Аудит КП “___”

1. Проверка сайта штатными средствами 1С-Битрикс

1.1. Тестирование конфигурации

Ошибок не выявлено.

Замечания:

1. Отправка почты. Отправлено. Время отправки: 1.51 сек.
2. Отправка почтового сообщения больше 64Кб. Отправлено. Время отправки: 2.37 сек.

Время приемлемое, немного дольше идеала битрикса.

Тестирование конфигурации

Конфигурация сервера, в целом, удовлетворяет требованиям.

Производительность конфигурации на 12.10.2018 12:55:43 составляет 49.89

Подсистема	Оценка	Эталон	Примечание
Конфигурация	**49.89**	30	
Среднее время отклика	0.0200	0.0330	секунд
Процессор (CPU)	49.2	9.0	миллионов операций в секунду
Файловая система	5 199.8	10 000	файловых операций в секунду
Почтовая система	1.5520	0.0100	время отправки одного письма (в секундах)
Время старта сессии	0.0001	0.0002	секунд
Конфигурация PHP	оптимально	оптимально	рекомендации
База данных MySQL (запись)	1 955	5 600	количество запросов на запись в секунду
База данных MySQL (чтение)	10 394	7 800	количество запросов на чтение в секунду
База данных MySQL (изменение)	3 540	5 800	количество запросов на изменение в секунду

Тестировать конфигурацию

Конфигурация веб-сервера и ПО

Рекомендуется отключить фиксацию баннеров. Данная опция может быть полезна для сайтов. В корпоративном портале нет рекламы, поэтому не нужно фиксировать показ баннеров.

Быстрый морфологический поиск выключен. Для более быстрого поиска рекомендуется установить поисковую систему Sphinx. Использование Sphinx в качестве поискового механизма позволит значительно увеличить скорость поиска и снизить нагрузку на сервер. Так как используется виртуальная машина 7.3.2, то можно установить Sphinx через виртуальную машину. Переиндексация и смена поисковой системы на Sphinx произойдет автоматически.

Настройки "Битрикс", непосредственно влияющие на производительность

Настройка	Значение	Рекомендации
Автокеширование компонентов	Включено	
Фиксация числа показов баннеров	Включена и есть баннеры с фиксацией	Рассмотрите возможность отключения
Настройки модуля поиска	Быстрый морфологический поиск выключен	Включите морфологический поиск и опцию быстрого поиска
Хранение кеша	Файлы	Возможные типы хранения: • Файлы • memcached • eAccelerator • APC • XCache Инструкция по настройке.
Управляемый кеш	Включен	
Закодированные модули	Не найдены	
Оптимизация и анализ таблиц базы данных	Была выполнена менее месяца назад	

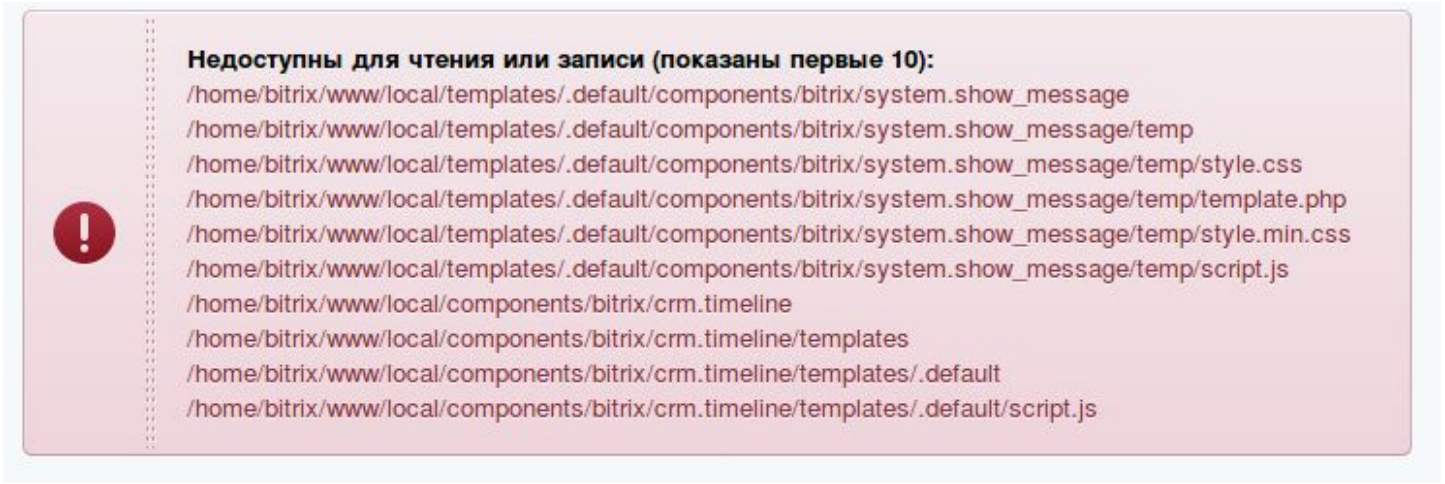
1.2. Тестирование скорости сайта.

Проведено тестирование производительности (1 ч, более 1 100 хитов).

Длительность выполнения запросов в пределах нормы, аномально долгих запросов нет. Время выполнения страницы не превышает 3 секунд.

1.3. Проверка доступа.

Недоступны для чтения или записи более 10 файлов.



Рекомендация: выставить верные права на файлы. Владельцем должен быть bitrix. Права на файлы выставить - 664, на папки - 755.

1.4. Резервное копирование портала.

Включено автоматическое резервное копирование. Резервные копии действительно делаются, в журнале резервного копирования ошибок нет.

1.5. SSL.

Сертификат настроен верно. Используется штатный dehydrated.

1.6. Сканер безопасности.

Найдены служебные файлы.

Файл /home/bitrix/www/mysql_debug.sql. Рекомендация: удалить файл или корректно ограничить к ним доступ. В данный момент злоумышленник может скачать бекап БД, перейдя по ссылке ___/mysql_debug.sql

Уровень безопасности административной группы не является повышенным.

Рекомендация: Желательно повысить уровень безопасности. На данный момент уровень безопасности - “Начальный”. Для этого перейдите в редактирование группы Администраторов (id=1). Во вкладке “Безопасность” у поля “Предопределенные настройки уровня безопасности” выставите значение “Повышенный”.

Включен расширенный вывод ошибок.

Рекомендация: Не желателен показ текста ошибки. Рекомендуется изменить параметр “debug” в конфигурационном файле /home/bitrix/www/bitrix/.settings.php.

Обнаружено как минимум 6 файлов или директорий с доступом на запись для всех пользователей окружения в котором работает веб-сервер.

`/bitrix/activities/custom/crmgetdataentityactivity`

`/bitrix/activities/custom/crmgetdataentityactivity/crmgetdataentityactivity.php`

`/bitrix/activities/custom/crmgetdataentityactivity/lang`

`/bitrix/activities/custom/crmgetdataentityactivity/lang/en`

`/bitrix/activities/custom/crmgetdataentityactivity/lang/en/.description.php`

Рекомендация: Изменить права доступа к файлам, папкам. Права на файлы выставить - 664, на папки - 755.

1.7. Веб-антивирус.

Рекомендация: Включить веб-антивирус (Административная панель -> Проактивная защита -> Веб-антивирус) для большей безопасности.

Также следует изменить конфигурацию PHP, чтобы файл
`/home/bitrix/www/bitrix/modules/security/tools/start.php`
обнаруживал вирусы до до старта буферизации вывода. Для этого нужно добавить запись
`auto_prepend_file = /home/bitrix/www/bitrix/modules/security/tools/start.php`
в файл /etc/php.ini, перезапустить веб-сервер Apache.

1.8. Защита от фреймов.

Рекомендация: Включить защиту от фреймов (Административная панель -> Проактивная защита -> Защита от фреймов) для предотвращения некоторых видов атак (Clickjacking, Framesniffing). Если планируется использовать открытые линии, то данную опцию включать не нужно. На данный момент создана открытая линия, но за всё время существования нет ни одного обращения, то есть фактически пока они не используются.

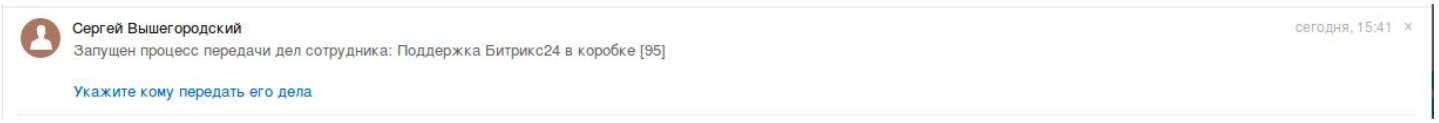
2. Аудит доработок портала.

2.1. ЭДО и РЕЕСТЕР, увольнение сотрудников.

БП “Передача дел уволенного сотрудника”.

Лишняя переменная “FirstEmp_id”, которая всегда пуста. В неё идёт запись {=Document:PROPERTY_OT_KOGO_ID}. Но приставка “_ID” к полю документа ничего не возвращает.

Если запустить бизнес-процесс, то появляется уведомление. Ссылка формируется неправильно - при её нажатии попадаем на карту сайта. Следует изменить формирование ссылки в действии бизнес-процесса.



В действии “PHP-код” никогда не вызовется функция делегирования
`MWIDelegateFired::DelegateAll($FirstEmp,$SecondEmp);`
так как эта функция выполняется только при условии, что FirstEmp_id не пустой. А FirstEmp_id всегда пустой (см. выше). То есть передача дел не происходит.

2.2. Канбан.

Заказчик сообщил, что доработка канбана на данный момент не завершена. С точки зрения пользователя появилась возможность фильтровать по отделу. Фильтрация действительно работает.

2.3. Записи при удаление задач.

Доработка выполнена через подписку на событие удаление задачи. Запись происходит в инфоблок “INTEGRATION - Удаляемая запись из сущности” сохраняется id удалённой задачи, кто удалил.
Замечаний нет.

2.4. Автозадачи.

Доработка выполнена через механизм Битрикс “Роботы”. Если у созданного лида ответственный - “Мистер Битрикс”, и источник лида - “Веб-сайт”, то создаётся задача. Данная логика работает.

Замечания:

1. Есть неиспользованные переменные (например “Лид наш или партнерский”), пустые блоки (“Добавить ещё задач”).
2. В бизнес-процессе заложена некая логика при условии, когда id лида равняется 0. Так как id созданной сущности всегда больше 0, то данный блок выполняться никогда не будет.

2.5. Подтягивание полей в сделку.

Происходит обновление сделки в init.php в зависимости от разных условий, например, по обновлению лида. Реализовано через подписку на события.
Замечаний нет.

2.6. Обязательный коммент в задаче.

Реализовано посредством JS (/local/lib/js/additional.js). Данный скрипт пытается вывести “Вы не сохранили комментарий” при уходе сотрудника со страницы задачи Бизнес-процесса, если текст в комментарии присутствует, но кнопка Сохранить не было нажата.
Замечание: Обязательность комментария можно выставить в настройках действия БП. Рекомендуется использовать встроенную функцию "обязательность комментария".

2.7. Обязательные причины отказа

Доработка попап Битрикса посредством JS (/local/lib/js/additional.js). В списке статусов лида убран положительный результат, программно выбирается отрицательный результат. Добавлено текстовое поле для причины отказа. По нажатию Сохранить, отправляется ajax.

Замечание:

1. В ajax-запросе в данном файле JS, например на строке 145, не передаётся id сессии. И соответственно, нет проверки на сервере, что создаёт уязвимость: возможна атака типа CSRF.
2. Относительно отрицательных стадий в канбане. В данный момент нельзя в канбане лид перевести в отрицательную стадию. Стадии скрыты от пользователя посредством css

(/local/lib/css/additional.css).

2.8. Настройка бекапа в облако microsoft onedrive.

Присутствует крон-задача на бекапирование с использованием duply:

```
0 3 * * * /usr/bin/duply ubitrix backup_verify_purge --force >>
/var/log/duply.log 2>&1; /usr/bin/duply etc backup_verify_purge --force >>
/var/log/duply.log 2>&1; /usr/bin/duply b24 backup_verify_purge --force >>
/var/log/duply.log 2>&1
```

В логах /var/log/duply.log ошибок не наблюдается.

2.9. Резервное копирование файлов Лида; Обязательные поля в лиде; Создание сделок из Лида.

Резервное копирование файлов Лида.

Заказчик точно не помнит, что подразумевалось под данной доработкой. Исследуя код, была обнаружена функция SaveAllLeadFiles (/local/php_interface/init.php). Сохранение происходит пользовательских полей типа Файл. Так как у лида нет полей данного типа, то бекапирование не происходит.

Замечание: В выборке CCrmLead::GetListEx используется переменная $SelectedFiles. Нет проверки на пустоту данной переменной. Из-за этого происходит выборка всех полей, что не подразумевалось.

Обязательные поля в лиде

Доработка выполнена через механизм Битрикс “Роботы”. Постановка задания на ответственного, если не заполнены обязательные поля. Но выполняется данная логика только при условии, что id лида = 0. Так как id созданного лида не может равняться 0, то задание никогда не ставится ответственному. Заказчик сообщил, что доработка в дальнейшем будет удалена.

Создание сделок из Лида

Доработка выполнена через механизм Битрикс “Роботы”. Создание сделки по смене стадии у лида. Создание сделки происходит только если id сделки равняется 0. Так как id созданного лида не может равняться 0, то сделка не создаётся. Заказчик сообщил, что доработка в дальнейшем будет удалена.

2.10. Создание персонализированных сообщений в разделе "Компания".

Заказчик не знает, что это за доработка. С точки зрения пользователя в компаниях не обнаружена возможность создавать персонализированные сообщения.

2.11. Новые лиды раскрасить в зеленый ; Подготовить поле товар (новое поле) под фрейм; Из лида все поля нужно тянуть в карточку сделки; Идентификатор партнера в товаре.

Новые лиды раскрасить в зеленый

Использование JS. Если название лида содержит “$”, то строка лида раскрашивается.

Из лида все поля нужно тянуть в карточку сделки

Используется событие OnAfterCrmLeadUpdate. На каждое обновление лида обновляется привязанная

сделка.
Замечание: возможна потеря данных. Если в сделке обновить поле, то оно может впоследствии быть перезаписано вследствие обновлении лида.

Идентификатор партнера в товаре

За определение признака в товаре отвечает функция CheckLeadProducts в init.php.

Замечание: в проверки ниже единица никогда не вернётся.

```
if(in_array(1, $product_types) && in_array(2, $product_types))
  return 3;
elseif(in_array(2, $product_types))
  return 2;
elseif(in_array(2, $product_types))
  return 1;
```

Подготовить поле товар (новое поле) под фрейм

В функции сохранения товара AfterProductRowsSave:

```
$entity = new CCrmLead(false);
$entity->update($ID, $fields);
```

```
$fields = array('UF_CRM_1529675483'=> true);
$entity = new CCrmLead(false);
$entity->update($ID, $fields);
```

Желательно не нагружать базу данных запросами, если это можно избежать, чтобы увеличить производительность портала. В данном случае, лучше собрать все изменения в один массив, а после произвести обновление.

Заказчик сообщил, что работы по блоку управления товарами приостановлена. На данный момент видна доработка по добавлению новой вкладки на детальную страницу лида путём модификации компонента crm.lead.details (см. ниже).

Замечание: есть зависимость от пользовательского поля UF_CRM_PRODUCT_TAB. Так как такого поля не существует, то вкладка добавляться не будет.

2.12. Автоматическое создание сделок по признаку.

См. выше “Создание сделок из Лида”.

2.13. Прочее.

Доступность лог файлов

Любой неавторизованный пользователь может прочитать логи по адресу:

___/local/log.txt

Рекомендация: изменить способ логирования, либо ограничить доступ к файлу.

Копирование файлов ядра

Некоторые сторонние доработки (например, Канбан задач) основаны на копировании файлов ядра Битрикс, и добавления в них новой функциональности. Скопированы некоторые шаблоны, компоненты, модуль tasks. Чем это грозит? При обновлениях портала Битрикс меняет файлы ядра. Но новая функциональность Битрикс при обновлениях может не работать, так как будут выполняться неактуальные скопированные файлы ядра. Таким образом, при обновлении портала могут появляться ошибки, на исправления которых может потребоваться очень много времени.

Рекомендация: не копировать файлы ядра. Использовать другие способы доработки: result_modifier и вызов оригинального шаблона, использование JavaScript, другие.

Вопрос заказчика: “Насколько масштабно был изменен нативный битриксовый код php. Насколько велик шанс, что обновления модулей приведут к сбоям или вообще не пройдут.”

Скопировано 12 компонентов, 6 шаблонов, 1 модуль. Это достаточно много. Сбои при обновлении будут зависеть от самих обновлений Битрикс. Если обновления будут касаться скопированных файлов ядра, то сбои почти неизбежны. В лучшем случае, новая функциональность Битрикс будет просто не видна.