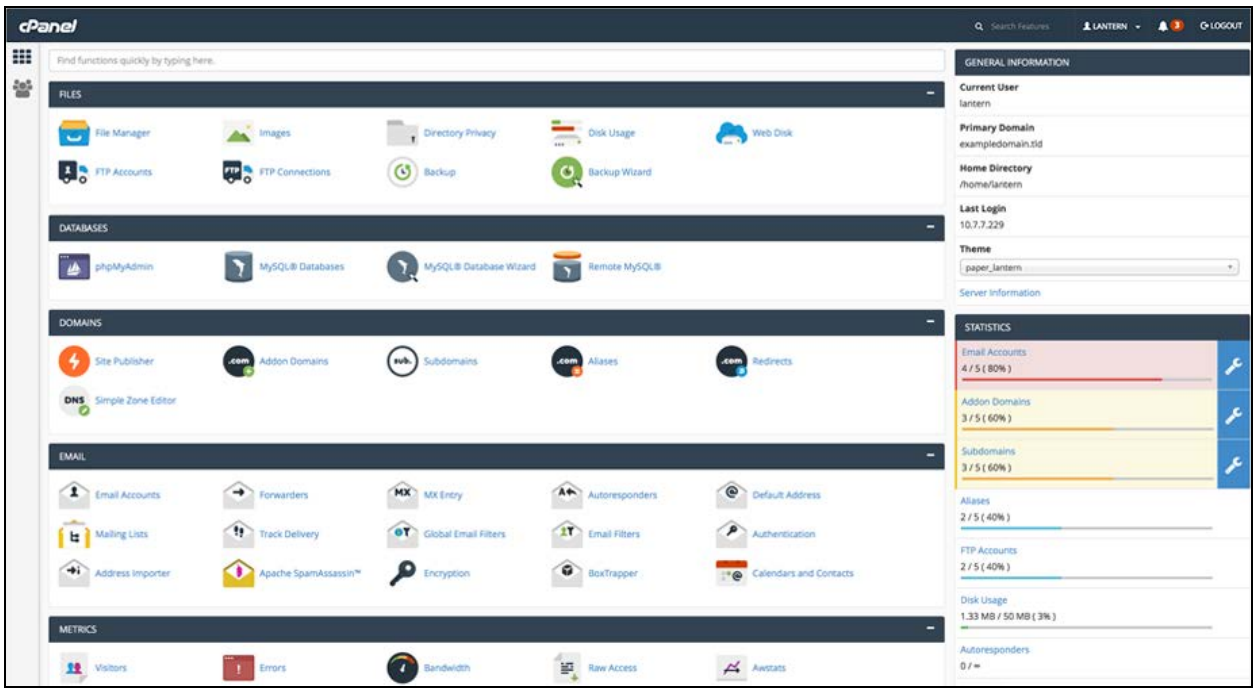

Рисунок 3 — Веб-интерфейс системы управления cPanel

Рекомендованные разработчиками системные требования:

1. PHP версии 7.2 или выше.
2. MySQL версии 5.6 или выше / MariaDB версии 10.0 или выше; поддержка HTTPS.

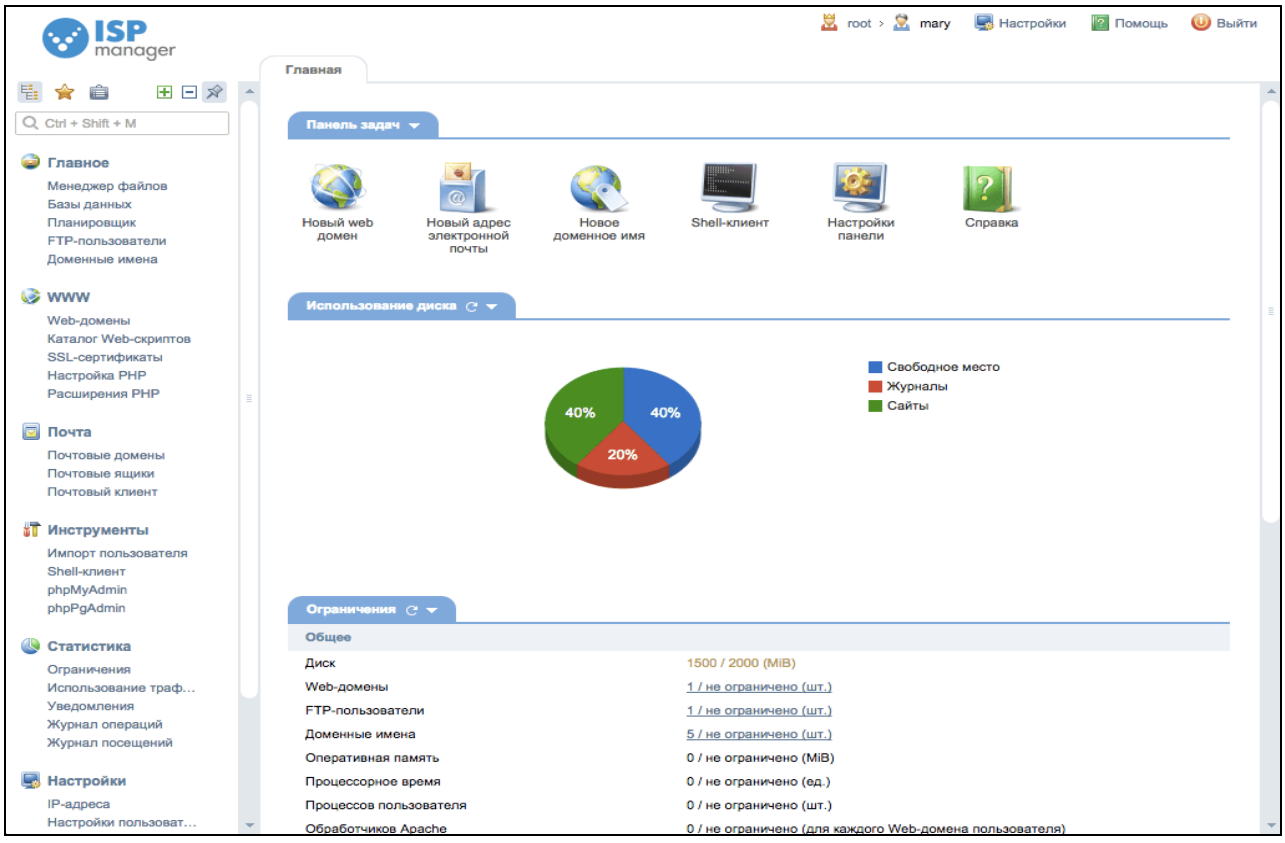

Рисунок 4 — Веб-интерфейс системы управления ISPmanager

Разработчики предупреждают, что если пользоваться устаревшим окружением, где доступны только старые версии PHP или MySQL, то WordPress также будет работать и с PHP 5.2.4+ и MySQL 5.0+, однако поддержка этих версий официально прекращена, и они могут подвергнуть сайт проблемам безопасности [20].

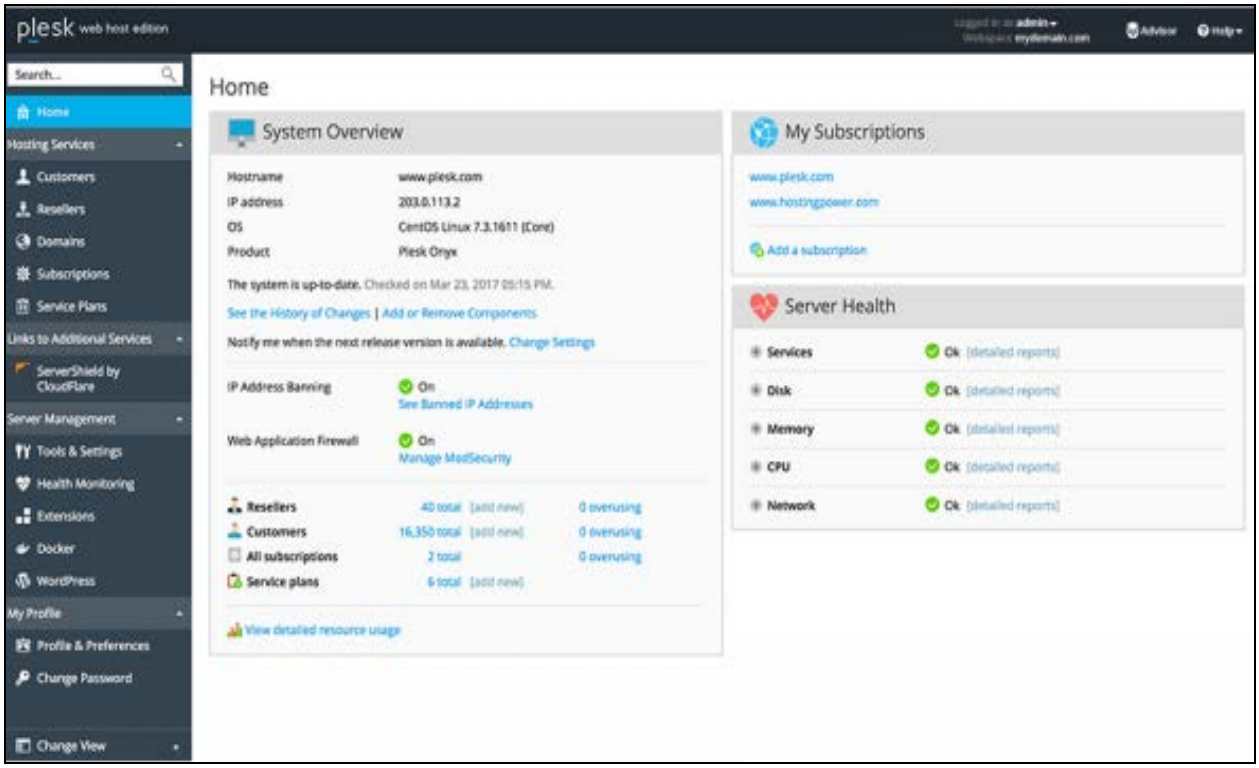

Рисунок 5 — Веб-интерфейс системы управления Plesk

Для повышения уровня безопасности необходимо запускать приложения PHP, такие как WordPress, от имени пользователя личной учетной записи, а не общей (например, www-data). Также следует уточнить у своего потенциального хостинг-провайдера, какие шаги предпринимаются для обеспечения безопасности клиентской учётной записи.

Необходимость покупать хостинг с доменом и размещать на нём сайт появится только после реализации и согласования конечной версии продукта с заказчиком.

Несмотря на то, что WordPress лучше всего работает на операционных системах Linux или UNIX, в процессе разработки сайта наиболее оптимальной работы WordPress можно достичь и в домашних условиях, используя дистрибутив XAMPP. XAMPP представляет собой кроссплатформенную

связку Apache, MariaDB, PHP и Perl и имеет небольшую систему управления (рисунок 6).

Загрузить актуальную версию дистрибутива возможно с официального ресурса [26].

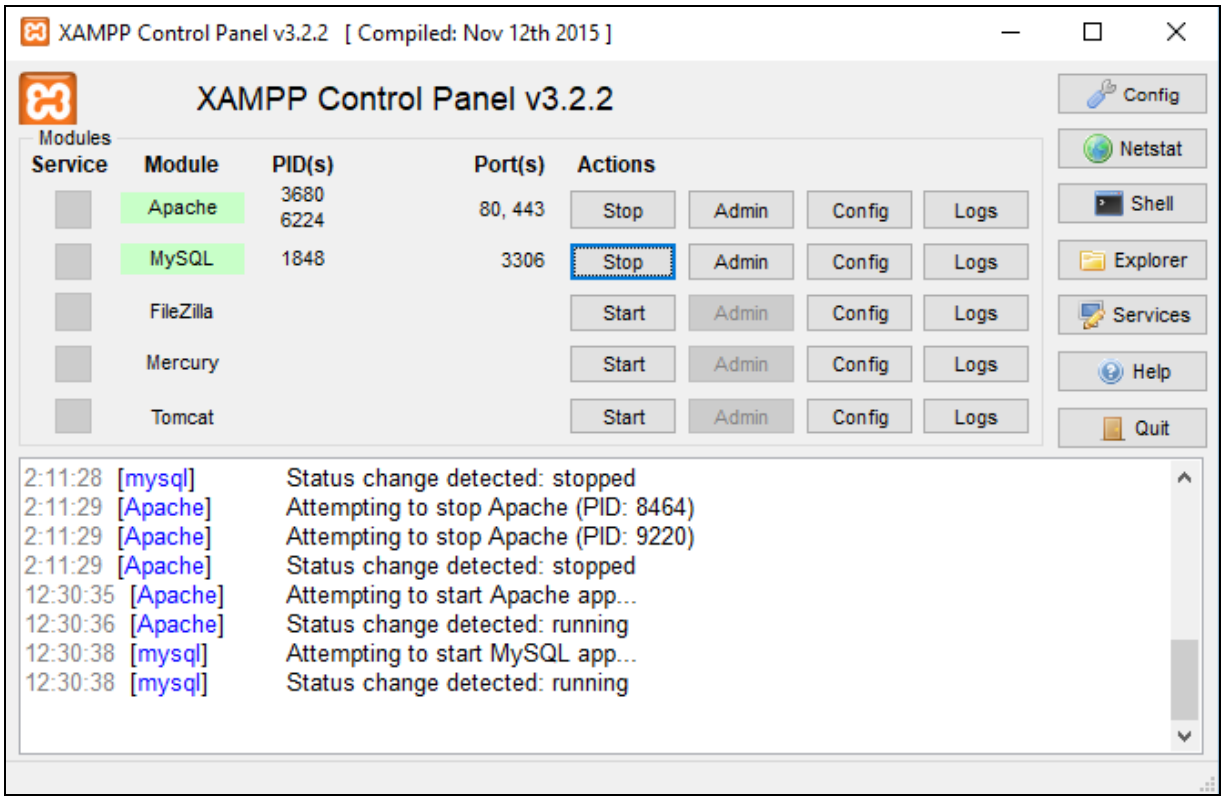

Рисунок 6 — Окно системы управления XAMPP для Windows

После установки дистрибутива XAMPP необходимо убедиться, что в настройках Apache активирован модуль mod_rewrite. Модуль выполняет функцию перезаписи URL-адресов на лету и за счёт этого в WordPress работают постоянные ссылки.

2.3 Загрузка и установка WordPress

Перед тем, как приступить к установке WordPress, необходимо загрузить актуальную версию CMS. Загрузка релиза может осуществляться с многочисленных ресурсов, но рекомендуется воспользоваться официальным ресурсом (рисунок 7). Если необходима русская версия, то её так же можно загрузить с официального ресурса [7].

Рисунок 7 — Сайт WordPress.org

Следует помнить, что загрузка программного обеспечения со сторонних ресурсов может нести риски заражения компьютера вирусами, а также иметь умышленно добавленные уязвимости для взлома сайта.

CMS WordPress переведена на множество языков, а это является отличным аргументом использования веб-разработчиками со всего мира. Новые релизы данной платформы выходят регулярно. При появлении более новой версии, система выводит информационное сообщение внутри административной панели о наличии обновлений, и предлагает обновить CMS в автоматическом режиме. Важно помнить, что нельзя забывать делать резервное копирование базы данных вашего сайта перед обновлением. Все посты, страницы и настройки хранятся в базе данных — по сути, это самый важный файл, с которого можно всё восстановить, если при обновлении возникнут проблемы.

В современных версиях CMS максимально упростили установку. Сейчас установка происходит в 4 этапа [25]:

- загрузка файлов на сервер;
- создание отдельной базы данных для CMS;
- запуск веб-интерфейса установки WordPress;
- установка прав доступа к директориям.

WordPress не является программой, которую необходимо устанавливать на компьютере. WordPress является системой управления сайтом, все файлы которой располагаются на самом сайте — туда его и надо будет установить.

Управление происходит в окне браузера. Загрузку файлов на сервер, возможно осуществить используя веб-интерфейс панели управления хостинг провайдера или же с помощью FTP-клиента.

При загрузке файлов CMS, необходимо учитывать, что файлы должны лежать в корневых директориях сайта, например, public_html, www или htdocs.

Именно эти директории являются корневыми для Apache и NGINX. После завершения загрузки файлов на сервер, создается база данных, которая будет использоваться выбранным CMS. Создание новой базы данных возможно через phpMyAdmin (рисунок 8) или при помощи веб-интерфейса панели управления хостинг провайдера.

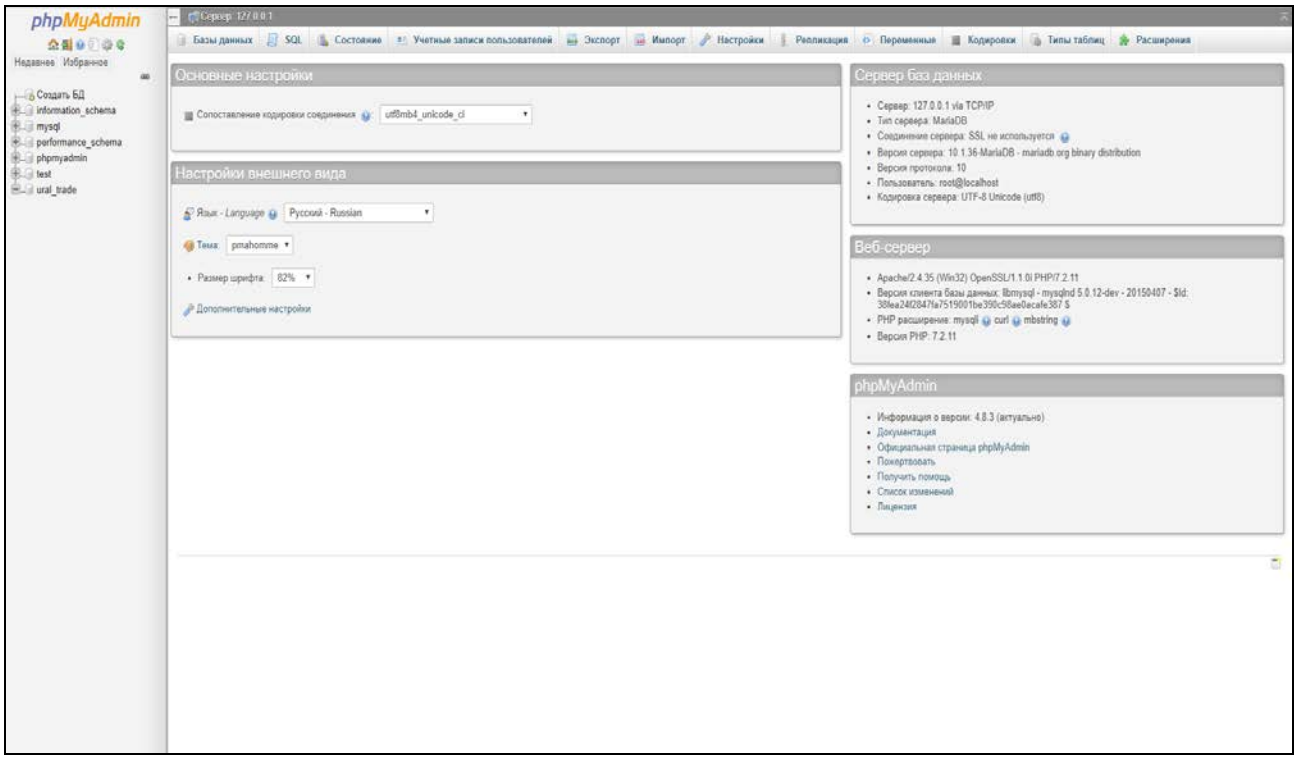

Рисунок 8 — Веб-интерфейс системы управления phpMyAdmin

Если использовать веб-интерфейс панели управления хостинг провайдера, то там требуется указать имя базы данных, а также имя пользователя и пароль для авторизации.

В случае если используется свой сервер, то создать базу данных можно в phpMyAdmin, но для этого необходимо заранее заготовить логин и пароль для авторизации в панели управления PMA.

После создания базы данных и авторизации необходимо перейти на главную страницу создаваемого сайта, чтобы начать автоматический запуск процесса установки (рисунок 9).

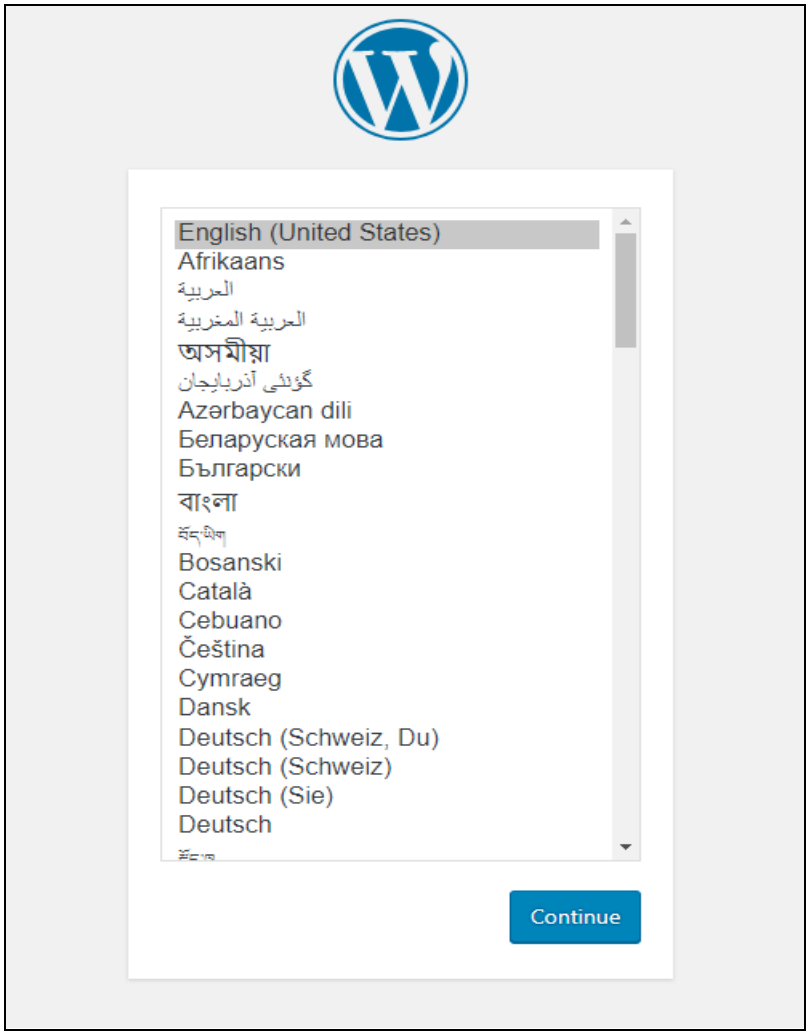

Рисунок 9 — Веб-интерфейс установочного скрипта WordPress

В некоторых случаях перед началом установки, приходится вручную изменять конфигурационный файл wp-config-sample.php. В данном файле описаны параметры, которые необходимы WordPress для успешной установки.

После внесения изменений, файл wp-config-sample.php нужно сохранить под именем wp-config.php.

В процессе установки понадобится указать имя базы данных, адрес сервера базы данных, имя пользователя и пароль для подключения к БД (рисунок 10).

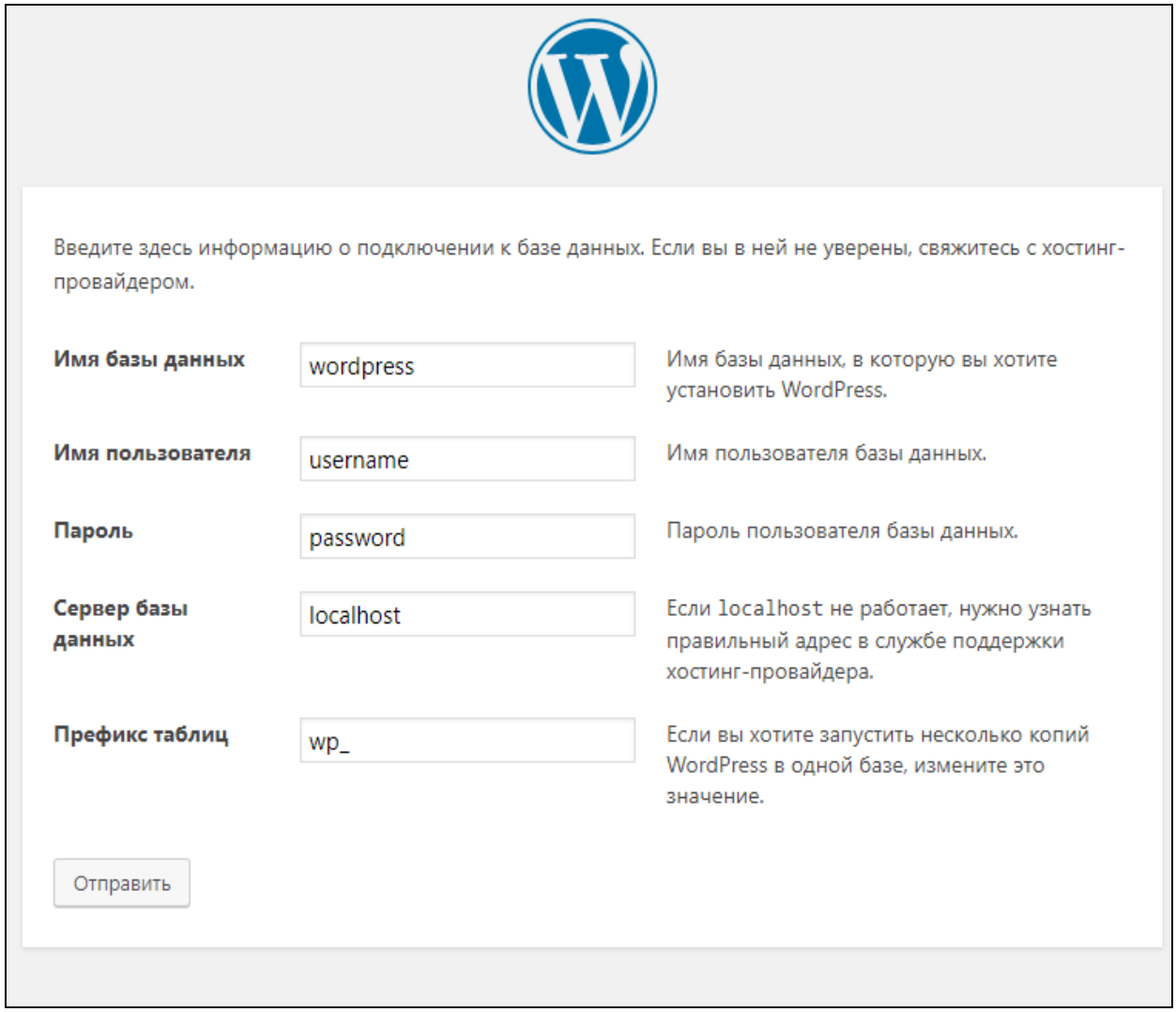

Рисунок 10 — Веб-интерфейс установочного скрипта WordPress

После откроется окно, где необходимо указать название создаваемого сайта адрес электронной почты и придумать себе имя пользователя и пароль (рисунок 11).

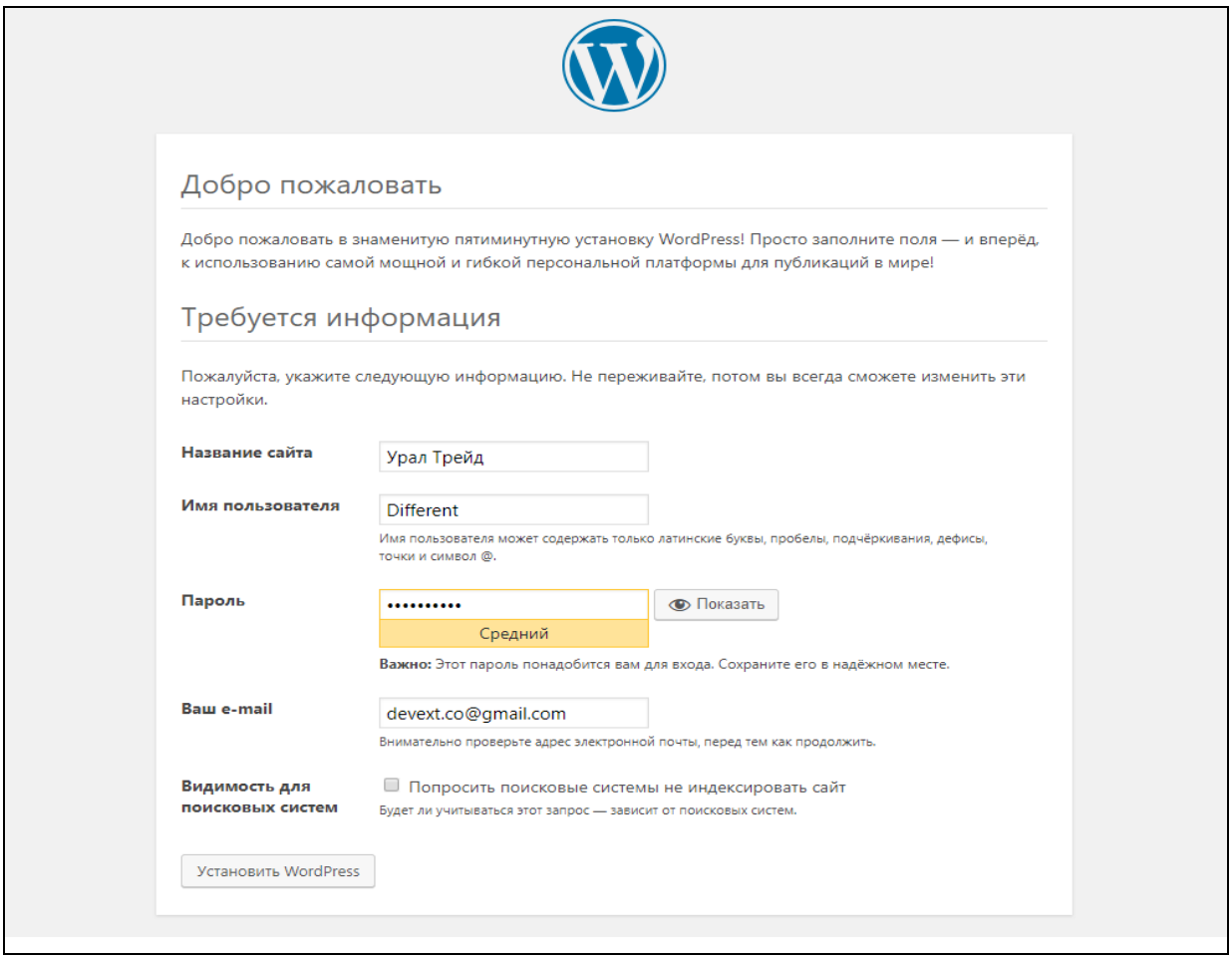

Рисунок 11 — Веб-интерфейс установочного скрипта WordPress

2.4 Структура и интерфейс сайта компании

Немаловажную часть в создании сайта играет структура и интерфейс. Важно, чтобы клиенту было просто и приятно работать с информацией, предоставленной на сайте. Безусловно, при поиске нужной информации на сайте можно не акцентировать внимание на мелкие недоделки или неудобства внешнего вида сайта. Но необходимо отметить, на пике развития интернет сайтов каждый пользователь, постоянно получавший информацию с сети, не обращал внимания на детали интерфейса: его удобство, навигацию и в целом внешнее оформление. В силу того, что сейчас современный человек ежедневно пользуется интернетом на работе или дома, то максимальное удобство сайта и быстрый поиск той или иной информации на интернет-ресурсе играет большую роль.

Интерфейс — это средство взаимодействия пользователя с программой, игрой или операционной системой самого устройства. Интерфейс позволяет узнавать любую программу или привычный текстовый редактор. Другими словами, этот термин означает совокупность различных средств, которые помогают человеку управлять работой компьютера [31].

Основной задачей интерфейса является управление информацией, и оттого, насколько удобен будет интерфейс, зависит, насколько быстро будет происходить обмен информацией.

Критерии, предъявляемые к интерфейсу сайтов:

1. Естественность (интуитивность). Работа с сайтом у пользователя не должна вызывать сложностей при поиске необходимой информации (элементов интерфейса) для управления процессом решения задачи.

2. Непротиворечивость. Если в процессе взаимодействия с сайтом пользователем были применены некоторые приёмы работы в системе, то в другой части ресурса эти приёмы должны быть подобны. Таким образом, интеграция с интерфейсом должна соответствовать привычным нормам (например, использование клавиши Esc).

3. Неизбыточность. Неизбыточность подразумевает уникальность информации, т.е. пользователю необходимо вводить минимальную информацию для работы с системой. Не нужно требовать от пользователя ввести информацию, которая была ранее введена или которая может быть логически получена.

4. Прямой доступ к системе помощи. При работе с сайтом, необходимо чтобы он предоставил пользователю понятную и простую систему помощи. Она должна отвечать следующим требованиям:

- качество обрабатываемых команд;
- характер информирования об ошибках;
- подтверждение выполняемых в данный момент сайтом команд.

5. Гибкость. Интерфейс сайта должен быть понятен людям с различными навыками обращения с персональным компьютером — как

любителям, так и профессионалам. Для неопытных пользователей система может представлять иерархическую структуру меню, а для опытных — управление при помощи комбинации клавиш.

6. Логичность. Запрос информации, касающейся одного логического блока, имеет смысл объединить и структурировать. К примеру, если необходимо ввести данные по нескольким клиентам, то необходимо запрашивать всю информацию вместе, и фамилию, и номер полиса.

7. Эргономика. Эргономика интерфейса сайта подразумевает минимизацию умственных и физических усилий пользователя ресурса. А именно — если есть возможность заменить ввод выбором, это необходимо реализовать [15].

Для того чтобы сделать интерфейс как можно дружественнее использованы следующие приемы:

- применение основных элементов управления;
- использование небольшого количества сочетаемых цветов;
- стандартизирование интерфейса.

На рисунке 12 предоставлена схема интерфейса сайта компании. Навигация является одним из важнейших элементов. Чем проще будет построена навигация, тем легче ориентироваться пользователю.

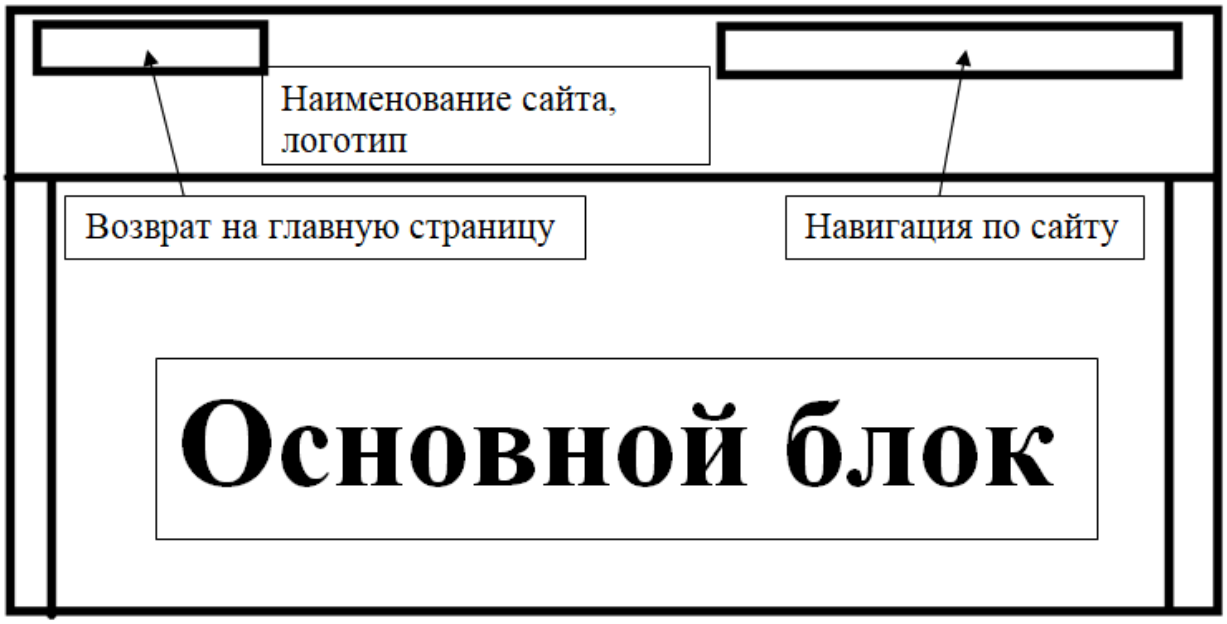

Рисунок 12 — Схема интерфейса сайта

Благодаря панели навигации (рисунок13) совершаются переходы по разделам. Панель навигации расположена в верхней правой части окна, на логотипе.

Рисунок 13 — Панель навигации

Панель навигации содержит несколько элементов:

- «Главная», с помощью которой осуществляется переход на главную страницу;
- вкладка «О нас»;
- вкладка «Услуги»;
- вкладка «Карьера»;
- вкладка «Документы»;
- вкладка «Контакты».

Элемент «Услуги» реализован выпадающим списком (рисунок 14), с помощью которого возможно перейти на одну из необходимых страниц.

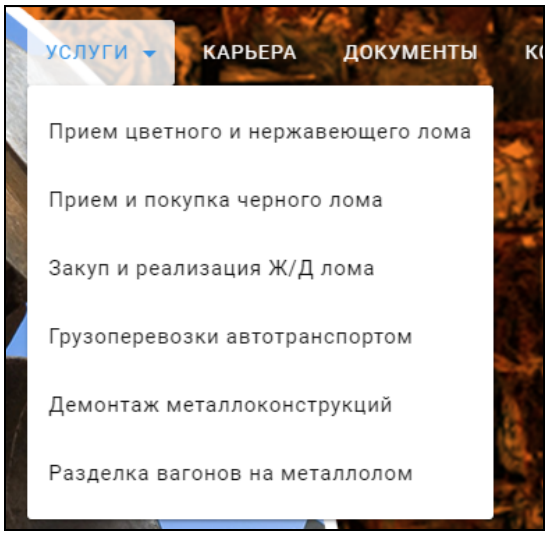

Рисунок 14 — Выпадающий список

Цветовое решение

Правильно подобранное цветовое решение играет далеко не последнюю роль при создании сайта. Цвет — мощный визуализатор, способный и улучшить интерфейс, и полностью уничтожить интерес пользователя, так

как влияет на настроение и самочувствие человека. Большую роль в создании сайта играет восприятие человеком цвета. Цвета также могут показать назначение сайта или программного продукта, их цели.

При выборе цветов для сайта были учтены следующие требования:

- цветовое разнообразие не должно быть большим, чтобы не рассеивать внимание клиента;
- текст должен быть тёмным, расположенным на светлом контрастном фоне, так как светлый текст на темном фоне быстро утомляет;
- цвета, использованные на сайте, не должны быть слишком яркими или слишком светлыми.

Описание разделов сайта

Структура сайта компании «УралТрейд» разработана по принципу Landing page (Целевая страница), которая представляет собой веб-страницу, главной задачей которой является конвертация посетителя в покупателя или клиента компании, побуждение к целевому действию [28]. Переход по ссылкам в шапке сайта переводит фокус на нужный раздел. Сайт является кроссплатформенным, открывается и работает в любом браузере. Сайт компании делится на шесть блоков, один из которых — на шесть страниц (рисунок 15): главная страница; о нас; услуги; карьера; документы; контакты.

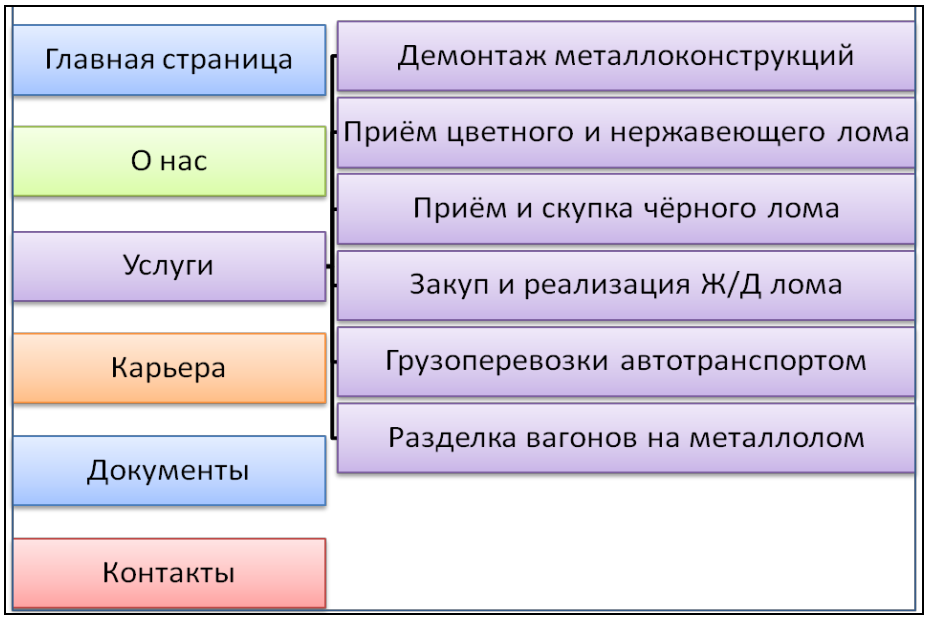

Рисунок 15 — Разработанная структура главной страницы сайта

Работа с сайтом начинается с его открытия по ссылке при поиске в поисковых системах или введения адреса сайта в адресную строку. При запуске открывается главная страница. Данная страница делится на три раздела (рисунок 16).

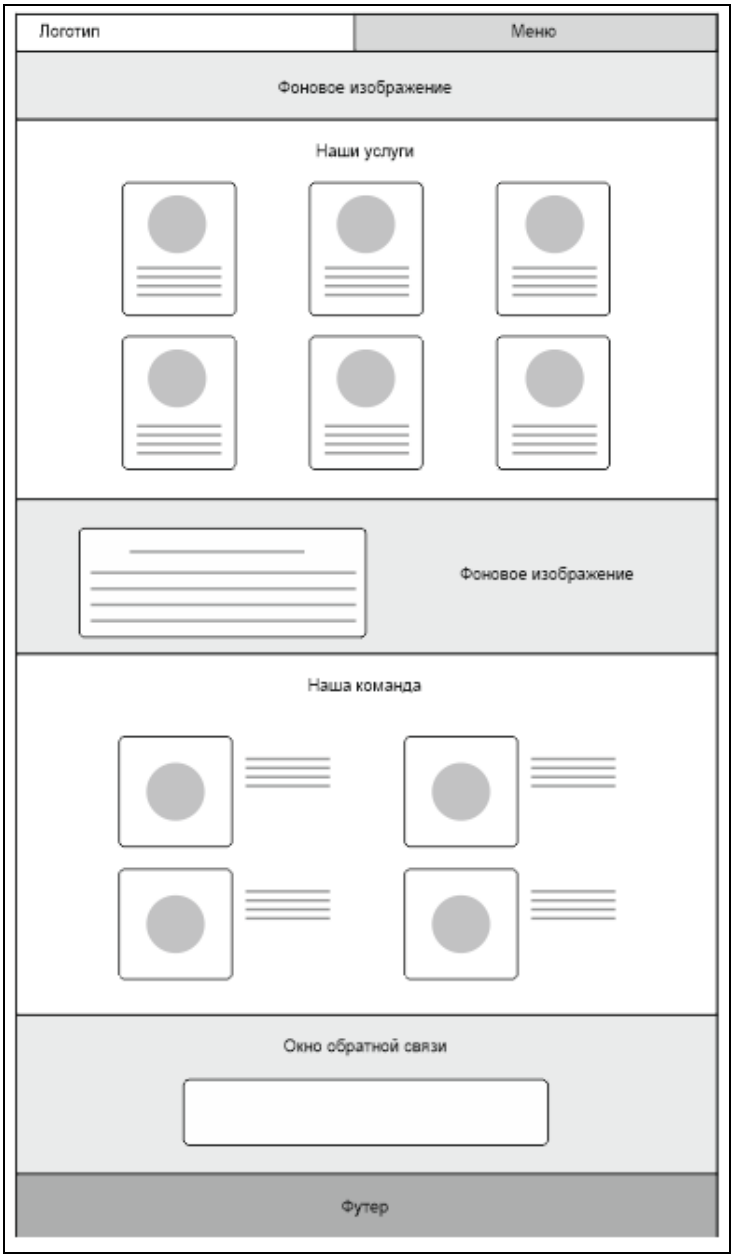

Рисунок 16 — Разработанная структура главной страницы сайта

Главная страница с логотипом и разделом «услуги» (рисунок 17). В данном разделе кратко описаны предоставляемые услуги компании и виды её деятельности. Чтобы пользователю было удобнее искать необходимую информацию, услуги разбиты на блоки с кратким описанием и ссылками для перехода на страницу, содержащую полный текст.

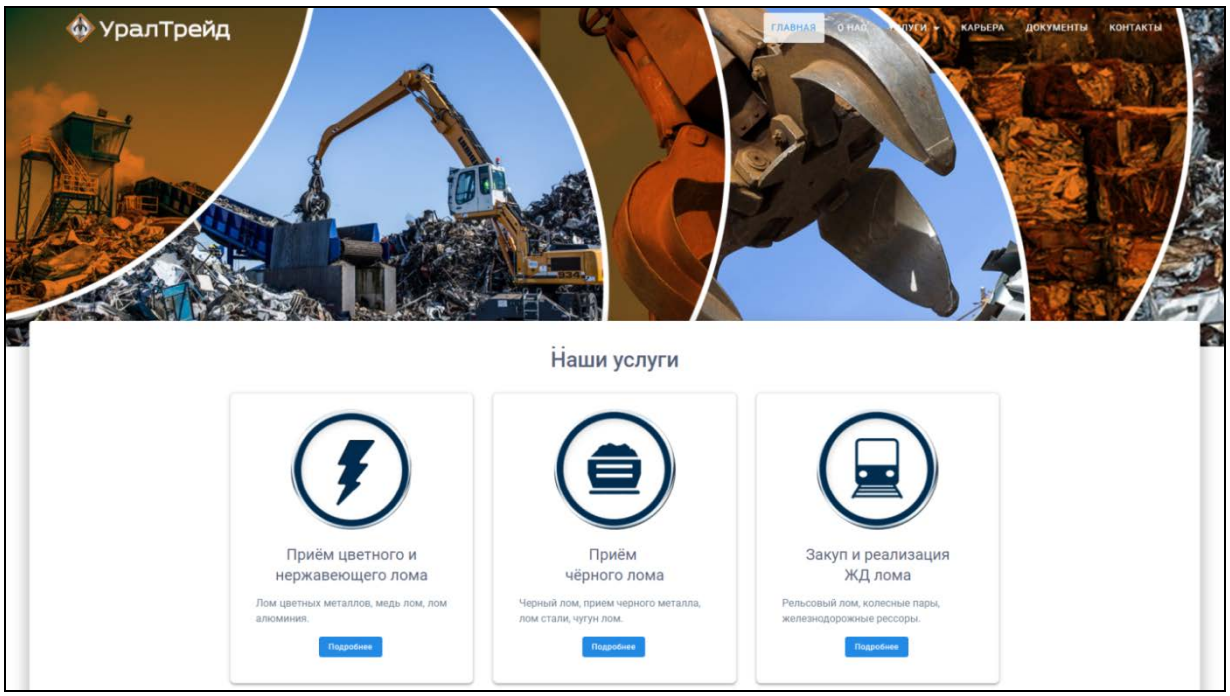

Рисунок 17 — Главная страница и раздел услуги

Главная страница с описанием достоинств и разделом сотрудников (рисунок 18). Этот раздел содержит краткое описание преимуществ компании, а также информацию о некоторых специалистах компании: их фотографии, контактные данные.

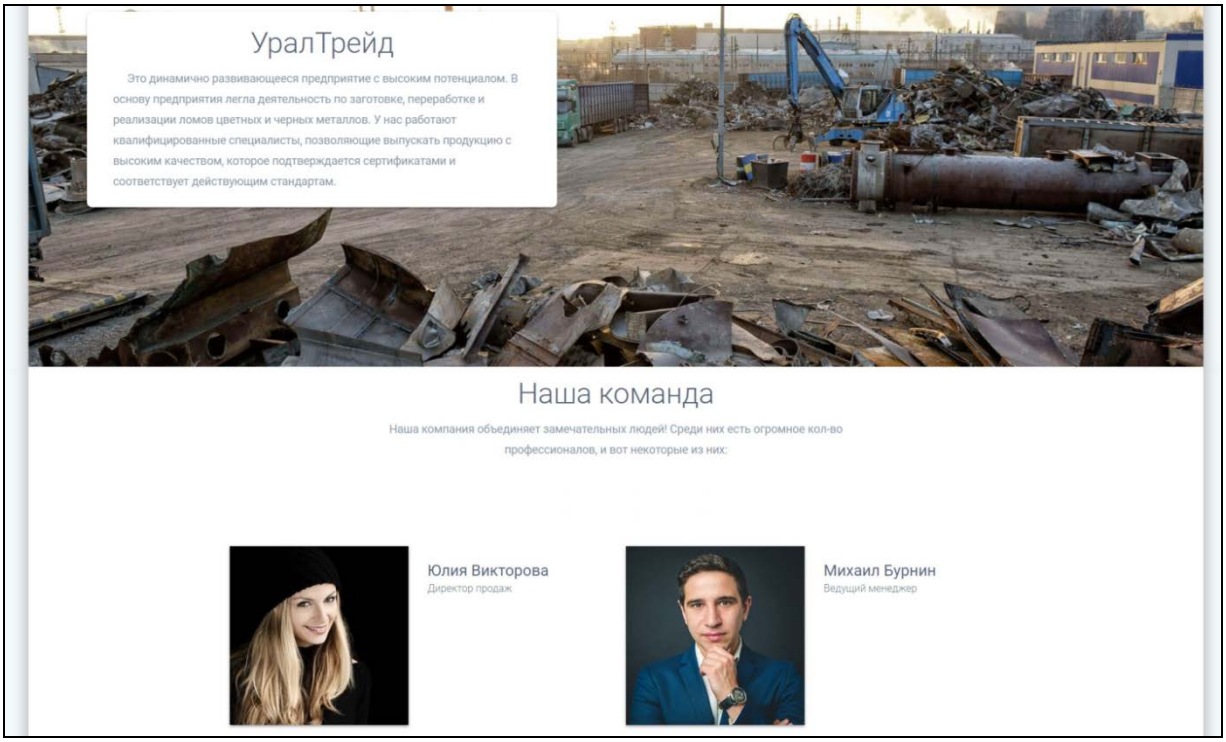

Рисунок 18 — Главная страница и раздел «Сотрудники»

Главная страница с разделом обратной связи и контактами (рисунок 19). В данных разделах содержится правовая информация, нормативные документы, фактические адреса местонахождения, а также удобная форма для обратной связи, с помощью которой пользователи могут уточнить интересующую их информацию, задать интересующие их вопросы или оставить заказ.

В контактной информации указан номер телефона для связи с менеджерами, адрес электронной почты, а также юридический адрес компании и ссылки на группы в социальных сетях.

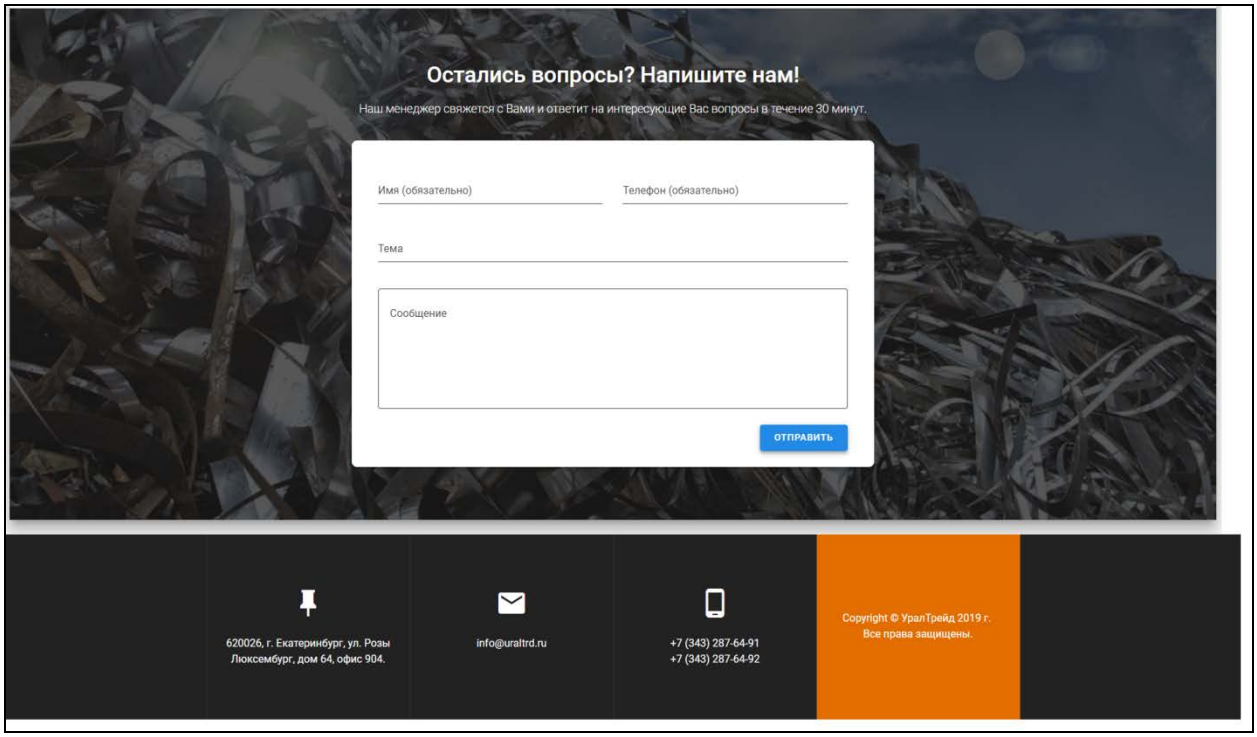

Рисунок 19 — Главная страница с обратной связью и контактами

Блок «О нас» (рисунок 20) содержит информацию о компании: её историю, миссию и цели, а также сведения о партнёрах компании. Информация описана сжато и имеет только главные сведения, чтобы не перегружать пользователя. Для удобства информация о партнёрах была предоставлена с помощью их логотипов.

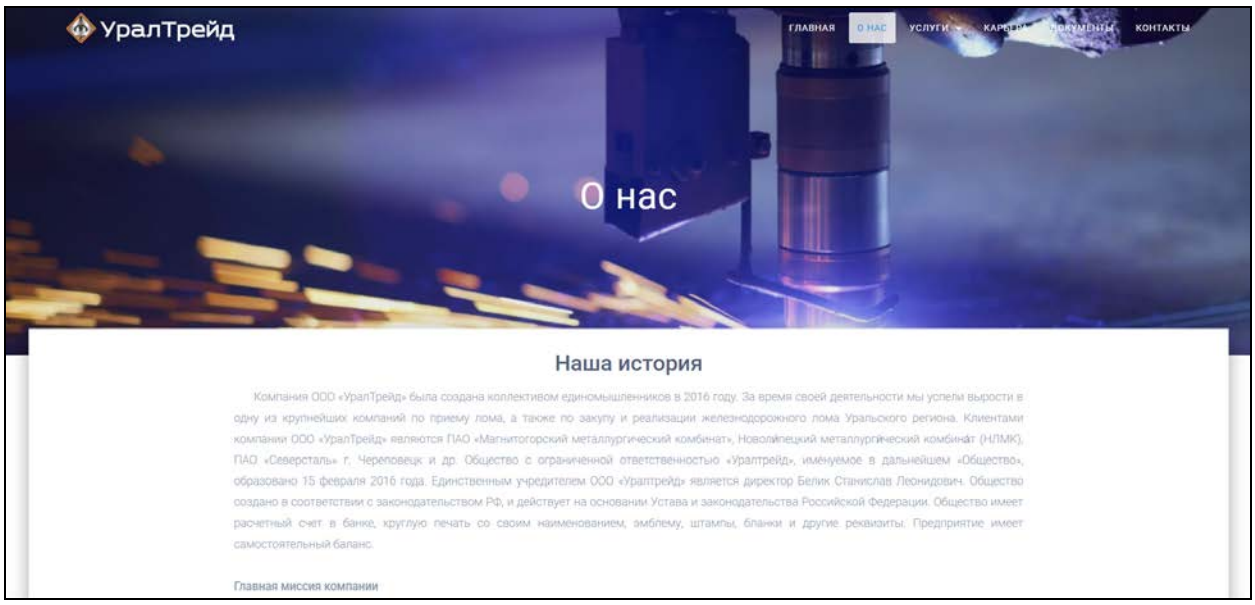

Рисунок 20 — Главная страница с обратной связью и контактами

Блок «Услуги» делится на несколько разделов:

- прием цветного и нержавеющего лома;
- прием и покупка черного лома;
- закуп и реализация Ж/Д лома;
- грузоперевозки автотранспортом;
- демонтаж металлоконструкций;
- разделка вагонов на металлолом.

Для удобства ссылки на данные страницы были помещены в выпадающее меню (рисунок 21).

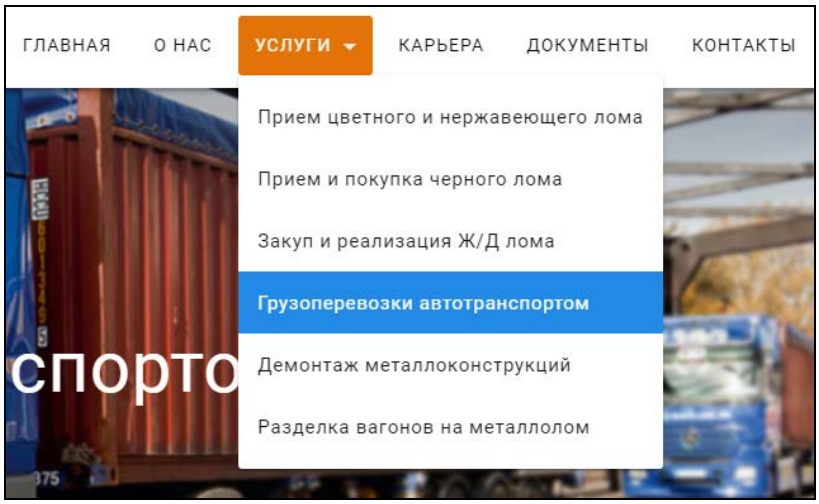

Рисунок 21 — Выпадающее меню для блока «Услуги»

Каждая страница заполнена информацией по теме в доступной для пользователя форме. Указаны преимущества необходимой услуги перед компаниями-конкурентами, описанные в понятной и доступной форме. Расписаны цены, разделённые на блоки, в которых указаны название, форма и стоимость лома. Так же этапы работы клиента с компанией. Каждый этап имеет пояснение (рисунок 22).

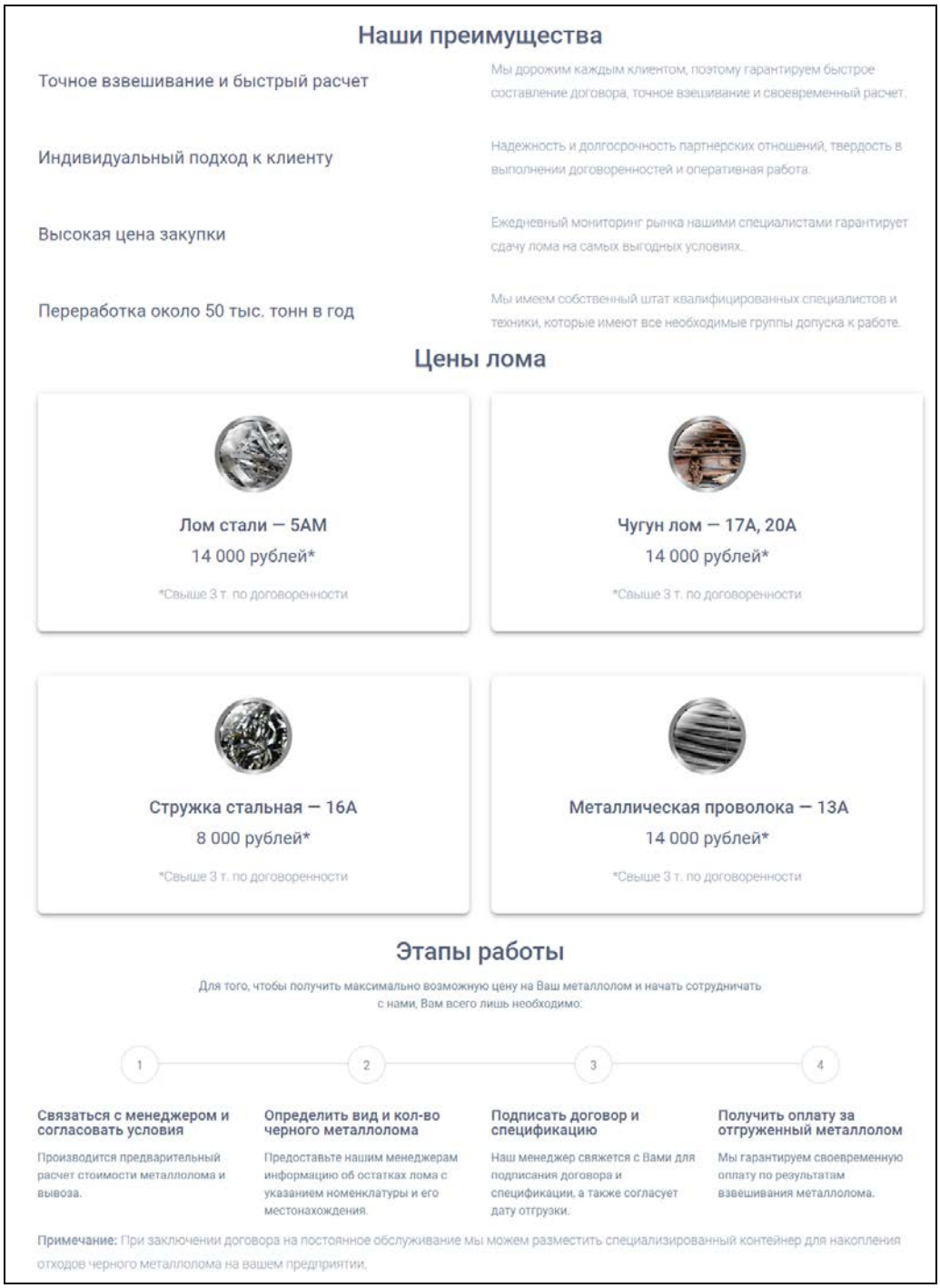

Рисунок 22 — Страница из блока «Услуги»

Блок «Документы» (рисунок 23) содержит информацию по основным учредительным документам, а также лицензию компании. При нажатии на кнопку «Скачать» выбранный файл открывается в новой вкладке, где можно с ним ознакомиться и, при необходимости, скачать в формате PDF.

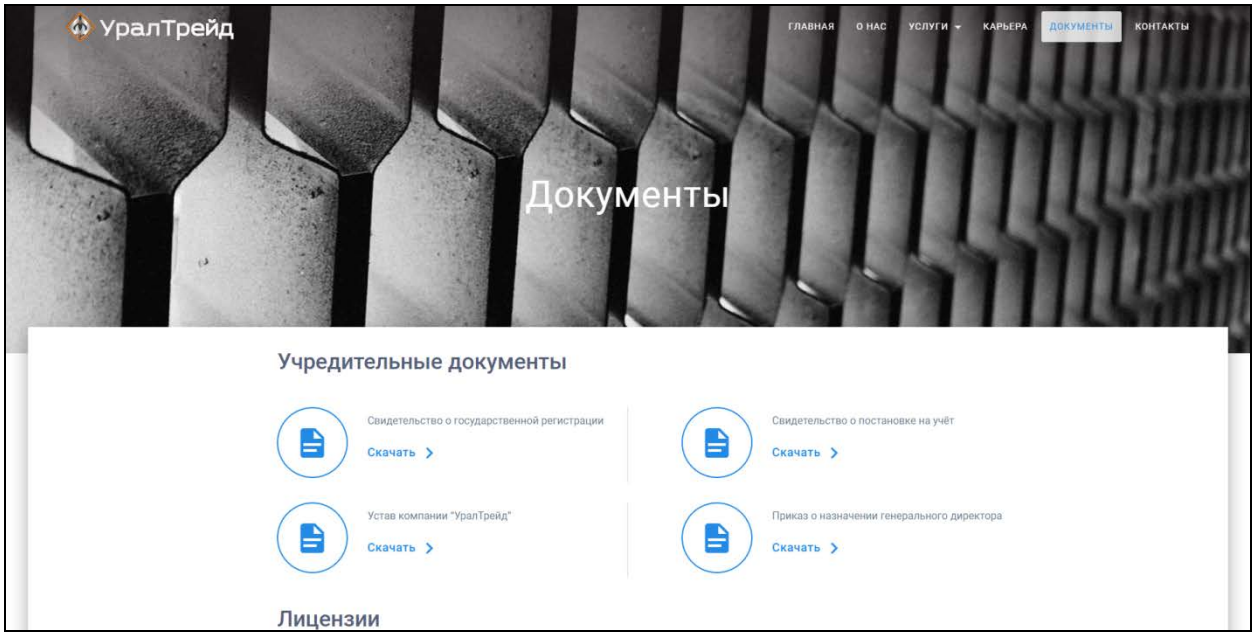

Рисунок 23 — Блок «Документы»

Блок «Контакты» (рисунок 24) содержит контактную информацию компании, номера телефонов, а также электронные и почтовые адреса.

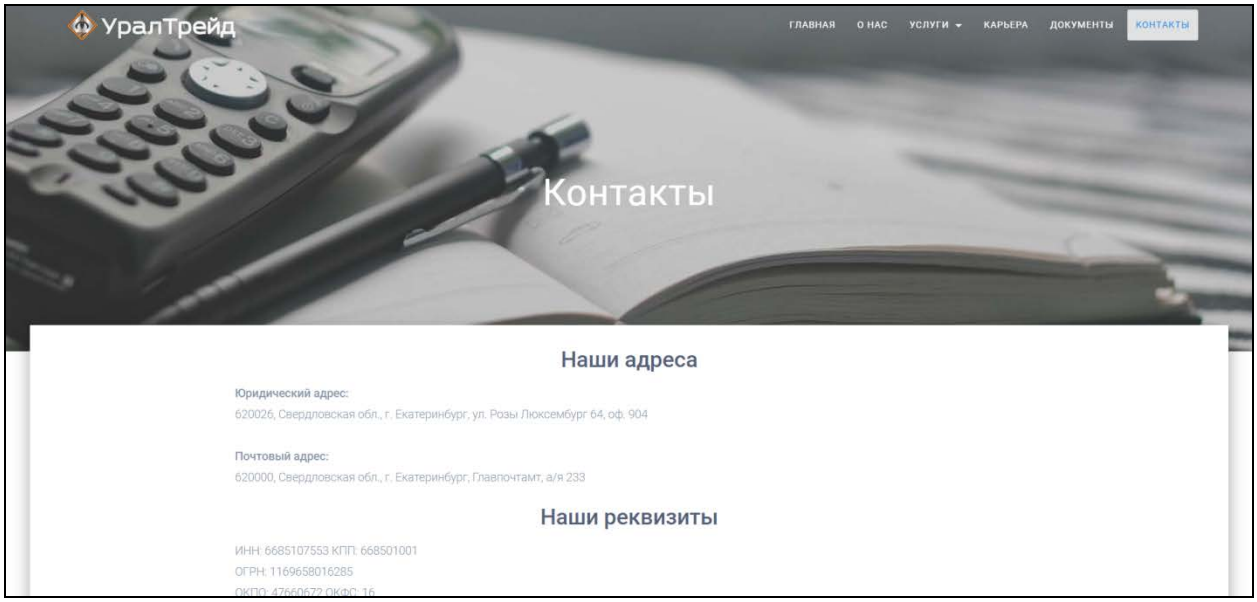

Рисунок 24 — Блок «Контакты»

Блок «Карьера» (рисунок 25) необходим для набора новых кадров, если в том будет потребность. На данной странице описаны преимущества работы

в компании, а также вакансии, на которые требуются специалисты с описанием требований, обязанностей, заработной платы, условий работы.

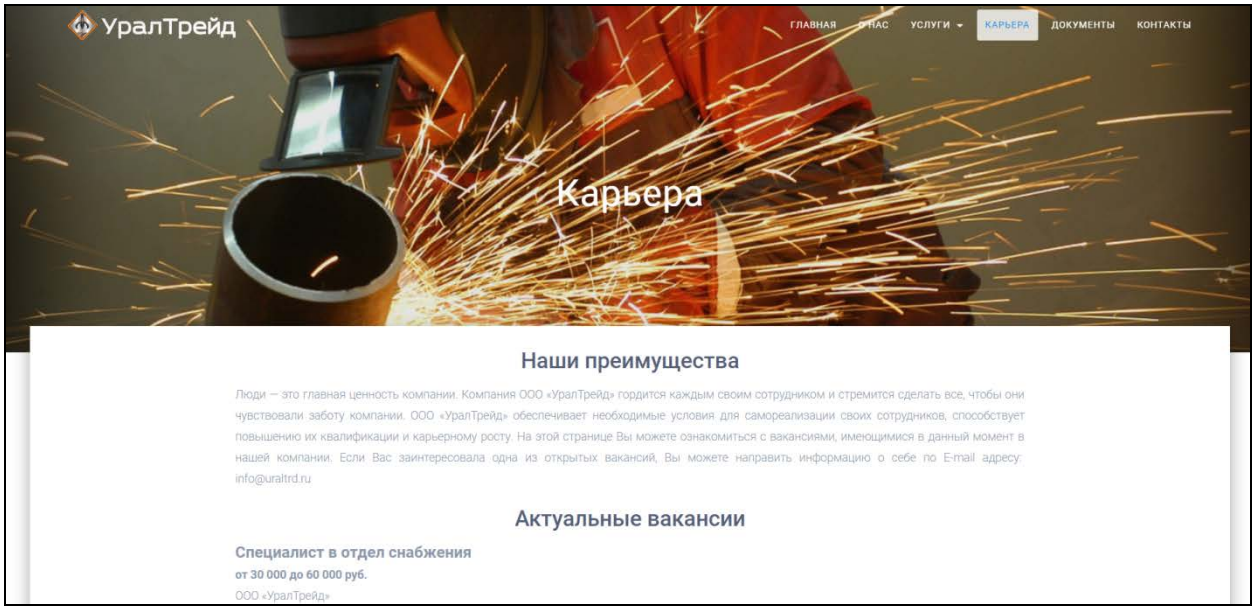

Рисунок 25 — Блок «Карьера»

2.5 Обеспечение безопасности сайта компании

2.5.1 Защита сайта средствами системы управления контентом

Для защиты средствами системы управления контентом (CMS) были установлены плагины All in One Security и WP Super Cache. All in One Security — это известный плагин для защиты от взлома WordPress. Функции плагина:

1. Защита аккаунтов:

- определяет аккаунт «admin» и предлагает поменять его на другой;
- определяет и сообщает об аккаунтах, в которых логин и имя пользователя совпадают — такие аккаунты взломать легче;
- генерирует сильные пароли.

2. Защита входа в систему и регистраций на сайте:

- опция Login Lockdown — блокирует пользователей за определенное количество неверных попыток входа в систему;
- завершает сессию в принудительном порядке для всех пользователей спустя установленное время бездействия;
- отслеживает активность в аккаунтах всех пользователей путем логирования информации;
- предоставляет отчёт о полном списке пользователей, которые выполнили вход в систему на данный момент;
- позволяет установить captcha в различные формы;
- позволяет вручную подтверждать все регистрации на сайте.

3. Защита базы данных:

- позволяет изменить WP-префикс базы данных на любой другой;
- предоставляет возможность использовать автоматическое резервное копирование.

4. Защита файловой системы:

- определяет папки и файлы с небезопасными правами доступа и сообщает об этом администратору;
- запрещает редактировать файлы с PHP-кодом из администраторской панели управления;
- позволяет запретить доступ к определенным файлам, с помощью которых злоумышленники могут выяснить версию WordPress.

5. Функция файервола позволяет использовать защиту с помощью .htaccess файла. Этот файл обрабатывается веб-сервером ещё до обработки любого кода сайта, поэтому правила .htaccess останавливают вредоносные скрипты ещё до того, как у них появится возможность достичь цели.

6. Предотвращение брутфорс-атак.

7. Сканирование безопасности:

- отслеживание файловых изменений и уведомление администратора об этом;

- сканирование таблиц базы данных на подозрительные строки — javascript и html код в базовых таблицах WordPress [37].

Плагин WP Super cache позволяет кэшировать страницы — то есть ускорять их загрузку. За счёт кеширования появляются и другие преимущества: при каждом запросе страницы, CMS не будет обращаться к базе данных и загружать данные из базы, а будет выводить заранее заготовленную копию страницы. Так как содержимое статичных страниц не меняется часто, то за счёт этого плагина можно добиться снижения нагрузки на CPU хостинг-аккаунта, что в разы увеличит время отклика сайта на действия пользователя, а также снизит риск вывода сайта из строя при большом количестве посетителей или запросов.

2.5.2 Защита сайта средствами MySQL

База данных является важнейшим элементом сайта, ведь именно туда сохраняется контент всех страниц, настройки самой CMS и установленных плагинов, а также пользователи, комментарии и отладочная информация. Страшно представить, какие финансовые и репутационные издержки может понести компания, а самое главное — утечку конфиденциальной информации, что может привести к очень серьёзным последствиям.

При работе с базами данных MySQL необходимо следовать приведенным ниже инструкциям:

1. Не предоставлять никому (за исключением пользователя MySQL под именем root) доступа к таблице user в базе данных MySQL.

2. Изучить систему прав доступа MySQL. Для управления доступом к MySQL служат команды GRANT и REVOKE. Нельзя предоставлять полные права всем пользователям.

3. Не следует хранить в базе данных незашифрованных паролей. Если злоумышленнику удастся получить доступ к базе данных или компьютеру

администратора, то в его руках окажется полный список паролей, которыми он может воспользоваться;

4. Нельзя использовать в качестве пароля слова из словарей. Для взлома такого рода паролей имеются специальные программы.

5. Запретить удалённое подключение к серверу MySQL и предоставлять такую возможность только определенным IP адресам.

6. Не доверять никаким данным, которые вводят пользователи. Возможны попытки перехитрить CMS путем ввода последовательностей специальных или экранированных символов в веб-формы или URL-адреса.

В настоящее время в любой организации действует разграничение доступа к информации на основе определённых знаний о пользователе. Такими знаниями могут служить роль пользователя в организации, его должность либо структурное подразделение, в котором работает пользователь. Многим известно, что проблема ограничения доступа может быть решена с помощью простейших механизмов на основе имени пользователя, таблиц, представлений и триггеров.

Для обеспечения безопасности при работе сайта с базой данных было принято решение создать специального пользователя со сложным паролем, имеющего ограниченный набор прав для доступа к базе данных. Это поможет предотвратить преднамеренный вред для базы данных при взломе.

На выбранном компанией хостинге, используется панель управления ISPManager, которая является удобным средством администрирования базы данных. Чтобы перейти к администрированию баз данных и их пользователей, необходимо открыть раздел базы данных (рисунок 26), для этого требуется авторизоваться в панели управления хостингом ISPManager.

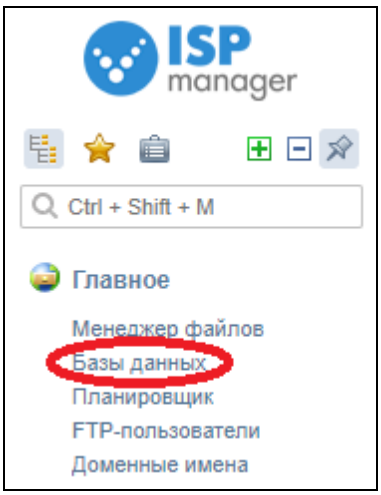

Рисунок 26 — Переход к администрированию баз данных

Для перехода к разделу пользователей базы данных необходимо отметить нужную базу данных и нажать кнопку пользователи в панели управления хостингом (рисунок 27).

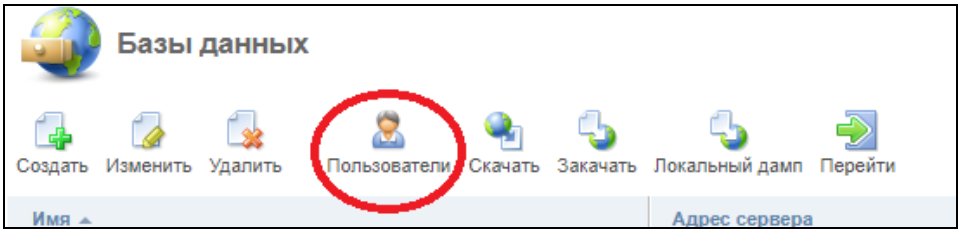

Рисунок 27— Переход в раздел пользователей базы данных

Для создания пользователя базы данных необходимо нажать кнопку добавить (рисунок 28).

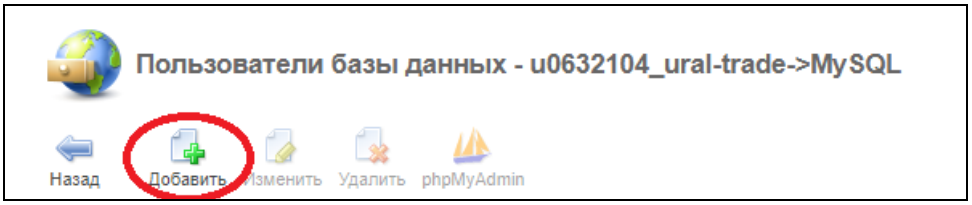

Рисунок 28— Переход к созданию пользователя

При создании пользователя базы данных нужно учитывать необходимые права доступа и никогда не предоставлять пользователю полный доступ. Чтобы понимать, какие привилегии будут необходимы, рассмотрим их значение более подробно:

- SELECT — позволяет делать выборки из таблиц;
- INSERT — позволяет записывать данные в таблицы;

- UPDATE — позволяет обновлять данные в таблицах;
- DELETE — позволяет удалять данные из таблицы;
- CREATE — позволяет создавать таблицы или базы данных;
- DROP — позволяет удалять таблицы;
- ALTER — позволяет изменять структуру таблиц;
- INDEX — позволяет создавать индексы для таблиц;
- TRIGGER — позволяет создавать триггеры;
- CREATE VIEW — позволяет создать некоторое представление в виде таблицы, которая фактически не существует как единая и содержит лишь данные других таблиц;
- SHOW VIEW — позволяет проверить каким запросом (из каких данных состоит) создано определенное представление, заданное с помощью CREATE VIEW;
- ALTER ROUTINE — позволяет изменить процедуру, созданную посредством CREATE ROUTINE;
- CREATE ROUTINE — позволяет создать процедуру, которая является заготовленным набором SQL-команд;
- GRANT —позволяет изменять права пользователей;
- REFERENCES — позволяет создавать связь между таблицами по внешнему ключу;
- LOCK TABLES — блокирует таблицу на время искусственного внесения в нее изменений (администрирование), чтобы данные внутри нее не могли измениться своим естественным путем (во время рабочего процесса).

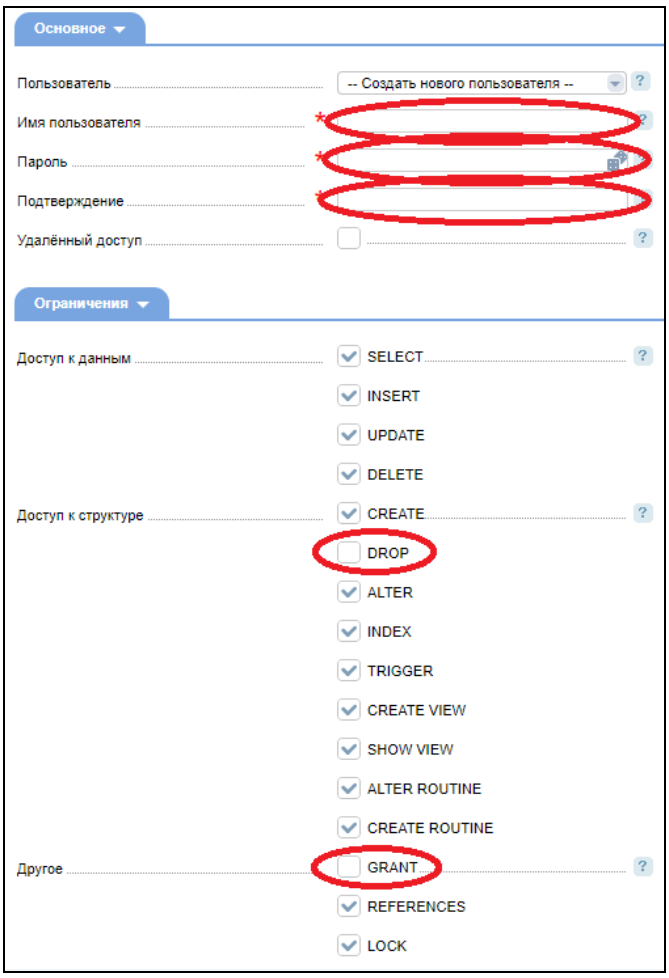

Рисунок 29 — Создание и настройка прав пользователя

Не рекомендуется позволять пользователям управлять чужими привилегиями и удалять таблицы, поэтому вводим имя пользователя и пароль, а также ограничим привилегии создаваемого аккаунта и сохраним изменения (рисунок 29). Включать удаленный доступ не рекомендуется, так как это увеличивает риск подбора пароля.

2.5.3 Защита сайта средствами файловой системы

Одним из ключевых моментов в безопасности сайта является файловая система, ведь именно в ней хранятся файлы конфигурации для подключения к базе данных. Очень важно правильно установить права доступа WordPress, чтобы защитить сайт от взлома и при этом не нарушить его работоспособность.

Если установить недостаточные права доступа, то операционная система не сможет выполнить какой-то скрипт или загрузить нужные файлы, что может привести к сбоям в работе сайта.

Может возникнуть и обратная ситуация, когда дано слишком много прав для посторонних пользователей, и злоумышленник может воспользоваться этим, например, дописав вредоносный код в конфигурационные файлы сайта.

Как правило, сайты размещаются на хостингах, работающих под Unix-подобными операционными системами (Linux, например). Эти операционные системы отличаются от привычной рядовому пользователю Windows, в частности тем, что позволяют гибко задавать различные права доступа для разных пользователей.

CHMOD (change file mode) — это программа для изменения прав доступа к файлам и каталогам в операционных системах типа Unix. Каждому файлу задаются атрибуты, показывающие, что и кому разрешено делать с этим файлом (например, владельцу читать и редактировать, а посторонним лицам только читать).

Существует несколько способов записи прав доступа — это буквенная и цифровая записи (рисунок 30).

Цифровая запись	Буквенная запись	Права
«0»	---	Ничего не разрешено
1	--x	Исполнение
2	-w-	Запись
3	-wx	Запись и исполнение
4	r--	Чтение
5	r-x	Чтение и исполнение
6	rw-	Чтение и запись
7	rwx	Чтение, запись и исполнение

Рисунок 30— Таблица соответствий прав доступа

Обычно права доступа записываются в виде трех цифр, каждая из которых относится к определенному виду пользователей:

- владелец файла;
- другие пользователи, входящие в группу владельца;
- остальные пользователи.

Для каждого из этих видов пользователей существует три права:

- чтение (4);
- запись (2);
- исполнение (1).

Права можно записать и другим способом — латинскими буквами:

- чтение (r);
- запись (w);
- исполнение (x);
- отсутствие прав(-).

Права для различных категорий пользователей, как в цифровом, так и в буквенном представлении, записываются последовательно (рисунок 31):

- если используется цифровая запись, первая цифра определяет права владельца, вторая права группы, третья — права всех остальных пользователей;
- при буквенной записи первые три символа определяют права владельца, вторые три определяют права группы, третьи три — права всех остальных пользователей.

Цифровая	Буквенная	Владелец	Группа	Все остальные
755	rwxr-xr-x	полный доступ	чтение и исполнение	чтение и исполнение
644	rw-r--r--	запись и чтение	только чтение	только чтение
555	r-xr-xr-x	чтение и исполнение	чтение и исполнение	чтение и исполнение

Рисунок 31— Примеры прав доступа в цифровой и буквенной записи

На выбранном компанией хостинге используется панель управления ISPManager, которая является весьма удобным средством администрирования файловой системы аккаунта.

Чтобы перейти к настройке файловой системы, необходимо открыть менеджер файлов (рисунок 32), для этого требуется авторизоваться в панели управления хостингом ISPManager.

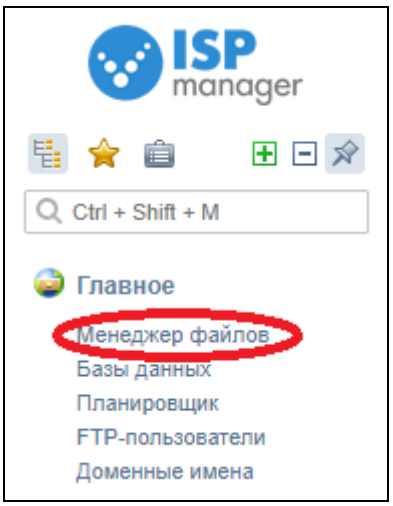

Рисунок 32— Открытие менеджера файлов

Файлы сайта, как правило, располагаются в директории /www/адрес_сайта/ (рисунок 33).

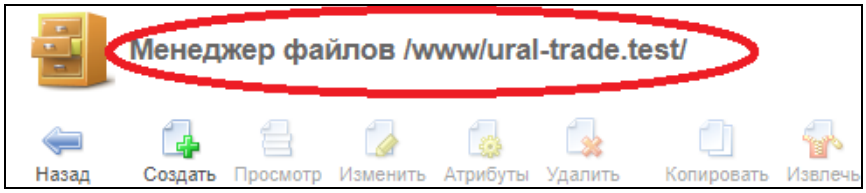

Рисунок 33 — Путь до директории сайта

Обычно корректными правами для папок являются «755», а для файлов «644», но возможны исключения, о которых должен знать разработчик сайта. Также информацию по используемым атрибутам доступа можно найти в документации или на тематических форумах используемой пользователем CMS.

Если при загрузке CMS на хостинг права будут выставлены правильно, то конфигурационный файл останется доступным для чтения всем пользователям сервера по умолчанию. Права на конфигурационный файл нужно обязательно менять и это касается не только WordPress, но и других систем управления.

Нужно беречь конфигурационный файл. Нельзя позволять никому, кроме владельца, даже читать документ, где написаны логины и пароли для доступа к базе данных, поэтому мы изменим права на файл wp-config.php. Для изменения атрибутов файла необходимо отметить нужный файл и нажать кнопку «Атрибуты» в панели управления хостингом (рисунок 34).

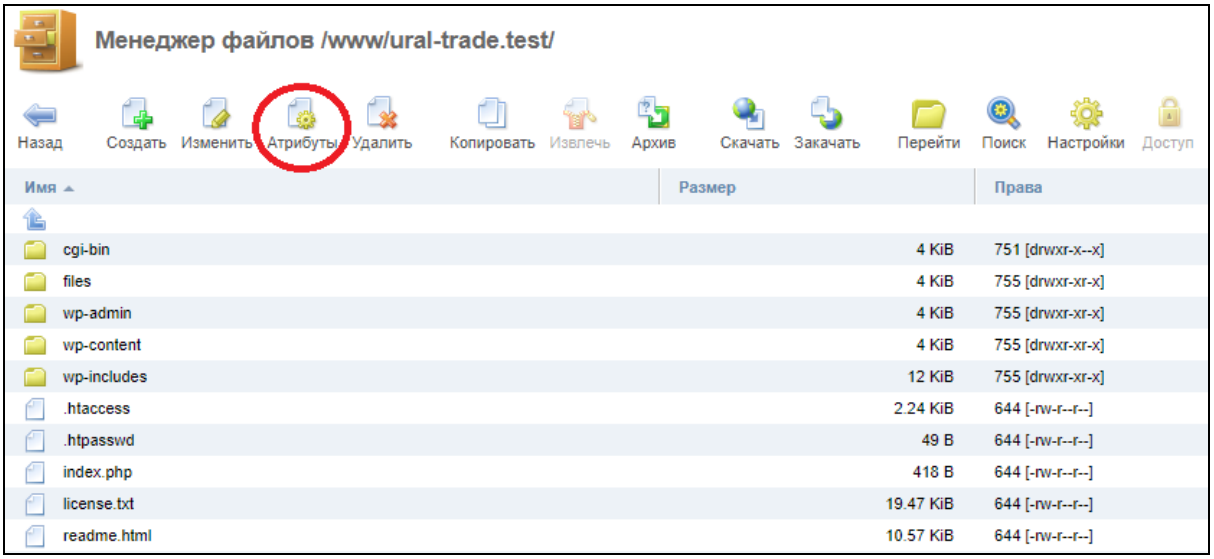

Рисунок 34 — Изменение атрибутов файла

Так как требуется запретить доступ на чтение для группы и остальных пользователей, то снимаем галочки напротив соответствующих полей и сохраняем изменения нажатием кнопки «ОК» (рисунок 35).

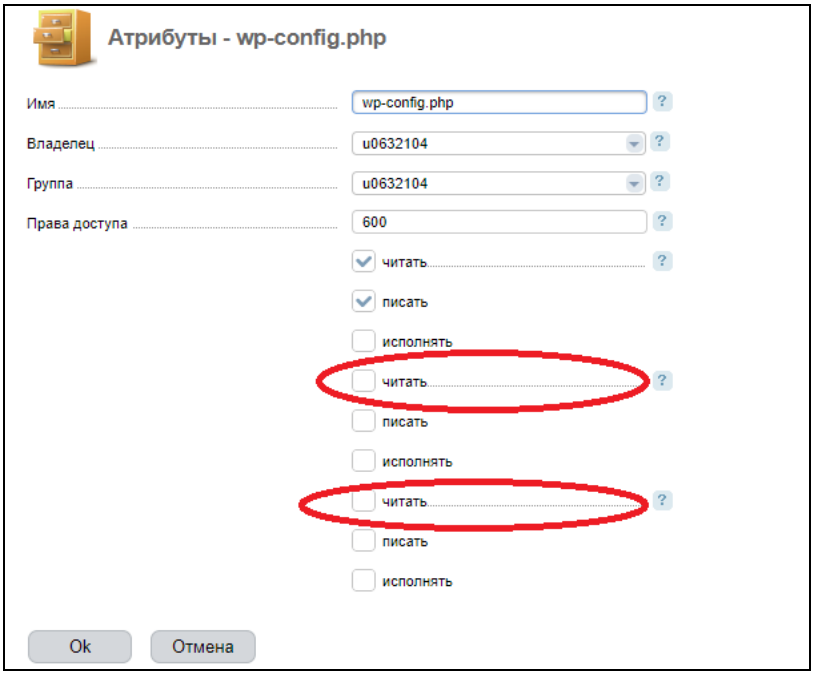

Рисунок 35 — Изменение прав доступа к файлу

Необходимо убедиться, что установленные ранее права доступа для файла сохранились, для этого находим файл в списке и проверяем права (рисунок 36).

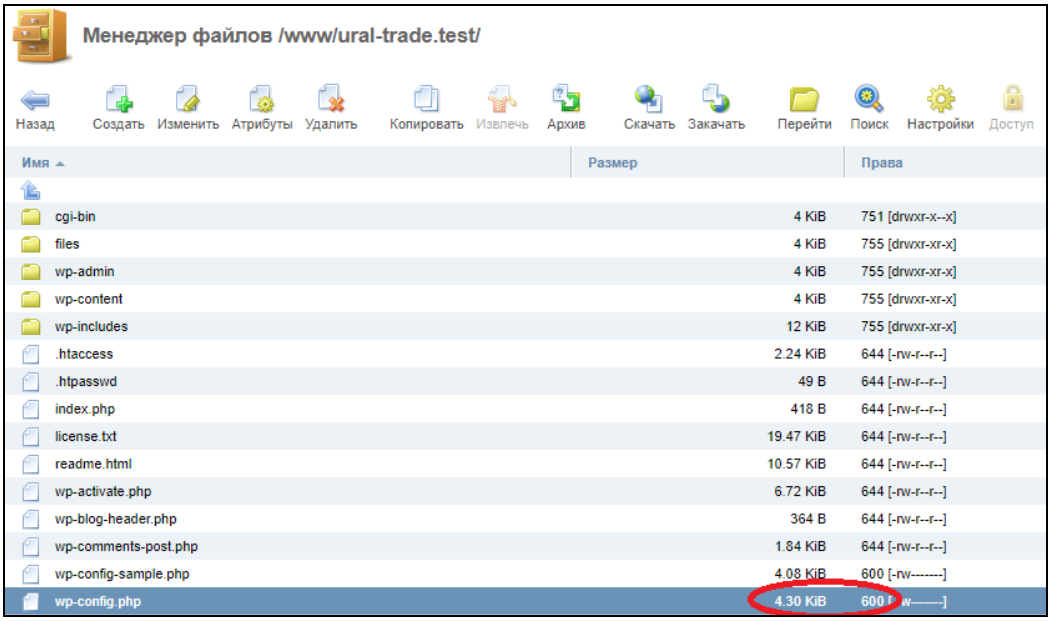

Рисунок 36—Проверка прав доступа к файлу

2.5.4 Защита сайта средствами .htaccess

Файл .htaccess — это специализированный служебный файл, использующийся для изменения настроек веб-сервера Apache и похожих серверов.

Его использование позволяет изменять работу сайта: настраивать доступ к папкам, файлам и прочим материалам, указывать правила переписи ссылок и предупреждения об ошибке. Вместе с этим не меняется функционирование всего сервера, настраиваются лишь дополнительные параметры у некоторых пользователей [27].

Главное предназначение .htaccess — настройка сайтов и каталогов в соответствии с определенными требованиями.

То есть, посредством этого файла, SEO-специалисты и программисты могут изменять настройки веб-сервера, даже не имея администраторских прав. Но изменения вносятся только для определенного сайта, и на сам сервер они никак не влияют.

Конфигурации сервера изменяются только с использованием директив (команд), включающих в себя «ключ» и «значение» для него. Все самые важные директивы, позволяющие управлять сервером, находятся в основном файле конфигурации, называющимся httpd.conf. Проблема в том, что у рядового пользователя нет возможности получить к нему доступ, так как там находится большое количество параметров, от которых зависит работоспособность всего веб-сервера.

Вот почему актуален .htaccess, позволяющий менять некоторые директивы в главном файле.

Для создаваемого сайта были применены следующие команды:

1. Запрет доступа по IP, что позволило ограничить доступ к администрированию (рисунок 37).

```
1  Order deny,allow
2  Deny from all
3  Allow from 82.193.155.236
```

Рисунок 37 — Код ограничения доступа к администрированию

Если пользователь с другим IP-адресом попытается открыть страницу, то появится ошибка (рисунок 38).

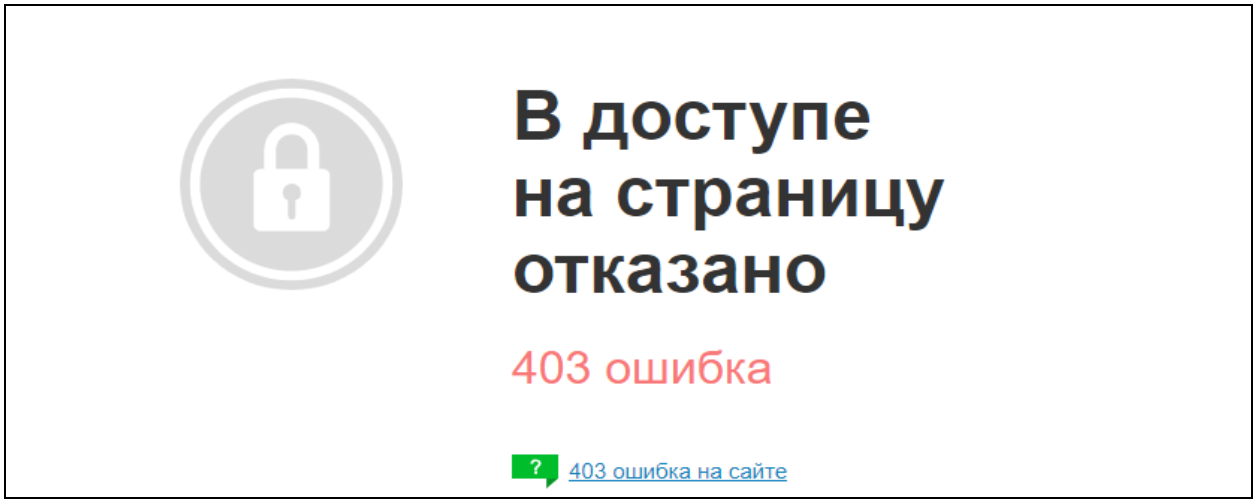

Рисунок 38— Окно ошибки

2. Установлена дополнительная авторизация на страницу административной панели (рисунок 39).

```
#
AuthUserFile /var/www/u0632104/data/www/uraltrd.com/.htpasswd
AuthName "Private access"
AuthType Basic
<FilesMatch "wp-login.php">
Require valid-user
</FilesMatch>

# Закрываем доступ к файлу .htpasswd для всех
<Files ".htpasswd">
Order allow,deny
Deny from all
</Files>
```

Рисунок 39 — Код дополнительной авторизации

При попытке входа в административную панель появится дополнительное окно авторизации (рисунок 40).

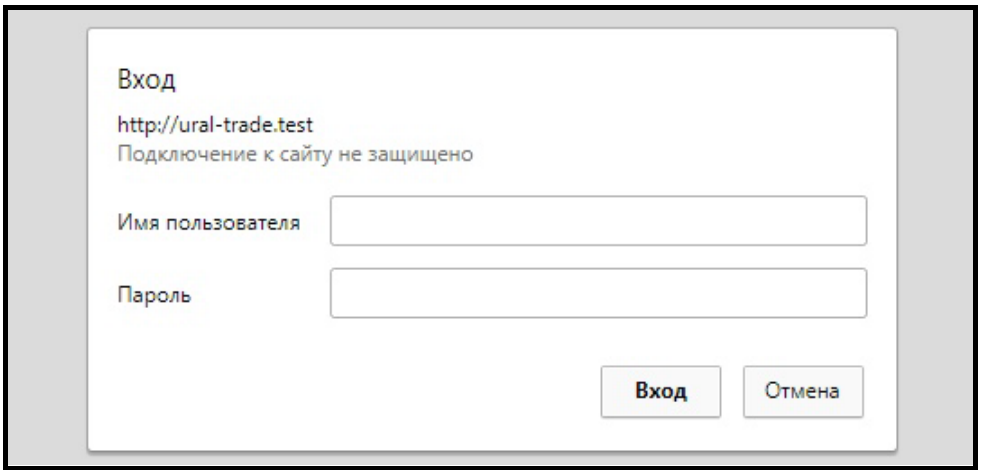

Рисунок 40 — Окно авторизации

Если пользователь не пройдёт авторизацию, то появится ошибка (рисунок 41).

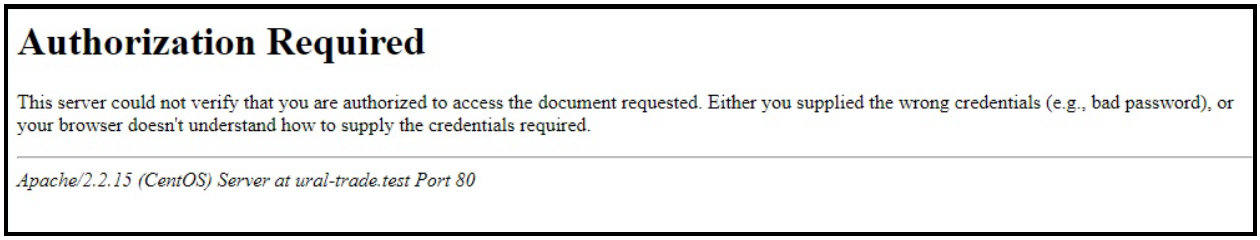

Рисунок 41 — Ошибка при авторизации

2.5.5 Защита сайта средствами резервного копирования

Одним из значимых способов повышения безопасности сайта является резервное копирование. Мало кто задумывается, что сайт может пострадать от действий злоумышленников, а именно от незаконного добавления, изме-

нения, удаления или копирования информации, сохраняющейся в базе данных или PHP скриптах. База данных или PHP скрипты могут пострадать не только от действий злоумышленников или третьих лиц, но и при внезапном выходе сервера из строя, либо при обстоятельствах непреодолимой силы (стихийные бедствия и др.). Так как большинство пользователей своевременно не заботятся о безопасности своих сайтов и не используют резервное копирование, то в случае возникновения эксцессов, оказываются не готовы к последствиям. При возникновении подобных ситуаций компания может понести финансовые и репутационные издержки, а самое главное — утечку конфиденциальной информации, что может привести к очень серьёзным последствиям. Чаще всего компании начинают задумываться о подобных мерах защиты только после возникновения экстренных ситуаций, когда уже нанесен непоправимый ущерб, что является в корне неверным подходом. Многие хостинг-провайдеры, оказывающие услуги на платной основе, обеспокоились подобной ситуацией и решили изменить тенденцию в лучшую сторону.

На выбранном компанией хостинге резервное копирование производится автоматически и не требует дополнительной настройки, что, несомненно, является большим плюсом.

В резервную копию включаются любые файлы, размер которых не превышает 300 мегабайт. Также в резервную копию включаются все созданные в аккаунте базы данных.

Для снижения нагрузки на сервера, резервное копирование данных производится ежедневно, но преимущественно в ночное время.

Для предотвращения избыточного хранения информации, каждая резервная копия хранится в течение 30 суток, после чего автоматически удаляется.

Помимо хранения резервной копии непосредственно на сервере, рекомендуется сохранять её на несколько устройств или носителей, в том числе энергонезависимых.

Чтобы перейти к скачиванию или восстановлению резервных копий, необходимо открыть систему резервного копирования, для этого требуется авторизоваться в панели управления хостингом.

Для скачивания резервной копии необходимо выполнить следующие действия: Во вкладке резервных копий выбрать нужную дату и адрес сайта (рисунок 42).

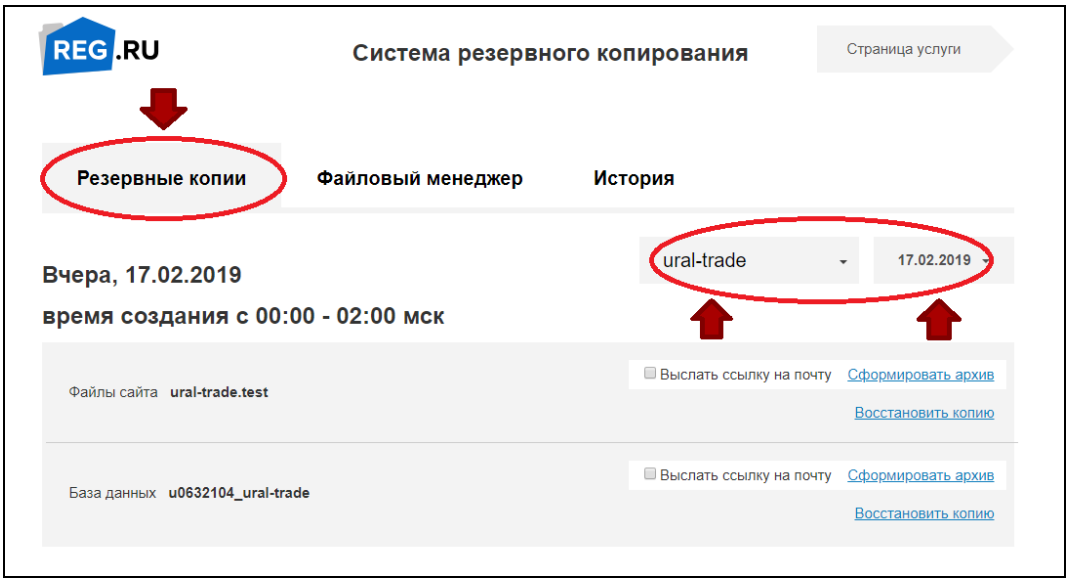

Рисунок 42 — Выбор сайта для резервного копирования

Напротив поля «Файлы сайта» необходимо нажать кнопку «Сформировать архив», если требуется чтобы ссылка на скачивание архива пришла на почту, нужно установить соответствующий флажок (рисунок 43).

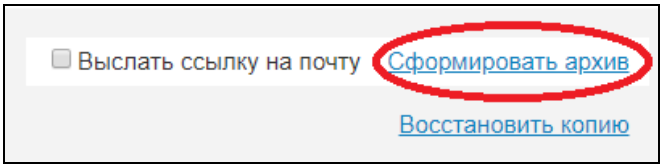

Рисунок 43 — Формирование и скачивание архива

После обновления страницы появится возможность скачать готовую резервную копию файлов или базы данных (рисунок 44).

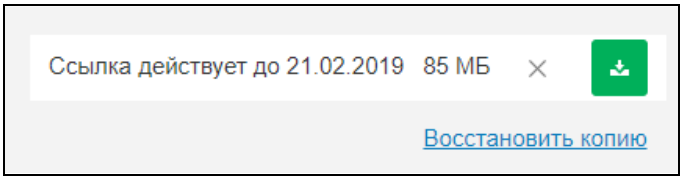

Рисунок 44 — Загрузка резервной копии

Для восстановления всего аккаунта, всех файлов, либо отдельного сайта или базы данных достаточно выбрать необходимый пункт и нажать кнопку «Восстановить копию» (рисунок 45).

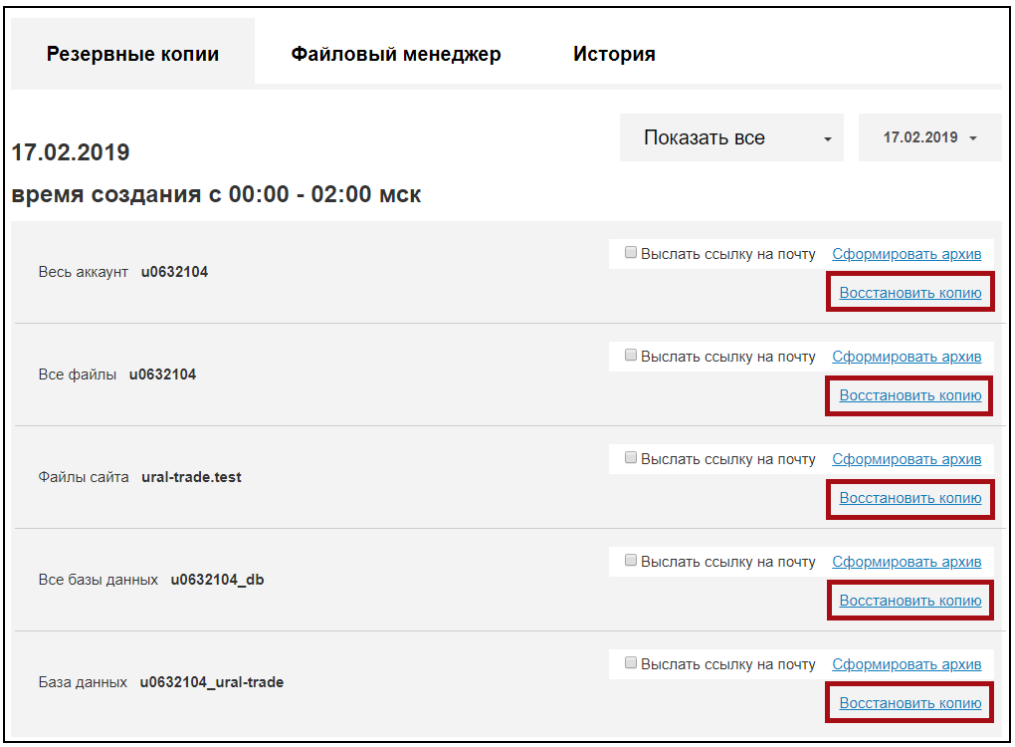

Рисунок 45 — Восстановление резервной копии

2.6 Сопроводительные лабораторные работы по обеспечению безопасности сайта

Безопасность сайта — это неотъемлемая часть успешного проекта и халатное отношение к вопросам безопасности недопустимо. Существует множество способов защиты и множество типов атак, но хорошей защищённости можно достичь лишь применением комплекса мер, нацеленных на повышение уровня безопасности сайта.

Лабораторная работа № 1.

Тема: Установка и настройка плагина All in One Security.

Цели работы:

- ознакомление с административной панелью;

- овладение навыками установки и настройки плагинов в CMS WordPress;

Для защиты от распространенных и известных уязвимостей существуют специальные плагины. Одним из таких плагинов является — All in One Security. Чтобы установить плагин All in One Security, не нужно искать и загружать его в интернете. Для этого в CMS предусмотрен каталог плагинов WordPress, он доступен прямо из административной панели.

Чтобы перейти в административную панель, необходимо:

1. Открыть браузер, перейти по ссылке: http://адрес_сайта/wp-admin/ (рисунок 46) и авторизоваться.

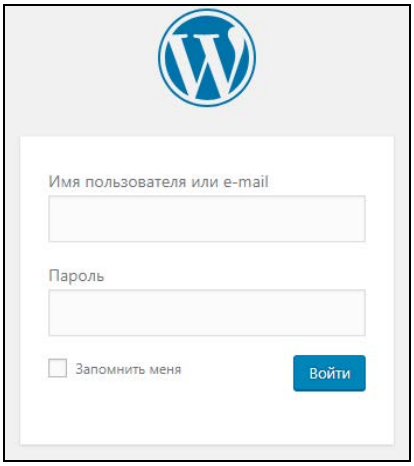

Рисунок 46 — Окно авторизации административной панели

2. В навигационной панели слева выбрать пункт меню — «Плагины», а правее — «Добавить новый» (рисунок 47).

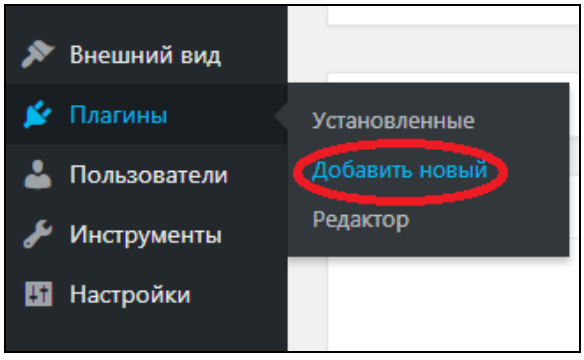

Рисунок 47—Переход к установке плагина

3. В правой части окна ввести в поле поиска название плагина —All in One Security и нажать «Enter» (рисунок 48).

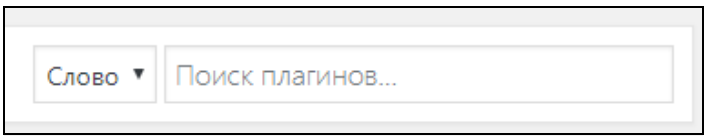

Рисунок 48—Поиск плагина

4. В центральной части окна найти необходимый плагин и нажать кнопку — «Установить» (рисунок 49).

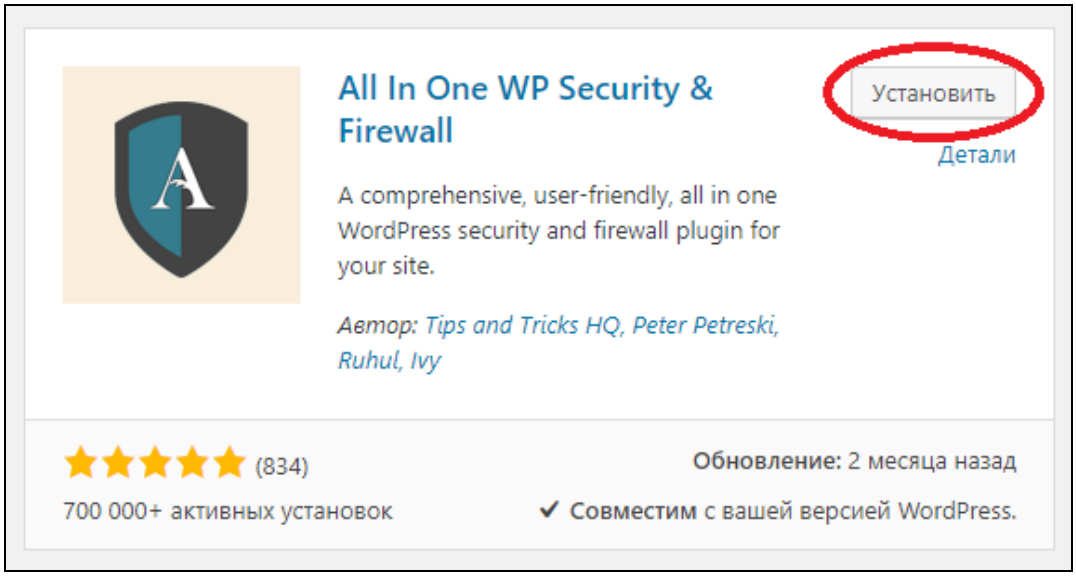

Рисунок 49 — Установка плагина

5. После завершения установки кнопка «Установить» изменится на «Активировать», её также необходимо нажать (рисунок 50).

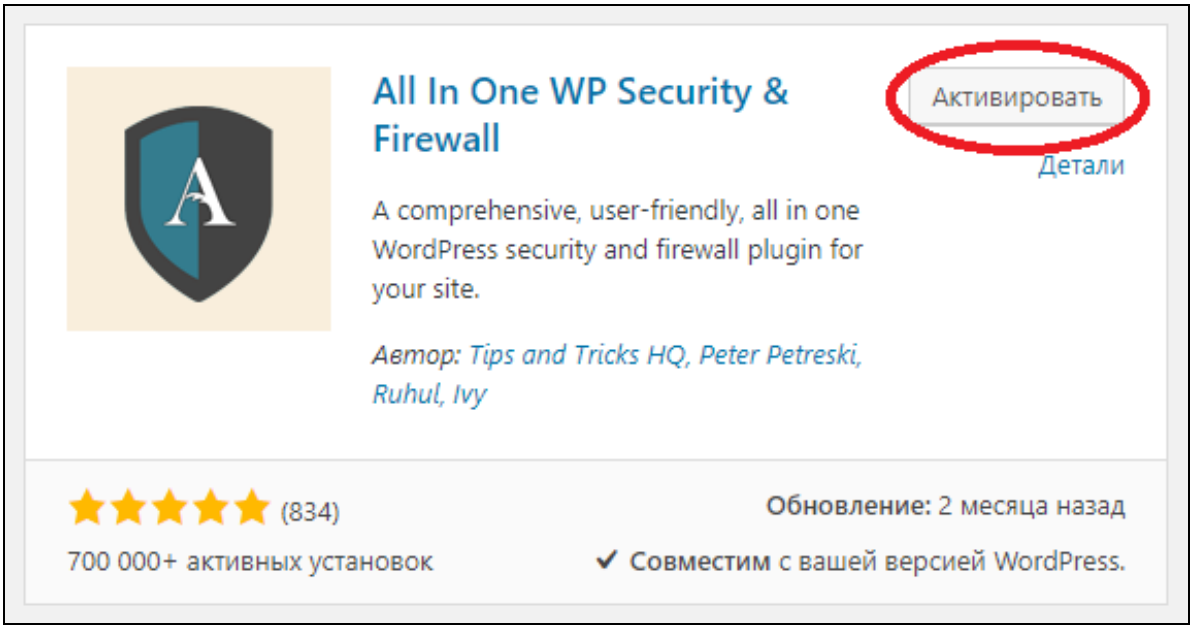

Рисунок 50 — Активация плагина

6. В навигационной панели слева выбрать пункт меню — «WP Security», а правее «Авторизация» (рисунок 51).

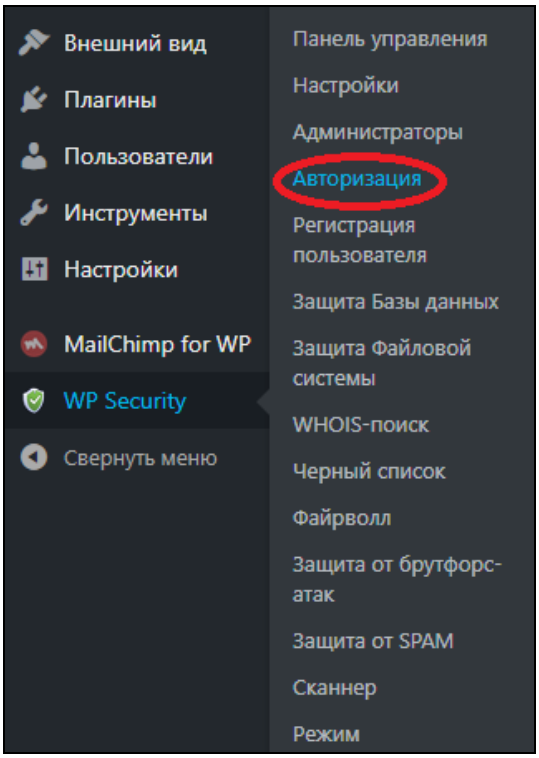

Рисунок 51 — Переход к настройкам авторизации WP Security

7. Активировать защиту от перебора паролей, установив соответствующие галочки (рисунок 52) и сохранить изменения.

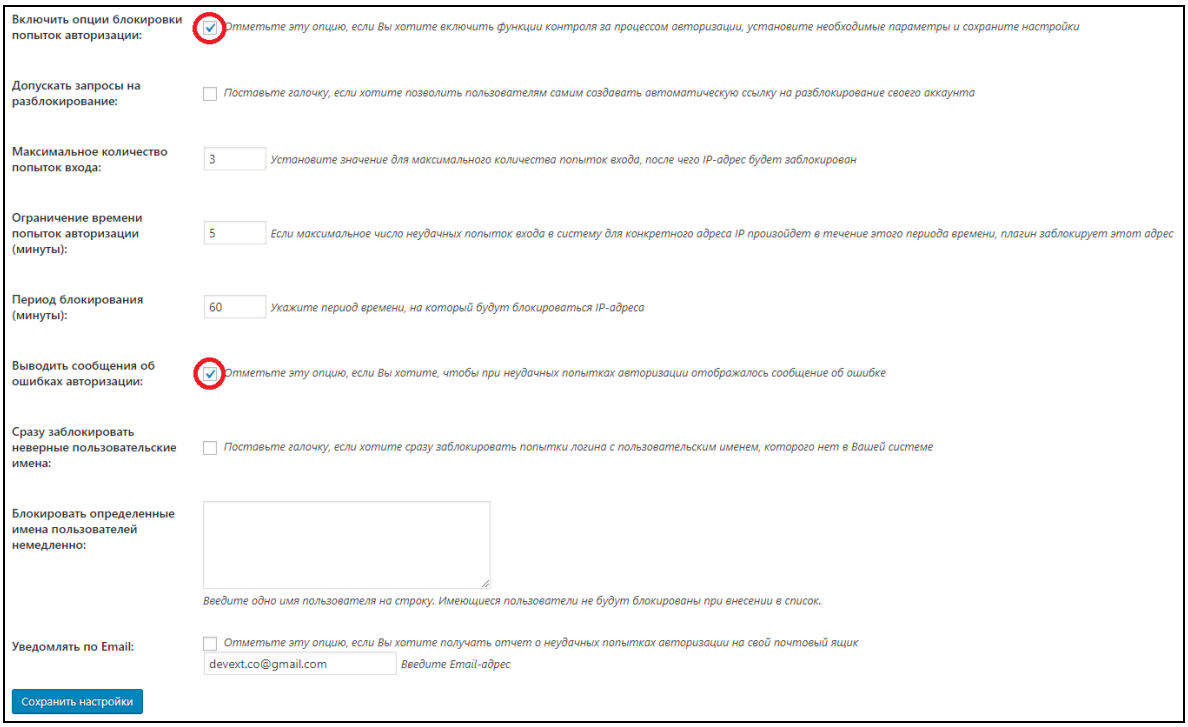

Рисунок 52 — Настройка защиты от перебора паролей

Защита от перебора паролей теперь активна. Если пользователь 3 раза неверно введет логин или пароль, то будет заблокирован на 60 минут.

Лабораторная работа № 2.

Тема: Обеспечение безопасности учетной записи администратора WordPress.

Цели работы:

- ознакомление с административной панелью;
- овладение навыками создания нового пользователя с правами администратора в CMS WordPress.

Стандартная учётная запись упрощает процесс взлома административной панели CMS WordPress. Необходимо изменить имя пользователя администратора или создать новую учетную запись администратора с другими данными. Для этого необходимо:

1. Открыть браузер, перейти по ссылке: http://адрес_сайта/wp-admin/ (рисунок 53) и авторизоваться.

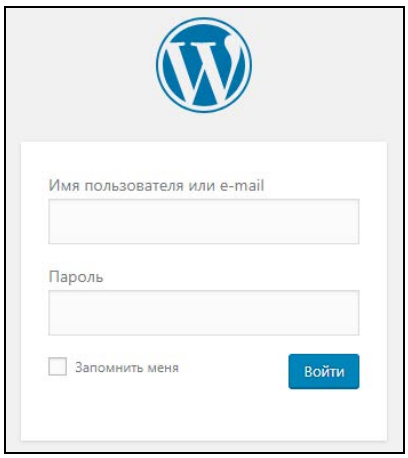

Рисунок 53 — Окно авторизации административной панели

2. В навигационной панели слева выбрать пункт меню — «Пользователи», а правее — «Добавить нового» (рисунок 54).

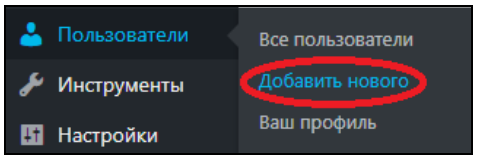

Рисунок 54 — Переход к созданию нового пользователя

3. Создать нового пользователя и назначить ему права Администратора (рисунок 55).

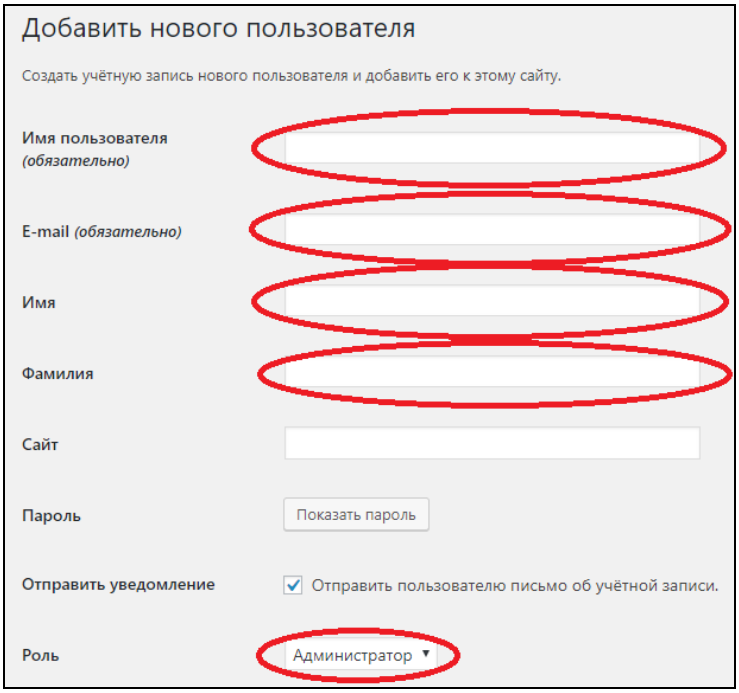

Рисунок 55 — Создание нового пользователя

По умолчанию отображаемое имя пользователя идентично логину аккаунта. Из соображений безопасности, этого допускать нельзя, так как это облегчает злоумышленнику работу. Необходимо указать Фамилию и Имя, а позже выбрать их в качестве отображаемого логина.

4. Переавторизоваться в административной панели WordPress с новыми данными.

5. В навигационной панели слева выбрать пункт меню — «Пользователи», а правее — «Все пользователи» (рисунок 56).

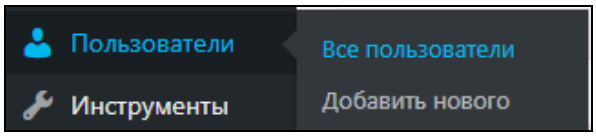

Рисунок 56— Переход к списку пользователей

6. Выбрать нужного пользователя (рисунок 57).

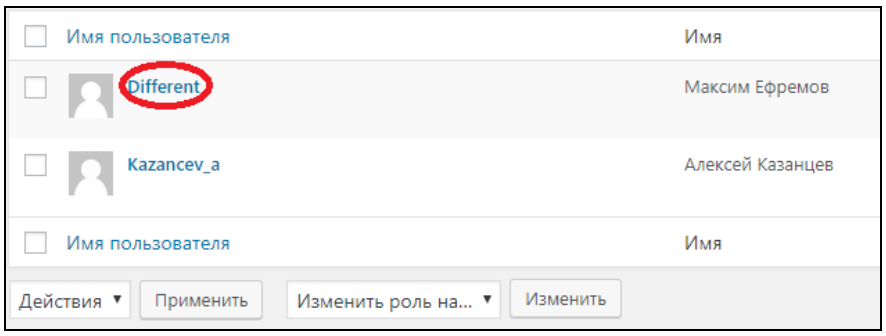

Рисунок 57— Переход к изменению пользователя

7. В разделе «Имя» нужно выбрать имя и фамилию в качестве отображаемого имени и сохранить настройки (рисунок 58).

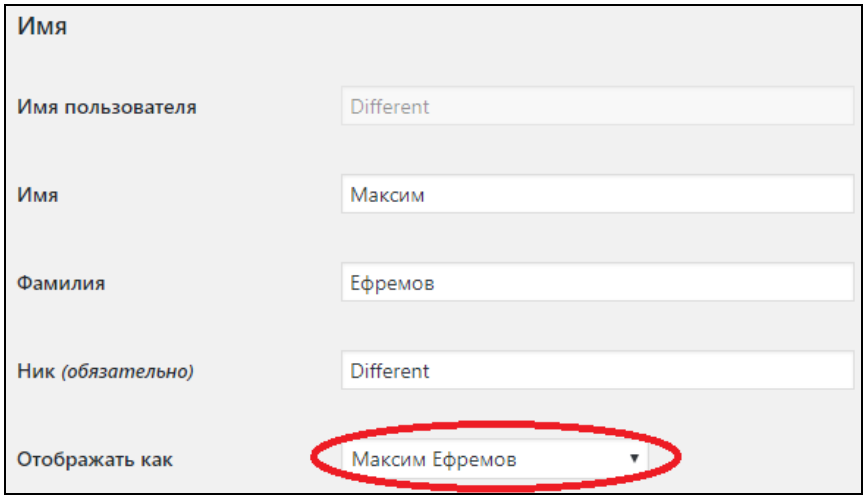

Рисунок 58 — Изменение отображаемого имени.

Теперь злоумышленнику будет гораздо сложнее узнать настоящий логин пользователя, имеющего права администратора.

Лабораторная работа № 3.

Тема: Защита административной панели WordPress средствами .htaccess.

Цели работы:

- ознакомление со структурой файла .htaccess;
- овладение навыками редактирования файла .htaccess.

Если нет уверенности в отсутствии уязвимостей административной панели CMS WordPress, то её можно защитить средствами .htaccess. Для защиты административной панели можно ограничить доступ к директории wp-

admin с помощью списка разрешенных IP-адресов. Процесс изменений будет описан на примере панели управления хостингом ISPmanager.

Чтобы обеспечить защиту доступа к директории wp-admin с помощью .htaccess, необходимо:

1. Открыть менеджер файлов, (рисунок 59), для этого требуется авторизоваться в панели управления хостингом ISPManager.

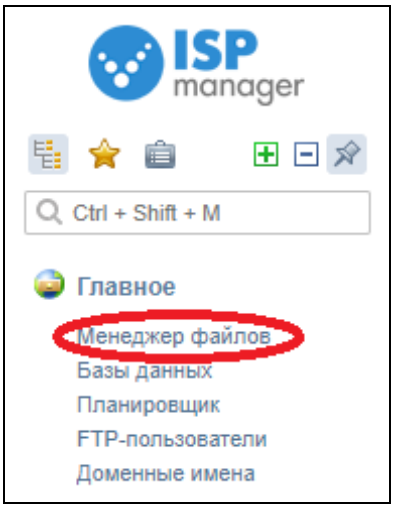

Рисунок 59 — Открытие менеджера файлов

2. Перейти в директорию /www/адрес_сайта/wp-admin/ (рисунок 60).

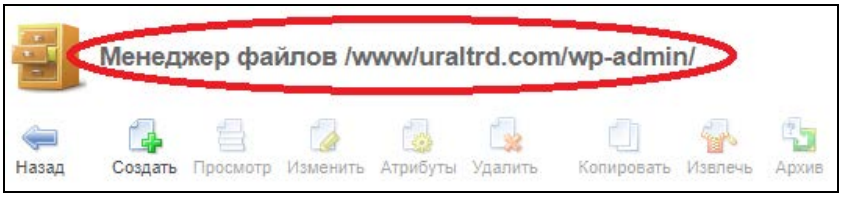

Рисунок 60 — Переход в директорию wp-admin

3. Создать файл .htaccess по нажатию кнопки «Создать» (рисунок 61).

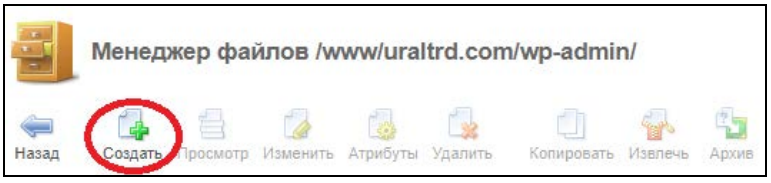

Рисунок 61 — Создание файла .htaccess

4. Указать имя файла — «.htaccess» и нажать кнопку «Ok» (рисунок 62).

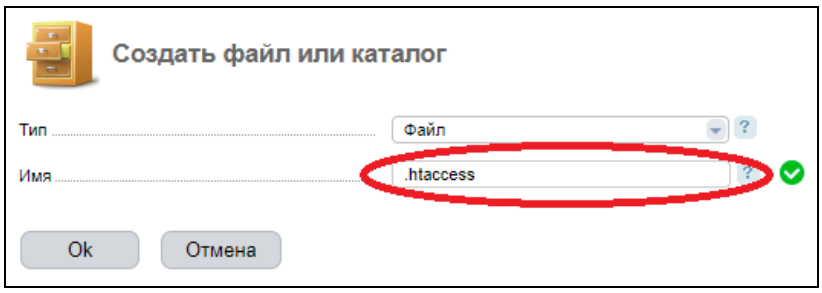

Рисунок 62 — Указание имени файла

5. Выбрать файл «.htaccess» и нажать кнопку «Изменить» (рисунок 63).

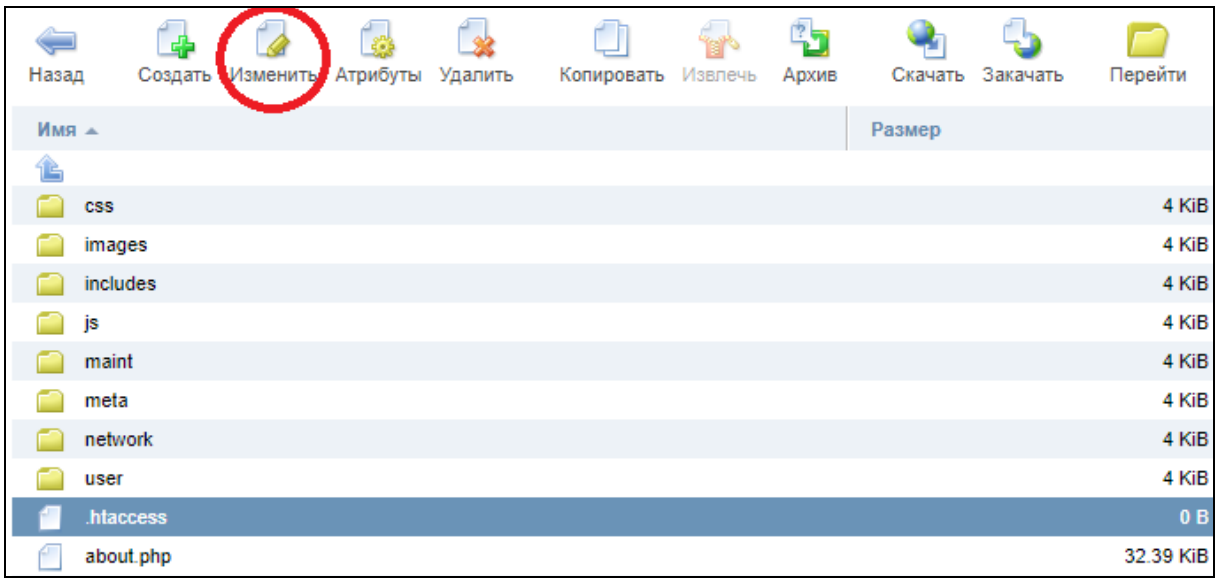

Рисунок 63 — Изменение файла «.htaccess»

6. Записать в файл строки с настройками блокировки и сохранить изменения (рисунок 64). В строке с текстом «Allow from» нужно указать разрешенный IP-адрес.

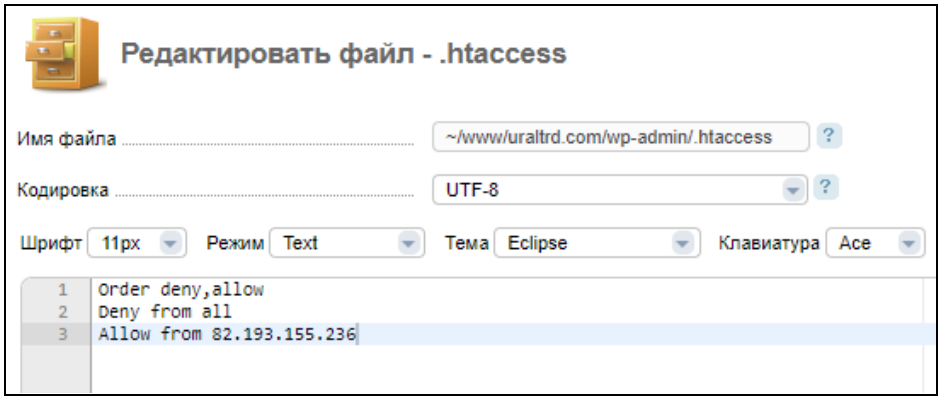

Рисунок 64 — Изменение файла «.htaccess»

Посредством Order определяется порядок обработки правил allow/deny. В случаях, когда требуется запретить доступ всем, но разрешить его опреде-

ленному пользователю, то правило запрета должно выполняться ранее, чем правило разрешения. Сначала сервер обработает правило «Deny from all», а затем разрешающее правило «Allow from». Если порядок обработки правил allow/deny будет обратным, то пользователь с разрешенным доступом все равно не получит его.

Для проверки работоспособности можно указать другой IP-адрес в качестве разрешенного, а затем попробовать открыть страницу http://адрес_сайта/wp-admin/. При правильной настройке, можно увидеть ошибку открытия страницы (рисунок 65).

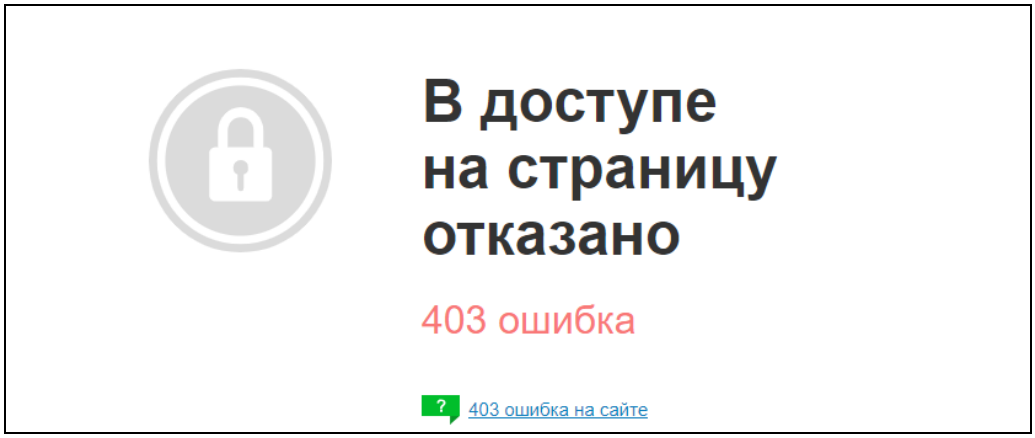

Рисунок 65 — Ошибка открытия страницы

2.7 Апробация

Апробация была проведена в ООО «УралТрейд». В ходе апробации были выявлены следующие замечания:

- отметили, что шрифт слишком мелкий, из-за чего неудобно работать с сайтом. Шрифт был увеличен на два пункта;
- орфографические ошибки, которые были исправлены.

Апробация показала, что при работе сданным сайтом у клиентов не возникнет проблем с навигацией и ориентированию по веб-сайту.

ЗАКЛЮЧЕНИЕ

В рамках выпускной квалификационной работы был разработан сайт, предназначенный для клиентов компании ООО «УралТрейд», основным видом деятельности которой является «оптовая торговля отходами и ломом». Цель компании — стать самой востребованной организацией, которой будет стремиться воспользоваться каждый потенциальный клиент: продать или купить металлолом, продать вагоны в разделку. Для того, чтобы цель компании была достигнута, важно создать индивидуальный, информативный и оригинальный сайт.

Чтобы сайт удовлетворял поставленным требованиям, был проведён анализ электронных ресурсов, устава компании, учредительных документов, из каждого источника выделены основные пункты и на их основе сделан выбор подходящей CMS, разработана максимально удобная и понятная структура сайта.

После разработки структуры сайта была установлена выбранная ранее CMS, загружен отвечающий требованиям шаблон, размещен согласно разработанной структуре контент.

При выполнении выпускной квалификационной работы были решены следующие задачи:

1. Был проведён анализ:
   - литературных источников и электронных изданий, нацеленных на сравнительный обзор различных CMS и их уязвимостей;
   - устава компании;
   - учредительных документов.
2. Реализован сайт средствами выбранной системы управления контентом. Содержит шесть блоков:
   - главная страница, которая делится на три раздела;

- страница «О нас» содержит информацию о компании: её историю, миссию и цели, а также сведения о партнёрах компании;
- страница «Услуги» делится на несколько разделов: прием цветного и нержавеющего лома; прием и покупка черного лома; закуп и реализация Ж/Д лома; грузоперевозки автотранспортом; демонтаж металлоконструкций; разделка вагонов на металлолом;
- страница «Карьера» необходим для набора новых кадров, если в том будет потребность;
- страница «Документы» содержит информацию по основным учредительным документам, а так же лицензию компании;
- страница «Контакты» содержит контактную информацию компании, номер телефоном, а так же электронные и почтовые адреса.

3. Обеспечена безопасность программной составляющей части сайта:
   - установлены плагины, обеспечивающие дополнительную защиту;
   - установлены сложные пароли.
4. Обеспечена безопасность серверной составляющей части сайта:
   - создан специальный пользователь с ограниченными правами на доступ к базе данных;
   - обеспечена защита конфигурационного файла;
   - применены дополнительные правила в .htaccess;
   - обеспечено автоматическое создание резервной копии базы данных и файловой системы.
5. Подготовлен обучающий материал для администратора сайта.

Проведена апробация сайта, которая позволила выявить и устранить недочеты. Апробация показала, что сайт позволяет узнать все возможности компании и начать работу с организацией в качестве клиента.

Таким образом, поставленные задачи можно считать выполненными в полном объеме, а цель достигнутой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. 10 советов по безопасности для защиты вашего сайта от хакеров [Электронный ресурс]. — https://www.internet-technologies.ru/articles/10-sovetov-po-bezopasnosti-dlya-zaschity-vashego-sayta-ot-hakerov.html (дата обращения: 01.02.2019).

2. 12 простых шагов, которые повысят безопасность сайта на WordPress [Электронный ресурс]. — https://starting-constructor.ru/bezopasnost-sajta-na-wordpress.html (дата обращения: 01.02.2019).

3. 6 лучших плагинов для защиты сайта на WordPress [Электронный ресурс]. — https://hostiq.ua/blog/security-plugins-wordpress/ (дата обращения: 21.10.2018).

4. Бакланова А. А. Разработка Информационного сайта для социального проекта «Живая история» [Текст] / А. А. Бакланова // Вестник Совета молодых ученых и специалистов Челябинской области. — 2016. — 67–69 с.

5. Бартлетт Д. WordPress для начинающих [Текст] / Д. Бартлетт. — Москва: Э, 2017. — 208 с.

6. Безопасность сайта. Проблема и решение [Электронный ресурс]. — Режим доступа: https://revisium.com/kb/general_website_security.html/ html (дата обращения: 28.01.2019).

7. Встречайте Wordpress [Электронный ресурс]. — Режим доступа: https://ru.wordpress.org (дата обращения: 21.10.2018)

8. Выбираем движок для сайта: платный vs бесплатный (2018 года) CMS [Электронный ресурс]. — Режим доступа: https://www.leader-web.ru/blog/razrabotka_sajtov/nofreecms/ (дата обращения: 25.11.2018).

9. Выбор CMS при создании сайта организации [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/v/vybor-cms-pri-sozdanii-sayta-organizatsii (дата обращения: 18.10.2018).

10. Выпуск №17. Выбор домена и хостинга — Setup.ru [Электронный ресурс]. — Режим доступа: https://www.setup.ru/client/subscription/48 (дата обращения: 21.10.2018).

11. Гибкость и простота Drupal [Электронный ресурс]. — Режим доступа: https://www.drupal.org/docs/7/understanding-drupal/overview (дата обращения: 29.11.2018).

12. Грачев А. Создаем свой сайт на WordPress: быстро, легко и бесплатно [Текст] / А. Грачев. — Санкт-Петербург: Питер, 2015. — 211 с.

13. Интерфейс — что это такое простыми словами, примеры интерфейса [Электронный ресурс]. — https://wikifin.ru/interfejs-chto-eto-takoe-prostymi-slovami-primery-interfejsa/ (дата обращения: 01.02.2019).

14. ИНТЕРФЕЙС САЙТА [Электронный ресурс]. — Режим доступа: https://www.webteg.ru/articles/interface/the-site.html (дата обращения: 14.01.2019).

15. Интерфейс [Электронный ресурс]. — Режим доступа: https://wiki.rookee.ru/interface/ (дата обращения: 01.02.2019).

16. История WordPress: от начала создания до наших дней [Электронный ресурс]. — Режим доступа: https://zacompom.ru/lessons/istoriya-wordpress.html (дата обращения: 18.10.2018).

17. Мощный плагин для защиты WordPress [Электронный ресурс]. — Режим доступа: http://wordsmall.ru/plaginy-dlya-wordpress/moshhnyj-plagin-dlya-zashhity-wordpress.html (дата обращения: 13.02.2019).

18. Основные термины из WP [Электронный ресурс]. — Режим доступа: http://seoslim.ru/gg/chto-takoe-wordpress-cms-opisanie-raboty.html (дата обращения: 04.12.2018).

19. Основные угрозы безопасности сайта [Электронный ресурс]. — Режим доступа: https://habr.com/ru/company/pentestit/blog/279787/ html (дата обращения: 28.01.2019).

20. Пункты приема металлолома в Череповце и Котласе, купим лом | Прогресс М [Электронный ресурс]. — Режим доступа: http://progress-m.biz/ (дата обращения: 21.10.2018).

21. Разработка алгоритма анализа CMS WordPress на наличие уязвимостей [Электронный ресурс]. — Режим доступа: https://moluch.ru/archive/138/38652/ (дата обращения: 21.10.2018).

22. Русский «Требования — WordPress» [Электронный ресурс]. — Режим доступа: https://ru.wordpress.org/about/requirements/ (дата обращения: 21.10.2018).

23. Самая лучшая защита WordPress сайта — плагин All In One WP Security [Электронный ресурс]. — Режим доступа: https://1akm.ru/sozdanie-sayta-na-wordpress/urok-9-samaya-luchshaya-zashhita-wordpress-sayta-plagin-all-in-one-wp-security/ (дата обращения: 13.02.2019).

24. Система управления содержимым — Википедия [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D1%81%D0%BE%D0%B4%D0%B5%D1%80%D0%B6%D0%B8%D0%BC%D1%8B%D0%BC (дата обращения: 18.10.2018).

25. Создание пользователя MySQL [Электронный ресурс]. — Режим доступа: https://losst.ru/sozdanie-polzovatelya-mysql (дата обращения: 16.02.2019).

26. Сравнительный обзор популярных современных (2018 года) CMS [Электронный ресурс]. — Режим доступа: https://web112.biz/news/6381-obzor-popylyarnih-cms-kakyu-sistemy-ypravleniya-kontentom-vibrat-v-2017-gody/ (дата обращения: 21.10.2018).

27. Угрозы информационной безопасности [Электронный ресурс]. — Режим доступа: http://www.pvsm.ru/informatsionnaya-bezopasnost/115774 (дата обращения: 01.02.2019).

28. Установка WordPress «WordPress Codex» [Электронный ресурс]. — Режим доступа: https://codex.wordpress.org/ru:Installation (дата обращения: 21.10.2018).

29. Установка и настройка сервера XAMPP на Windows | Инструменты | makegood [Электронный ресурс]. — Режим доступа: http://makegood.ru/tools/-xampp/ (дата обращения: 21.10.2018).

30. Файл .htaccess: что это такое, зачем он нужен, как правильно создать и настроить [Электронный ресурс]. — Режим доступа: https://webmasterie.ru/razrabotka/hosting/htaccess (дата обращения: 01.02.2019).

31. Целевая страница — Википедия [Электронный ресурс] — Режим доступа: https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%B5%-D0%B2%D0%B0%D1%8F_%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0 (дата обращения: 21.10.2018).

32. Часто используемые и потенциальные уязвимости WordPress [Электронный ресурс]. — Режим доступа: https://premium.wpmudev.org (дата обращения: 21.10.2018).

33. Что такое .htaccess? [Электронный ресурс]. — Режим доступа: https://ru.hostings.info/schools/htaccess.html (дата обращения: 01.02.2019).

34. Что такое CMS или система управления контентом? [Электронный ресурс]. — Режим доступа: https://blogwork.ru/chto-takoe-cms-ili-sistema-upravleniya-kontentom/ (дата обращения: 04.12.2018).

35. Что такое интерфейс? [Электронный ресурс]. — Режим доступа: http://otvetcenter.ru/chto/interface/ (дата обращения: 02.12.2018).

36. All In One WP Security & Firewall [Электронный ресурс]. — Режим доступа: https://ru.wordpress.org/plugins/all-in-one-wp-security-and-firewall/ (дата обращения: 13.02.2019).

37. WordPress характеристики и преимущества: Факты и статистика [Электронный ресурс]. — Режим доступа: https://inbenefit.com/wordpress-%D1%85%D0%B0%D1%80%D0%B0%D0%BA%D1%82%D0%B5%D1%80%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B8/ (дата обращения: 18.10.2018).

38. Wordpress: плюсы и минусы движка [Электронный ресурс]. — Режим доступа: https://pro-wordpress.ru/poleznoe/preimushhestva-i-nedostatki-vordpress.php (дата обращения: 21.10.2018).

Приложение

Лист задания