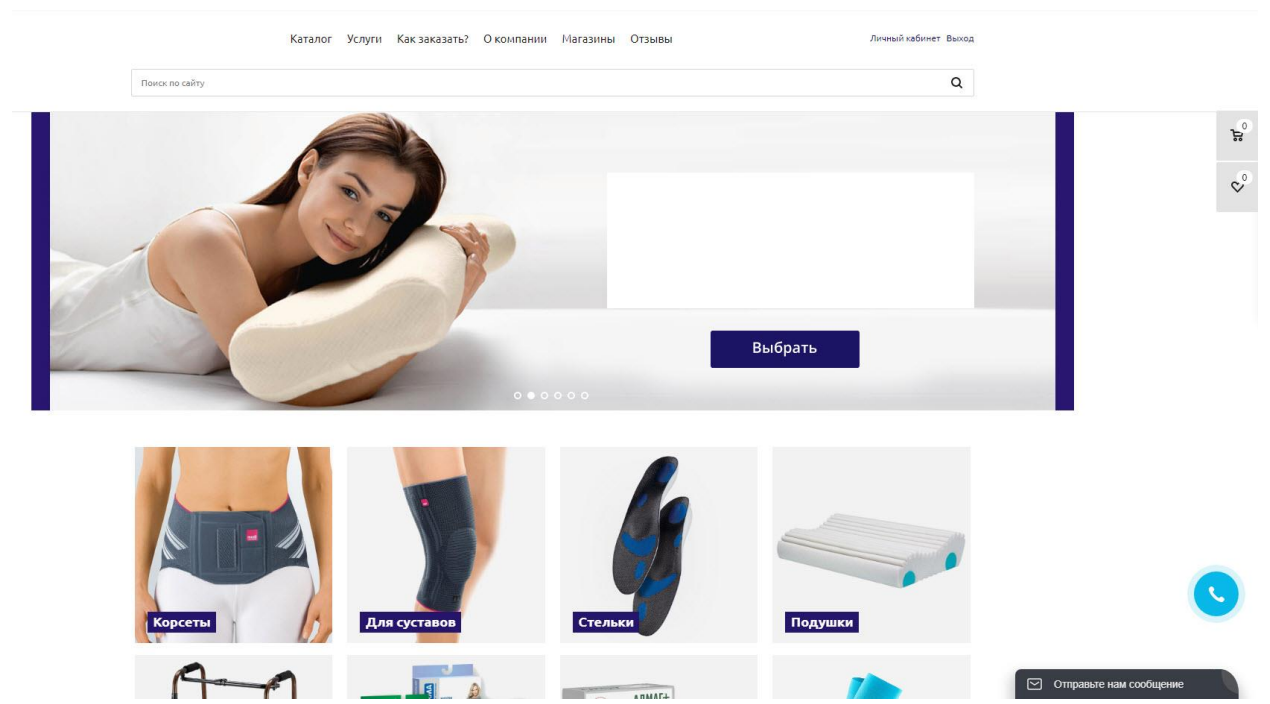


Технический аудит сайта



Содержание

Введение	3
1. Возможности Битрикс по подключению минифицированных CSS и JS файлов.....	3
2. Панель производительности конфигурации – оптимальные показатели.....	4
3. Панель производительности Битрикс	4
4. Сканер безопасности.....	5
5. Панель безопасности	6
6. Проверка оптимальности настройки сервера	7
7. Фасетный индекс	8
Проверка производительности текущего тарифного плана хостинга	9
1. Shared hosting.....	9
2. Нагрузка на сервер	9
3. Скорость работы сайта	10
4. Резервное копирование	10
5. Безопасность.....	10
6. Тарифный план	11

Введение

Целью технического аудита является выявление проблем и ошибок, влияющих на работоспособность сайта.

В ходе аудита сайта были проведены следующие работы:

- Проверка соответствия выполнения требований CMS 1С-Битрикс, предъявляемых к серверу сайта
- Проверка сайта на уровень безопасности
- Проверка производительности текущего тарифного плана хостинга

В ходе технического аудита сайта <https://name.ru> было выявлено:

1. Возможности Битрикс по подключению минифицированных CSS и JS файлов

Оптимизация CSS	
Объединять CSS файлы:	☒
Объединять JS файлы:	☒
Подключать минифицированные версии CSS и JS файлов:	☐
Переместить весь Javascript в конец страницы:	☐
Создавать сжатую копию объединенных CSS и JS файлов:	☒

Примечание: Включение минифицированных файлов может привести к ошибкам на сайте.

2. Панель производительности конфигурации – оптимальные показатели

Подсистема	Оценка	Эталон	Примечание
Конфигурация	48.65	30	
Среднее время отклика	0.0206	0.0330	секунд
Процессор (CPU)	88.0	9.0	миллионов операций в секунду
Файловая система	10 476.6	10 000	файловых операций в секунду
Почтовая система	0.0091	0.0100	время отправки одного письма (в секундах)
Время старта сессии	не измерено ³	0.0002	секунд
Конфигурация PHP	оптимально	оптимально	рекомендации
База данных MySQL (запись)	6 658	5 600	количество запросов на запись в секунду
База данных MySQL (чтение)	28 628	7 800	количество запросов на чтение в секунду
База данных MySQL (изменение)	7 113	5 800	количество запросов на изменение в секунду

Тестировать конфигурацию

3. Панель производительности Битрикс

Необходимо произвести оптимизацию и анализ базы данных.

Примечание: необходимо произвести создание резервной копии перед началом выполнения оптимизации и анализа таблиц базы данных.

4. Сканер безопасности

В ходе проверки найден ряд критических ошибок.

- Включен расширенный вывод ошибок
- Включена отладка SQL запросов (\$DBDebug в значении true)
- Произвести обновление системы SiteUpdate
- В коде обнаружено 15 проблемных мест. По возможности необходимо исправить

Проверка

Сканер безопасности

Запустить сканирование

Обнаружено угроз: 11, из них критичных: 4

Последняя проверка: 26.09.2019

1. Включен расширенный вывод ошибок

Расширенный вывод ошибок может раскрыть важную информацию о ресурсе

Что делать?

Важно!

2. Включена отладка SQL запросов (\$DBDebug в значении true)

Отладка SQL запросов может раскрыть важную информацию о ресурсе

Что делать?

Важно!

3. Не удалось проверить доступность обновлений платформы

Возможно доступно обновление системы SiteUpdate или у вашей копии продукта истек период получения обновлений

Что делать?

Важно!

4. Статический анализ уязвимостей обнаружил 15 проблемных мест

Важно!

5. Панель безопасности

- Существуют попытки атаки через XSS. По возможности необходимо данные IP адреса добавить в стоп-лист

ID	Время	Событие	Объект	IP	URL	Пользователь	Описание
823786	23.09.2019 04:49:25	Попытка атаки через XSS	\$_SERVER['REQUEST_URI']	46.158.41.45	/contacts/stores/jav/jav/jav/javascript:void%280%29		
823785	23.09.2019 04:49:25	Попытка атаки через XSS	\$_SERVER['HTTP_REFERER']	46.158.41.45	/contacts/stores/jav/jav/jav/javascript:void%280%29		
823784	23.09.2019 04:49:19	Попытка атаки через XSS	\$_SERVER['REQUEST_URI']	46.158.41.45	/contacts/stores/jav/jav/jav/javascript:void%280%29		
823783	23.09.2019 04:49:19	Попытка атаки через XSS	\$_SERVER['HTTP_REFERER']	46.158.41.45	/contacts/stores/jav/jav/jav/javascript:void%280%29		
823782	23.09.2019 04:49:13	Попытка атаки через XSS	\$_SERVER['REQUEST_URI']	46.158.41.45	/contacts/stores/jav/jav/jav/javascript:void%280%29		
823781	23.09.2019 04:49:13	Попытка атаки через XSS	\$_SERVER['HTTP_REFERER']	46.158.41.45	/contacts/stores/jav/jav/jav/javascript:void%280%29		

- Включить использование CAPTCHA при регистрации на сайте
- Включен показ ошибочных запросов базы данных. Необходимо выключить.
- Веб-антивирус выключен. Необходимо включить.

6. Проверка оптимальности настройки сервера

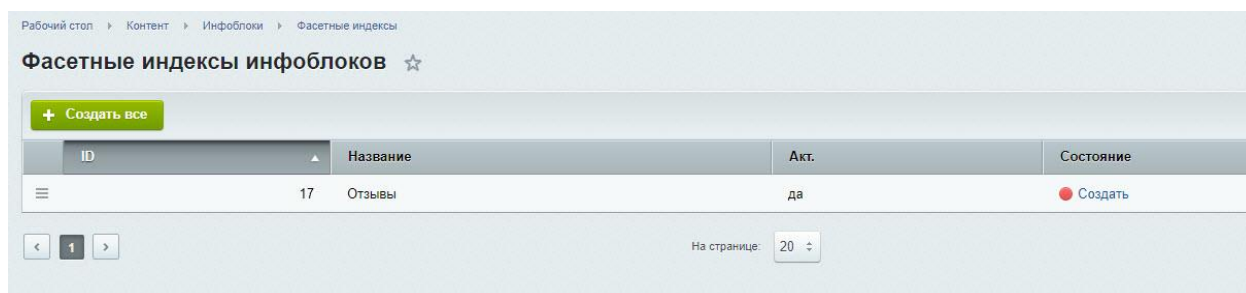
При проверке оптимальности настройки сервера ошибок не обнаружено.
Обнаружено замечание «Размер стека и pcre.recursion_limit»

Тестирование конфигурации			Проверка доступа	Техподдержка
Значения переменных сервера			✓	Корректные
Сохранение сессии			✓	Успешно
Параметры настройки UTF (mbstring и константа BX_UTF)			✓	Правильные. Сайт работает в UTF кодировке
Служебные скрипты в корне сайта			✓	Отсутствуют
Работа с сокетами			✓	Успешно
Выполнение агентов на соп			✓	Успешно
Дополнительные функции				
Параметры подключения к базе данных			✓	Успешно
Лишний вывод в файлах конфигурации			✓	Успешно
Сохранение сессии без UserAgent			✓	Успешно
Настройки сайтов			✓	Правильные
Передача объектов по ссылке			✓	Успешно
Размер стека и pcre.recursion_limit			!	Замечание. Возможны проблемы в работе с длинными строками из-за системных ограничений
Загрузка файла			✓	Успешно
Загрузка файла больше 4Мб			✓	Успешно
Загрузка файла через php://input			✓	Успешно
Передача POST запроса с большим числом параметров			✓	Успешно

Примечание: Если параметр pcre.recursion_limit превышает системный размер стека (обычно 8 Мб), то PHP падает с ошибкой Segmentation fault при выполнении сложных регулярных выражений.

7. Фасетный индекс

На сайте установлен умный фильтр. Даже если самой фильтрации на данный момент не происходит, умному фильтру необходимо построить набор свойств для показа. Это будет происходить быстрее, если создан «Фасетный индекс». На данный момент «Фасетный индекс» не валиден.



+ Создать все			
ID	Название	Акт.	Состояние
17	Отзывы	да	Создать

Примечание: Создание индексов занимает продолжительное время, если в каталоге сотни тысяч товаров. Рекомендуется выполнять индексацию в период минимальной нагрузки на сервер.

Проверка производительности текущего тарифного плана хостинга

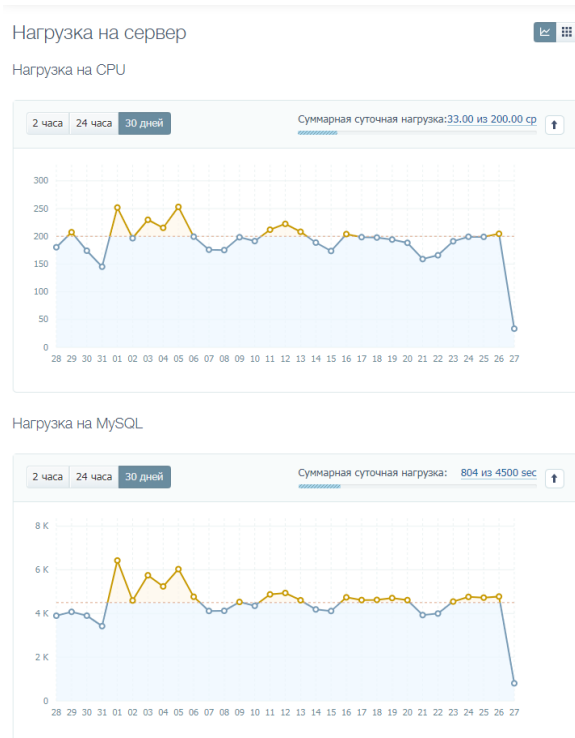
1. Shared hosting

Сайт расположен на Shared hosting - Ваши ресурсы делят все клиенты провайдера, которых он разместил на одном сервере с Вами, что неизбежно накладывает определенные ограничения.

Виртуальный хостинг является экономичным решением для обеспечения работы сайтов с относительно небольшой аудиторией и нагрузкой на сервер.

2. Нагрузка на сервер

Нагрузка на CPU и MySQL систематически превышает лимит. В ближайшее время необходимо увеличить процессорное время.



Примечание: предоставление графиков нагрузки возможно при использовании Shared hosting.

Предоставления графиков нагрузки VDS осуществляется в том случае, если данные графики предоставляет провайдер в личном кабинете.

3. Скорость работы сайта

Время загрузки контента (время, когда пользователь увидит страницу сайта) – 5сек.

Время загрузки для взаимодействия со страницей (время, когда пользователь сможет выполнять различные действия на странице) – 13,3сек.

Рекомендации: для уменьшения времени загрузки страницы необходимо произвести оптимизацию изображений, используя утилиты (JPEGOptim/ OptiPNG). Для произведения оптимизации изображений необходимо обратиться к специалистам.

Успешный аудит: TTFB (время до получения первого байта, отклик сервера при подключении клиента) – 240мс

4. Резервное копирование

Резервное копирование средствами хостинга – хранится 3 копии, выполняется через день, входят в состав тарифа, выполняются автоматически.

5. Безопасность

Для доступа в административную часть сайта у пользователей, которые принадлежат к группе «Администраторы», рекомендуется сменить пароль.

Рекомендации: в пароле должны содержаться: цифры, прописные буквы, строчные буквы, спец символы, длина пароль не менее 8 символов

Также необходимо перейти с незащищенного протокола FTP на защищенный протокол SFTP для передачи данных.

6. Тарифный план

На данный момент к основному тарифу подключены дополнительные услуги, что увеличивает абонентскую плату почти в 2 раза:

Добавлено дисковое пространство 6 ГБ, добавлен лимит нагрузки на CPU и на базы данных

Тариф

Eterno 990 Р		Итого в месяц 1790 Р	Сохранить изменения
 Количество сайтов 30	 30 99		
 Дисковая квота, ГБ 26 + 450 Р	 20 99		
 Лимит нагрузки на CPU сервера, CP ? 200 + 100 Р	 150 250		
 Базы данных неограниченно	 ∞ ∞		
 Пользователи FTP 30	 30 99		
 Лимит нагрузки на базы данных ? 4500 + 250 Р	 2500 6500		

Дополнительные услуги


IPv4

Дополнительный IP


 Обратите внимание! SSL-сертификаты переехали в [отдельный раздел](#)

Список подключенных услуг

Услуга	Стоимость	Дата подключения	Оплачено до
1Гб на диске	75 Р	29 июл 2019	Бессрочно (75 Р/мес)
1Гб на диске	75 Р	29 июл 2019	Бессрочно (75 Р/мес)
1Гб на диске	75 Р	29 июл 2019	Бессрочно (75 Р/мес)
1Гб на диске	75 Р	29 июл 2019	Бессрочно (75 Р/мес)
1Гб на диске	75 Р	29 июл 2019	Бессрочно (75 Р/мес)
1Гб на диске	75 Р	29 июл 2019	Бессрочно (75 Р/мес)
увеличение лимита нагрузки CPU 50ср	100 Р	29 июл 2019	Бессрочно (100 Р/мес)
увеличение лимита нагрузки MySQL 2000сек	250 Р	29 июл 2019	Бессрочно (250 Р/мес)

Рекомендации:

- Для экономии и оптимальной работы сайта рекомендуется перенести сайт на VPS-сервер.
- Примерная стоимость тарифа 800 Р/мес (например <https://cloud.yandex.ru/>). На данном сервере уменьшится время загрузки, время отклика сервера, время обработки запросов к базам данных