



ООО “ДигИнКор”, Россия, г.Ижевск,  
ул. Карла Маркса, 421.

[Sale@Digincore.com](mailto:Sale@Digincore.com), тел. +7-912-851-7281

[www.digincore.com](http://www.digincore.com), [www.digincore.org](http://www.digincore.org)

## Развертывание страницы блокировки. Описание решения.

### Решаемая задача

Запросы к сайтам из блэклистов перенаправлять на страницу блокировки, дающую возможность пользователю запросить экспертную переоценку заблокированного сайта.

### Техническое решение

Исполнитель предоставляет Заказчику код страницы блокировки под свободной лицензией *MIT License*. Заказчик размещает на своем выделенном домене страницу блокировки и настраивает перенаправление на нее, указывая в качестве параметра блокируемый URL (пример использования такого сервиса - <http://blocked.digincore.com/?url=google.com>).

После ввода пользователем CAPTCHA и email (по желанию), домен попадает на экспертную оценку специалистам Digincore.

По факту оценки экспертами на указанный пользователем адрес высылается письмо о результатах проверки и, в случае смены категории сайта, изменения сразу же вносятся в ближайшее обновление блэклистов (выгрузка происходит с 11:00 до 14:00 (GMT+3) в соответствии с [Техническим регламентом](#)). В случае, если месячная квота на экспертную проверку исчерпана, возможно либо блокирование этой функциональности до наступления следующего учетного месяца оказания услуг, либо активация платной услуги по экспертной оценке.

### Развертывание и настройка решения

Страница блокировки написана на PHP. Актуальная версия страницы блокировки - 3.0.1. Требования к серверу обеспечивающему функционирование страницы блокировки:

- PHP 5.3.10 с использованием Zend Framework 2.2.2. и выше;
- Apache 2.2 и выше.

В конфигурационный файл `/config/digincore.config.php` необходимо внести следующие изменения:

- параметр `userId` - внести действующий Ключ Пользователя (выдается

- при заключении договора);
- параметр urlAPI - изменить адрес тестового API на рабочий (<https://digincore.com/api/json.test.php> на <https://digincore.com/api/json.php>).

IP-адрес сервера, где размещена страница блокировки должен быть сообщен в службу поддержки Digincore ([support@digincore.com](mailto:support@digincore.com)). Запросы с неавторизованных IP-адресов *блокируются* системой безопасности!

Редактирование содержания страницы осуществляется посредством изменения следующих файлов:

- /module/Application/view/layout/layout.phtml - общий вид страницы;
- /module/Application/view/application/index/index.phtml - форма ввода каптчи, email пользователя;
- /module/Application/view/application/index/noturl.phtml - выдача сообщения об ошибке (отсутствует, либо пустой передаваемый параметр url);
- /module/Application/view/application/index/send.phtml - ответ на отправленный пользователем запрос.
- /public/css/ - используемые CSS;
- /public/img/ - используемые картинки.

#### **Настройка перенаправления в squidGuard 1.4.**

Для перенаправления заблокированного ресурса на страницу блокировки (например, blocked.mysite.com) необходимо проделать следующие шаги:

- внести белый список squidGuard (while list) домен страницы блокировки;
- настроить список контроля доступа (acl) с указанием, куда будет происходить редирект;
- создать (или отредактировать) файл /var/www/blocked.php

#### 1. Настройка белого списка (white list):

- а. в домашней директории баз squidGuard (в файле конфигурации она хранится в переменной *dbhome*) создаем файл со списком ресурсов, которые мы хотим посещать независимо от блокируемого списка доменов и вносим в него:

*blocked.mysite.com*

Прим.: так же необходимо ввести список ip-адресов из локальной сети, потому что если в настройках squid3 выключена возможность обойти прокси введением ip-адреса ресурса (*url\_rewrite\_bypass off*), то вы не сможете попасть на компьютеры локальной сети.

- б. в файле конфигурации squidGuard (/etc/squid/squidGuard.conf) настраиваем ресурс, в который мы пропишем путь до только что созданного файла белого списка

```
dest white_dest {
    domainlist    digincore/white
```

- }
2. Настраиваем перенаправление заблокированного ресурса на страницу блокировки.

- a. в конфигурационном файле squidGuard необходимо настроить список контроля доступа (acl), в котором мы укажем, какие из уже созданных нами ресурсов проверять по блэклисту, а какие нет. В нем же указывается путь до страницы, на которую мы хотим перенаправлять запросы на заблокированные домены:

```
#
# ACL RULES:
#
acl {
    default {
        pass white_dest !digincore_bl !lin-addr all
        redirect http://localhost/blocked.php?u=%u
    }
}
```

Как видно из примера, squidGuard теперь будет пропускать все домены из белого списка (white в параметре pass) и блокировать содержание доменов, находящихся в нашем блэклисте (!digincore\_bl). Также, ему указано блокировать доступ по ip-адресу (!lin-addr). В самом конце разрешается доступ ко всем остальным доменам (all).

Ниже в параметре redirect указываем путь, куда мы хотим перенаправить запросы к заблокированному контенту. Здесь можно указать любой ресурс на ваше усмотрение, в нашем случае указан файл /var/www/blocked.php с входящим параметром в который мы передаем url (про параметр %u подробнее смотрите на <http://www.squidguard.org/Doc/redirect.html>) на который пытается зайти пользователь.

- b. создаем файл /var/www/blocked.php со следующим содержанием

```
<?php
    header("Location: http://blocked.mysite.com/?url=".$_GET['u']);
?>
```

Что проделывает данный скрипт: он получает введенный в качестве параметра запроса url (\$\_GET['u']) и подставляет его в качестве параметра в страницу финального назначения (<http://blocked.mysite.com/?url=>), куда и происходит редирект.

3. Перезапускаем squidGuard и squid3:

```
squidGuard -d -C all
/etc/init.d/squid3 restart
```

Прим.: Вышеописанные манипуляции необходимы для того, чтобы страница финального редиректа отображалась корректно в браузере пользователя. При прямом редиректе, т.е. если в настройках acl вместо

'redirect <http://localhost/blocked.php?u=%u>'

указать

'redirect <http://blocked.mysite.com/?domain=%u>'

то в адресной строке браузера по прежнему будет находится изначально запрашиваемый адрес сайта, а не blocked.mysite.com, что приведет к некорректному отображению картинок и непредсказуемой работе функционала страницы.

В случае, описанном нами в пункте 2.b, браузеру будет предоставлен новый адрес и отображение финальной страницы будет корректным.

Например, при попытке зайти на ресурс sex.com, в адресной строке браузера появится следующая ссылка <http://blocked.mysite.com/?url=http://sex.com/>

### **Документация и поддержка**

- Технический регламент оказания услуг (форматы и сроки выкладки блэклистов, сроки обработки запросов к Digincore API):  
<https://digincore.com/uslugi-i-servisy/tehnicheskij-reglament-na-okazanie-uslug>
- Общее описание Digincore API:  
<https://digincore.com/uslugi-i-servisy/digincore-api>
- Документация по использованию Digincore API:  
<https://digincore.com/uslugi-i-servisy/digincore-api/dokumentatsiya-po-ispolzovaniyu-digincore-api>
- Тестовый веб-интерфейс проверки json-запросов к Digincore API:  
<https://digincore.com/api/json.test.html>
- Рабочий Digincore API:  
<https://digincore.com/api/json.php>

Техническая и консультационная поддержка решения осуществляется командой Digincore.com: [support@digincore.com](mailto:support@digincore.com)

Контактное лицо: Ирисов Евгений, тел: +7-912-851-7281, skype: eugene\_irisov