Тел.: (495) 363-37-53; (4012) 51-05-64; e-mail: info@1c-bitrix.ru, http://www.1c-bitrix.ru

1С-Битрикс: Управление сайтом

Руководство по настройке модуля

Проактивная защита

Содержание

Введение

Одной из первостепенных задач для владельцев веб-проектов является качественная и надежная защита от хакерских атак, взлома и кражи хранящейся на сайте информации. Для этого в системах *"1С-Битрикс: Управление сайтом"* и *"1С-Битрикс: Корпоративный портал"* предусмотрен модуль **Проактивная защита**, с помощью которого реализуется целый комплекс защитных мероприятий для сайта и сторонних приложений.

Уровень защиты, обеспечиваемый стандартными сборками дистрибутивов *"1С-Битрикс: Управление сайтом"* и *"1С-Битрикс: Корпоративный портал"*, достаточно высок. Но во время реализации проектов на основе *"1С-Битрикс: Управление сайтом"* и *"1С-Битрикс: Корпоративный портал"* выполняется кастомизация компонентов, дописываются собственные инструменты, безопасность которых не всегда проверяется. Модуль **Проактивная защита** является важным дополнением к стандартной политике безопасности продукта и существенно повышает уровень защиты веб-проекта.

В документе рассматриваются основные операции по настройке модуля **Проактивная защита**. Руководство предназначено для администраторов *"1С-Битрикс: Управление сайтом"* и *"1С-Битрикс: Корпоративный портал"* и подготовленных специалистов по информационной безопасности.

Что такое проактивная защита?

Проактивная защита – это комплекс технических и организационных мер, которые объединены общей концепцией безопасности и позволяют значительно расширить понятие защищенности и реакции веб-приложений на угрозы.

Понятие проактивной защиты веб-проекта объединяет в себе следующее:

- надежную аутентификацию пользователя с использованием одноразовых паролей;
- технологию защиты сессии пользователя;
- проактивный фильтр защиты от атак;
- контроль целостности системы;
- защиту от фишинга;
- шифрование данных.

Глава 1. Настройка проактивной защиты

Любой веб-проект на базе **Bitrix Framework** обязательно имеет начальный уровень защиты. Повысить этот уровень можно с помощью модуля **Проактивная защита**, настроив один из следующих уровней безопасности:

- стандартный;
- высокий;
- повышенный.

Причем для уровней справедливо понятие «вложенности». Т.е., чтобы настроить защиту сайта на высоком уровне, необходимо сначала настроить стандартный уровень защиты, а затем настроить все параметры высокого уровня. Соответственно, чтобы настроить защиту на повышенном уровне, необходимо настроить высокий уровень защиты, а затем настроить параметры повышенного уровня.

Информация о текущем уровне безопасности сайта представлена на странице **Панель безопасности** (*Настройки > Проактивная защита > Панель безопасности*) (Рис. 1.1). Для каждого уровня приведена соответствующая таблица параметров и их значений, а также указаны, в случае необходимости, рекомендации по изменению значений параметров.

Текущий уровень безопасности: Стандартный.

Уровень безопасности: Стандартный

Параметр	Значение	Рекомендации
Проактивный фильтр (Web Application Firewall)	Включен	
Исключения проактивного фильтра	Нет	
Журнал вторжений за последние 7 дней	8	Просмотреть записи
Контроль активности	Включен	
Уровень безопасности группы администраторов	Повышенный	
Использовать CAPTCHA при регистрации	Да	
Режим вывода ошибок (error_reporting):	Только ошибки	
Показ ошибочных запросов базы данных	Выключен	

Уровень безопасности: Высокий

Параметр	Значение	Рекомендации
Журналирование событий главного модуля	Не все включены	Включить
Защита административной части	Выключена	Включить
Хранение сессий в базе данных	Выключено	Включить
Смена идентификатора сессий	Выключена	Включить
Защита редиректов от фишинга	Выключена	Включить

Уровень безопасности: Повышенный

Параметр	Значение	Рекомендации
Одноразовые пароли	Выключены	Включить
Контроль целостности	Никогда не выполнялся	Выполнить
Веб-антивирус	Включен	
Действия при обнаружении вируса	Только оповещение	Включить вырезание
Исключения веб-антивируса	Нет	
Журнал заражений за последние 7 дней	0	

Рис. 1.1 Панель безопасности

Если для какого-то параметра установлено несоответствующее значение, то в поле **Рекомендации** будет отображено необходимое для выполнения действие.

Стандартный уровень безопасности

Для того чтобы защита веб-проекта осуществлялась на стандартном уровне безопасности, необходимо настроить должным образом все параметры данного уровня (Рис. 1.2).

Уровень безопасности: Стандартный

Параметр	Значение	Рекомендации
Проактивный фильтр (Web Application Firewall)	Включен	
Исключения проактивного фильтра	Нет	
Журнал вторжений за последние 7 дней	0	
Контроль активности	Включен	
Уровень безопасности группы администраторов	Повышенный	
Использовать CAPTCHA при регистрации	Да	
Режим вывода ошибок (error_reporting):	Только ошибки	
Показ ошибочных запросов базы данных	Выключен	

Рис. 1.2 Параметры стандартного уровня безопасности

⚠ ***Примечание:*** *если стандартный уровень не настроен полностью, то защита сайта будет осуществляться на* ***начальном*** *уровне, но с учетом настроенных параметров на стандартном, высоком и повышенном уровнях.*

Проактивный фильтр и исключения из него

Проактивный фильтр (**Web Application Firewall**) – это набор специализированных средств, которые выполняют фильтрацию трафика. Фильтр обеспечивает защиту от большинства известных атак на веб-приложения. В потоке внешних запросов пользователей проактивный фильтр распознает большинство опасных угроз и блокирует вторжения на сайт.

Включение или отключение проактивного фильтра выполняется на странице **Проактивный фильтр** (*Настройки* > *Проактивная защита* > *Проактивный фильтр*) с помощью кнопки **Включить проактивную защиту** (или **Отключить проактивную защиту**) (Рис. 1.3).

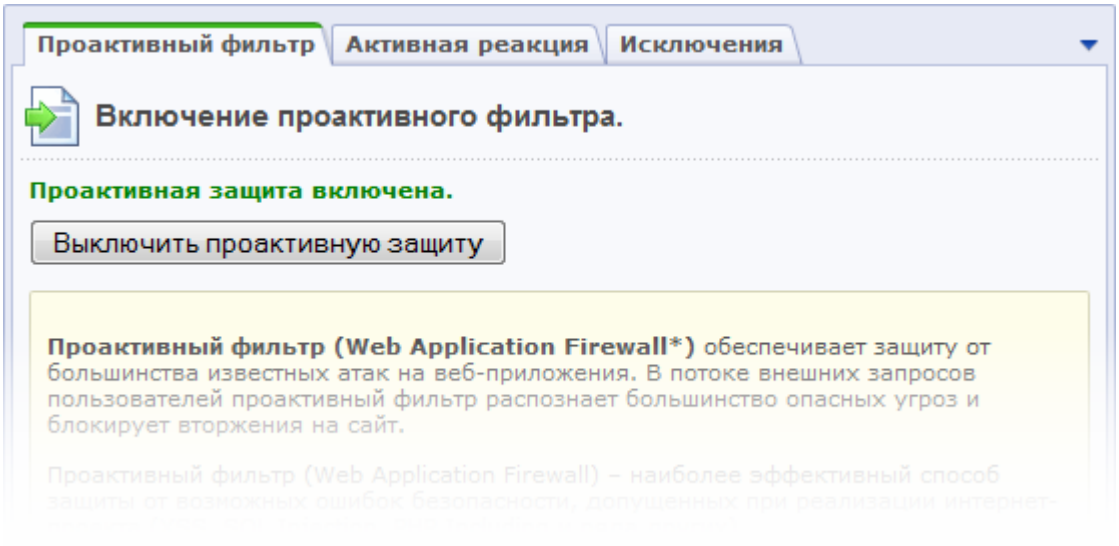

Рис. 1.3 Проактивный фильтр

При необходимости могут быть заданы исключения из проактивного фильтра (закладка **Исключения**), т.е. проактивный фильтр не будет применяться на страницах, указанных на данной закладке.

⚠ ***Примечание:*** *для того чтобы защита сайта осуществлялась на стандартном уровне, проактивный фильтр должен быть включен и не должно быть задано ни одного исключения.*

На закладке **Активная реакция** (Рис. 1.4) настраиваются действия системы при попытке вторжения на сайт:

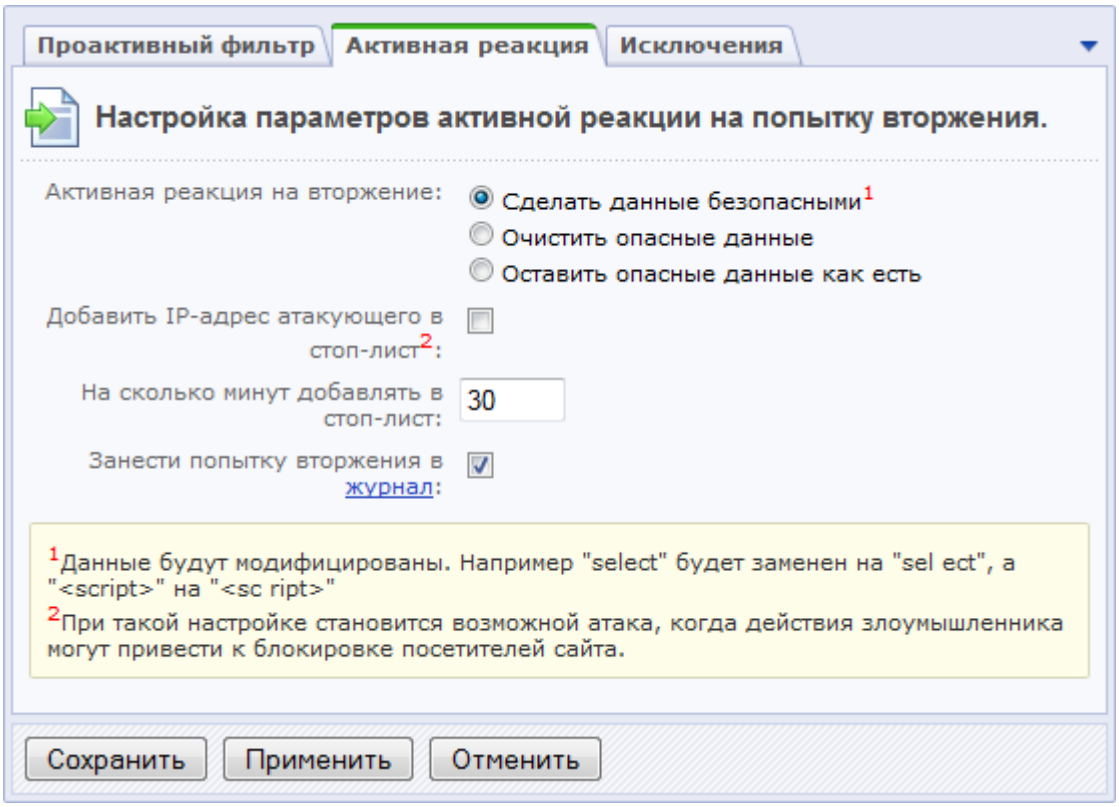

Рис. 1.4 Параметры активной реакции на вторжение

- Выберите необходимый вам способ реакции на вторжение:
  - **Сделать данные безопасными** – опасные данные будут модифицированы (например, **select** будет заменен на **sel ect**).
  - **Очистить опасные данные** – введенные опасные данные будут удалены.
  - **Оставить опасные данные как есть** – с опасными данными никаких действий выполняться не будет.
- Чтобы заблокировать пользователя на некоторое количество минут, отметьте опцию **Добавить IP-адрес атакующего в стоп-лист**. При этом период времени блокировки задается в поле **На сколько минут добавлять в стоп-лист**.

  ⚠ ***Примечание:*** *при настройке параметров добавления IP-адреса атакующего в стоп-лист становится возможной атака, когда действия злоумышленника могут привести к блокировке посетителей сайта.*

- Для фиксирования попыток атаки отметьте опцию **Занести попытку вторжения в журнал**.

⚠ ***Обратите внимание,*** *что некоторые действия пользователей, не представляющие угрозы, тоже могут выглядеть подозрительно и вызывать ложное срабатывание фильтра.*

⚠ ***Примечание:*** *проактивный фильтр не работает для тех групп пользователей, для которых в правах доступа к модулю* ***Проактивная защита*** *разрешена операция* ***Обход проактивного фильтра*** *(см. уровни доступа к модулю* ***Проактивная защита****) (Рис. 1.5).*

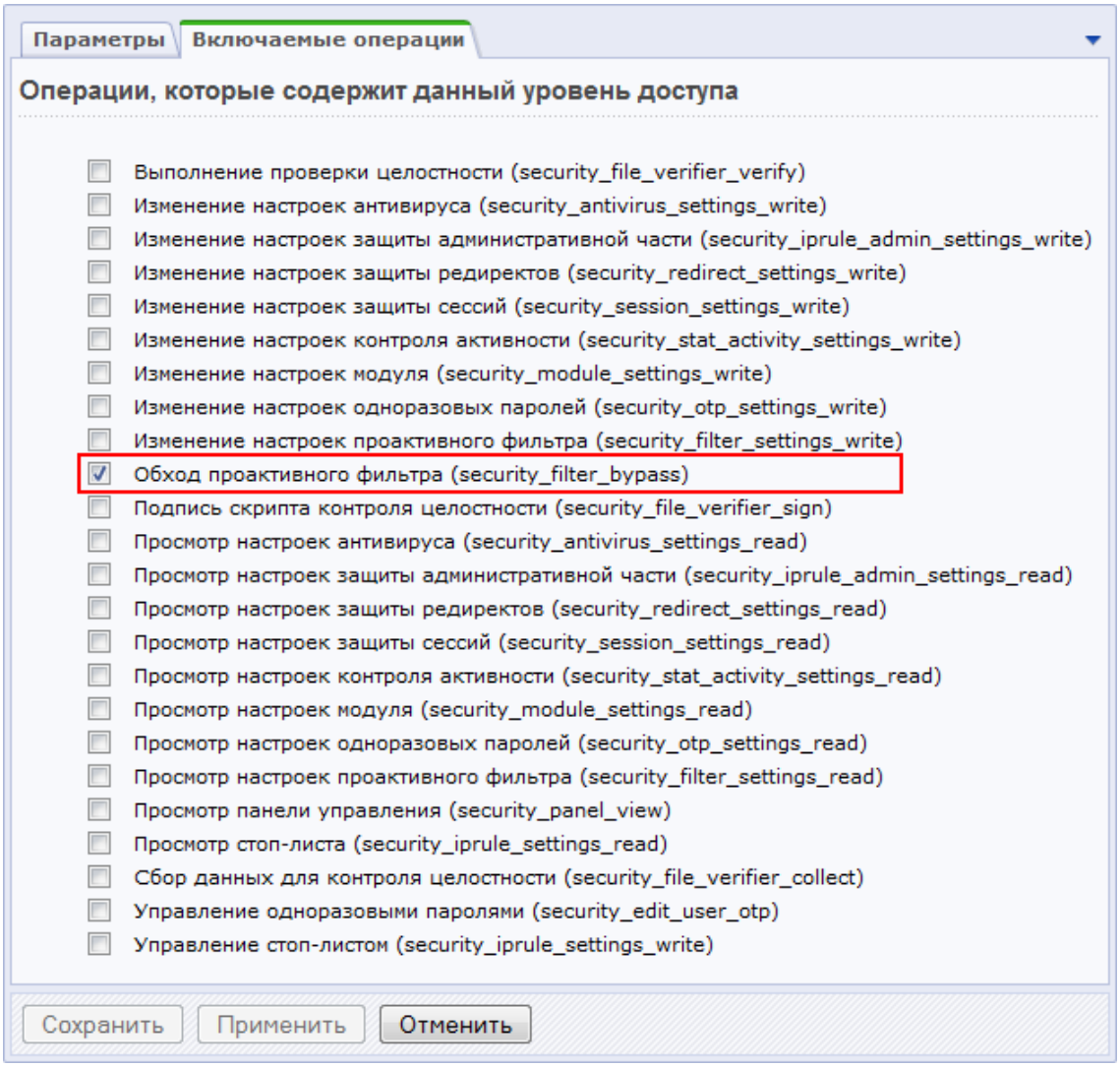

Рис. 1.5 Включаемые операции уровня доступа к модулю Проактивная защита

Журнал вторжений

Журнал вторжений (*Настройки* > *Проактивная защита* > *Журнал вторжений*) (Рис. 1.6) предназначен для ведения логов событий, связанных с потенциальными угрозами для безопасности сайта. Период времени, в течение которого хранятся записи, определяется настройками **Главного модуля** на закладке **Журнал событий**.

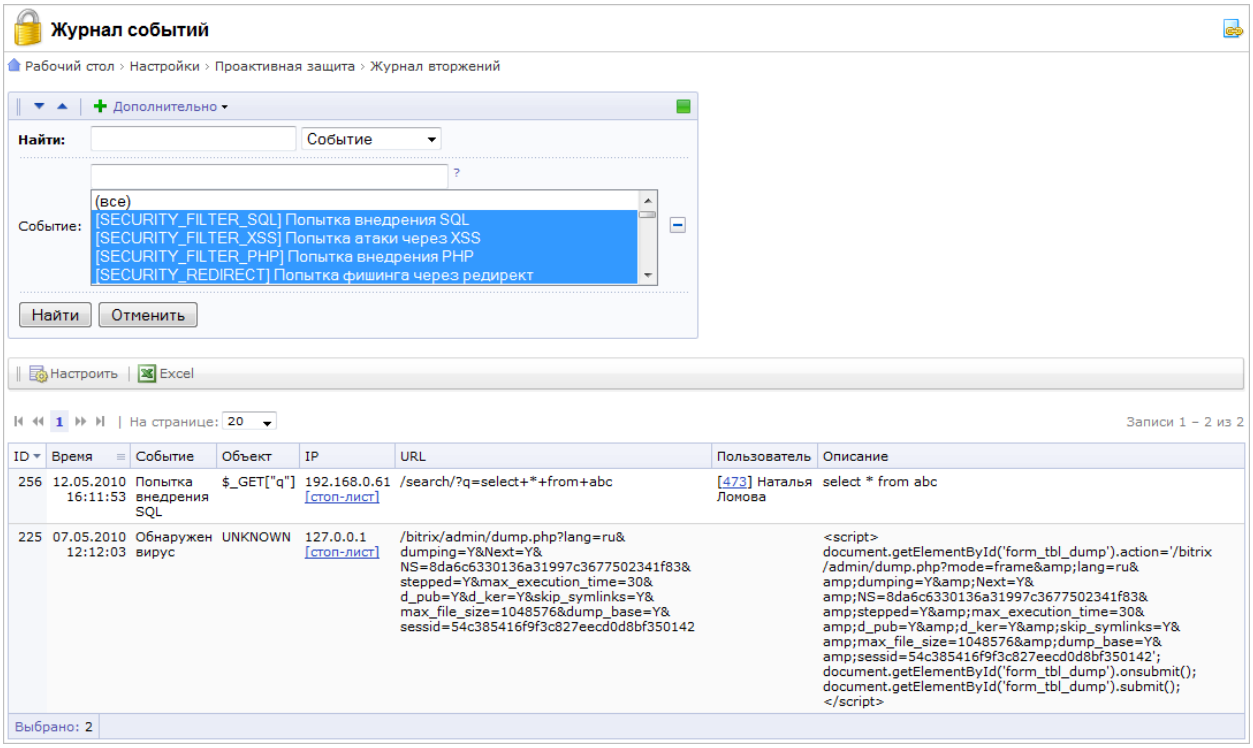

Рис. 1.6 Журнал вторжений

В журнале представлена следующая информация о событии:

- дата и время события;
- название произошедшего события;
- объект события;
- IP-адрес, с которого производилась атака. По ссылке **[стоп-лист]** можно добавить адрес в стоп-лист модуля **Веб-аналитика**.
- URL страницы, на которой выполнялось вторжение;
- имя пользователя, если событие было выполнено зарегистрированным пользователем или идентификатор гостя (при наличии модуля **Веб-аналитика**);
- описание события;
- срочность (**SECURITY** или **WARNING**);
- источник события;
- используемый **User Agent**;
- сайт, на котором произошло событие.

В журнале фиксируются события следующих типов:

- Со стороны модуля **Веб-аналитика**: превышение лимита активности.
- Со стороны модуля **Проактивная защита**: попытки внедрения SQL и PHP, попытки атак через XSS, попытки заражения вирусами и фишинга через редирект.
- Со стороны модуля **Форум**: операции над темами и сообщениями форумов.
- Со стороны **Главного модуля**: успешный вход и выход из системы, запрос на смену и смена пароля пользователя, ошибки входа и входа при сохраненной авторизации, регистрация нового пользователя, ошибка регистрации и удаление пользователя.

Контроль активности

Контроль активности пользователей ведется на основе средств модуля **Веб-аналитика** и, следовательно, доступен только в тех редакция продукта, в которые входит этот модуль. Контроль активности позволяет установить защиту от чрезмерно активных пользователей, программных роботов, некоторых категорий DDoS-атак, а также отсекать попытки подбора паролей перебором.

Включение или отключение контроля активности выполняется на странице **Контроль активности** (*Настройки* > *Проактивная защита* > *Контроль активности*) с помощью кнопки **Включить контроль активности** (или **Выключить контроль активности**) (Рис. 1.7):

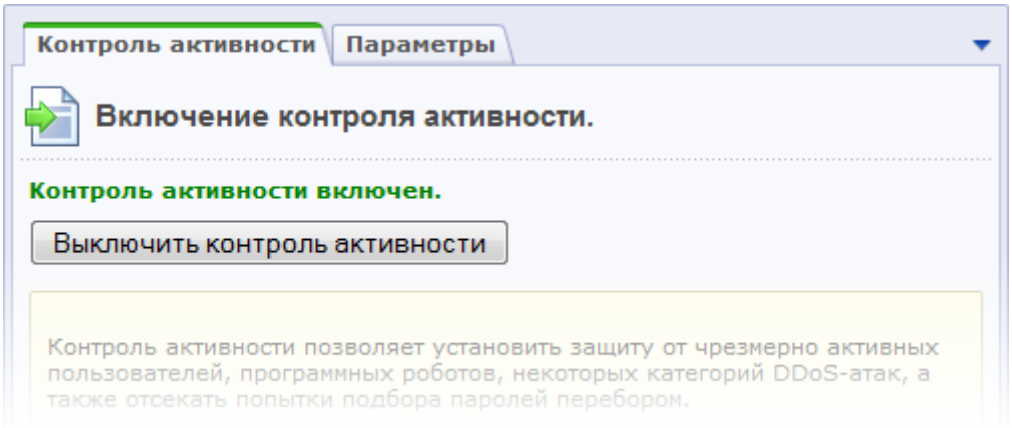

Рис. 1.7 Контроль активности

На закладке **Параметры** задаются параметры максимальной активности пользователей вашего сайта (Рис. 1.8).

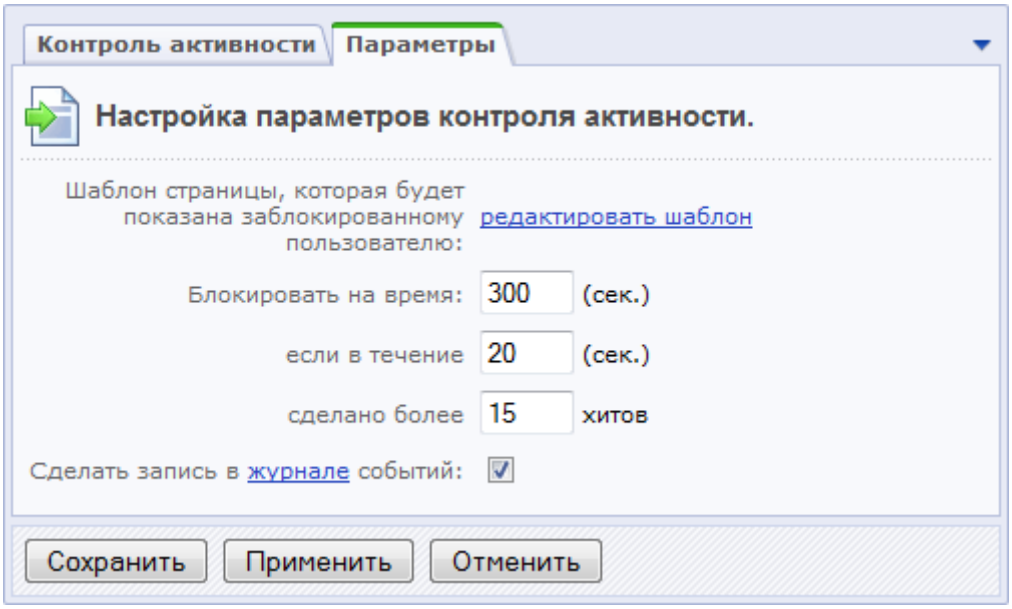

Рис. 1.8 Настройка параметров контроля активности

Таким образом, если пользователь превысит количество запросов за указанное количество секунд, то он будет заблокирован на заданное время. При этом ему будет отображена специальная страница, шаблон которой можно отредактировать по ссылке

редактировать шаблон. Для фиксирования превышения лимита активности в журнале вторжений необходимо отметить опцию **Сделать запись в журнале событий**.

⚠ ***Примечание:*** *для того чтобы защита сайта осуществлялась на стандартном уровне, контроль активности должен быть включен.*

Уровень безопасности группы администраторов

Чтобы защита веб-проекта осуществлялась на стандартном уровне, необходимо задать повышенный уровень безопасности для группы администраторов. По умолчанию данный параметр уже настроен. Если по каким-либо причинам уровень безопасности группы администраторов отличается от повышенного, то необходимо выполнить следующее:

- На странице **Панель безопасности** (*Настройки > Проактивная защита > Панель безопасности*) нажмите ссылку **Включить повышенный**. Откроется форма редактирования группы на закладке **Безопасность** (Рис. 1.9).

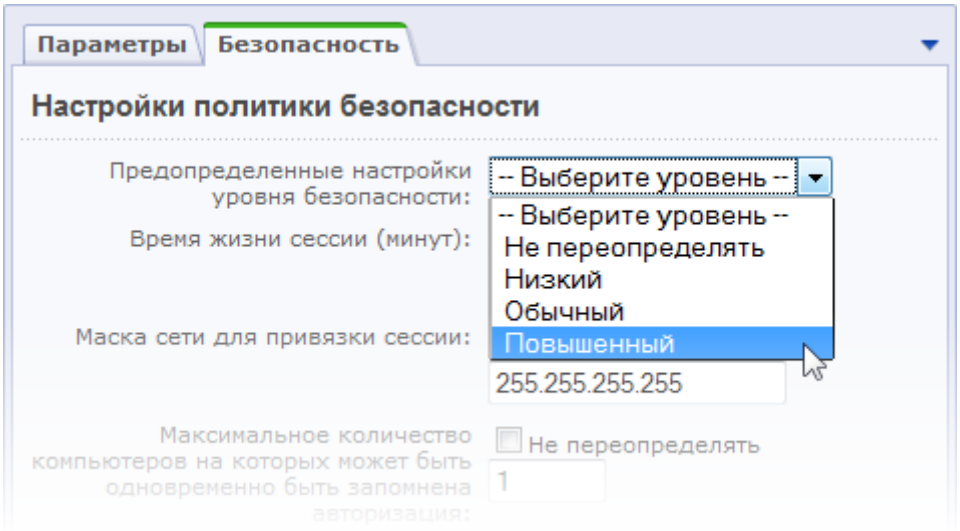

Рис. 1.9 Настройка уровня безопасности группы

- В поле **Предопределенные настройки уровня безопасности** укажите **Повышенный** уровень.
- Сохраните внесенные изменения.

Использовать CAPTCHA при регистрации

Необходимым условием для защиты сайта на стандартном уровне является использование **CAPTCHA** при регистрации новых пользователей. Данная опция включается в настройках главного модуля на закладке **Авторизация** (Рис. 1.10):

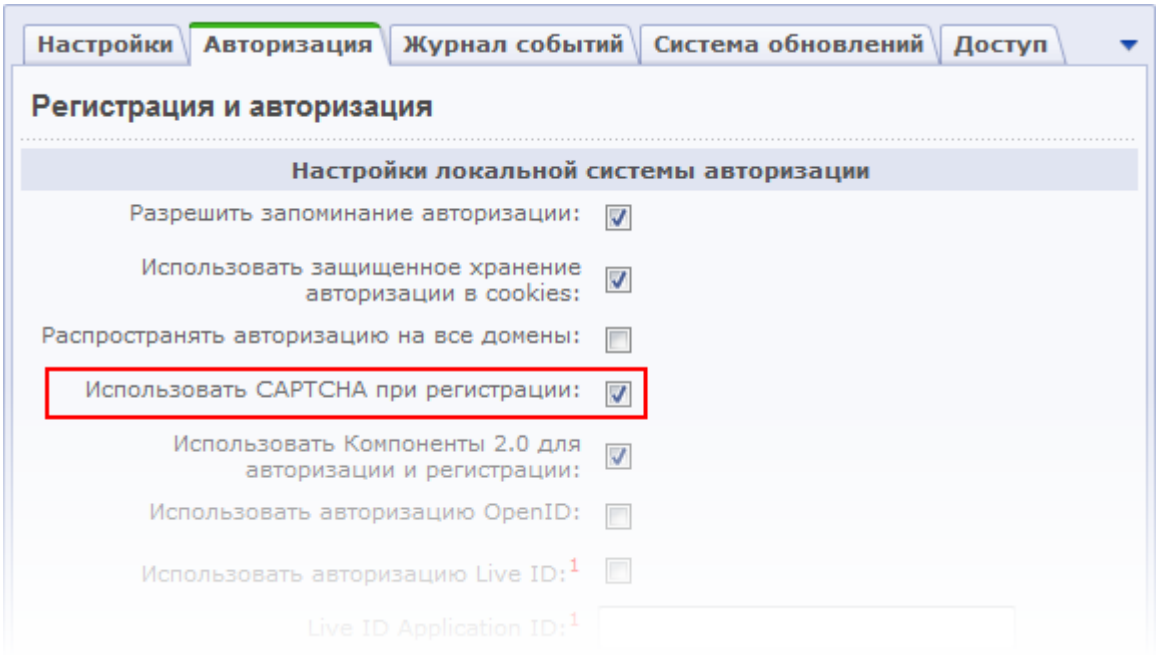

Рис. 1.10 Настройка использования CAPTCHA при регистрации

Настройка внешнего вида **CAPTCHA** выполняется на странице **CAPTCHA** (*Настройки* > *Настройки продукта* > *CAPTCHA*).

Режим вывода ошибок

Наряду с параметром **Использовать CAPTCHA при регистрации**, необходимо настроить еще один параметр главного модуля – **Режим вывода ошибок (error_reporting)**, чтобы защита сайта осуществлялась на стандартном уровне безопасности.

- Перейдите на страницу настроек **Главного модуля** (*Настройки* > *Настройки продукта* > *Настройки модулей* > *Главный модуль*).
- В поле **Режим вывода ошибок (error_reporting)** укажите **Только ошибки** или **Не выводить** (Рис. 1.11).

⚠ ***Примечание:*** *если выбрать режим* ***Ошибки и предупреждения****, то будет установлен начальный уровень безопасности.*

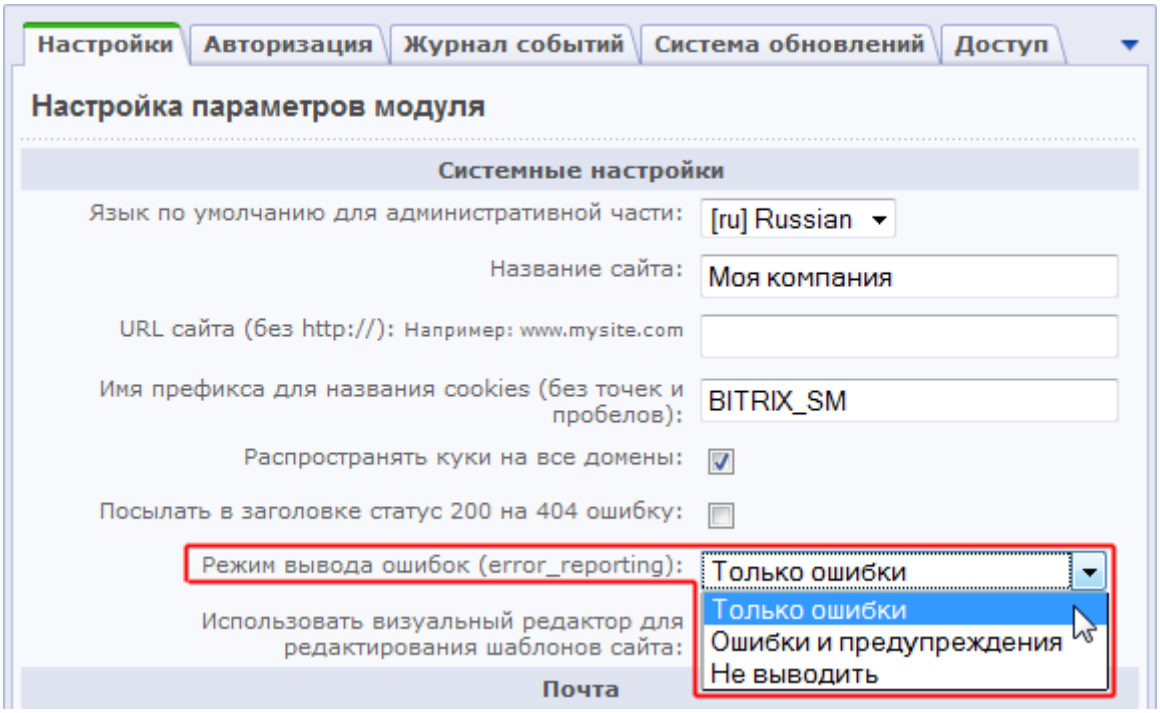

Рис. 1.11 Настройка режима вывода ошибок

- Сохраните внесенные изменения.

Показ ошибочных запросов базы данных

Для осуществления защиты веб-проекта на стандартном уровне показ ошибочных данных должен быть выключен, т.е. переменная **$DBDebug** должна принимать значение **false**. Таким образом, в случае ошибки при создании соединения с базой или выполнения запроса полный текст ошибки будет отображаться только администраторам сайта. Если же переменная принимает значение **true**, то полный текст ошибки будет отображаться всем пользователям сайта.

Изменение значения переменной **$DBDebug** выполняется в файле **/bitrix/php_interface/dbconn.php**.

Высокий уровень безопасности

Для того чтобы защита веб-проекта осуществлялась на высоком уровне безопасности, сначала необходимо настроить стандартный уровень безопасности, а затем выполнить настройку параметров для высокого уровня (Рис. 1.12).

Уровень безопасности: Высокий

Параметр	Значение	Рекомендации
Журналирование событий главного модуля	Все включены	
Защита административной части	Включена	
Хранение сессий в базе данных	Включено	
Смена идентификатора сессий	Включена	
Защита редиректов от фишинга	Включена	

Рис. 1.12 Параметры высокого уровня безопасности

⚠ ***Примечание:*** *если некоторые параметры высокого уровня безопасности принимают несоответствующие значения, то защита сайта будет осуществляться на* ***стандартном*** *или* ***начальном*** *(если настроены не все параметры стандартного уровня) уровне, но с учетом настроенных параметров на стандартном, высоком и повышенном уровнях.*

Журналирование событий главного модуля

Параметр **Журналирование событий главного модуля** подразумевает целый ряд настроек **Главного модуля** (*Настройки > Настройки продукта > Настройки модулей > Главный модуль*) (Рис. 1.13):

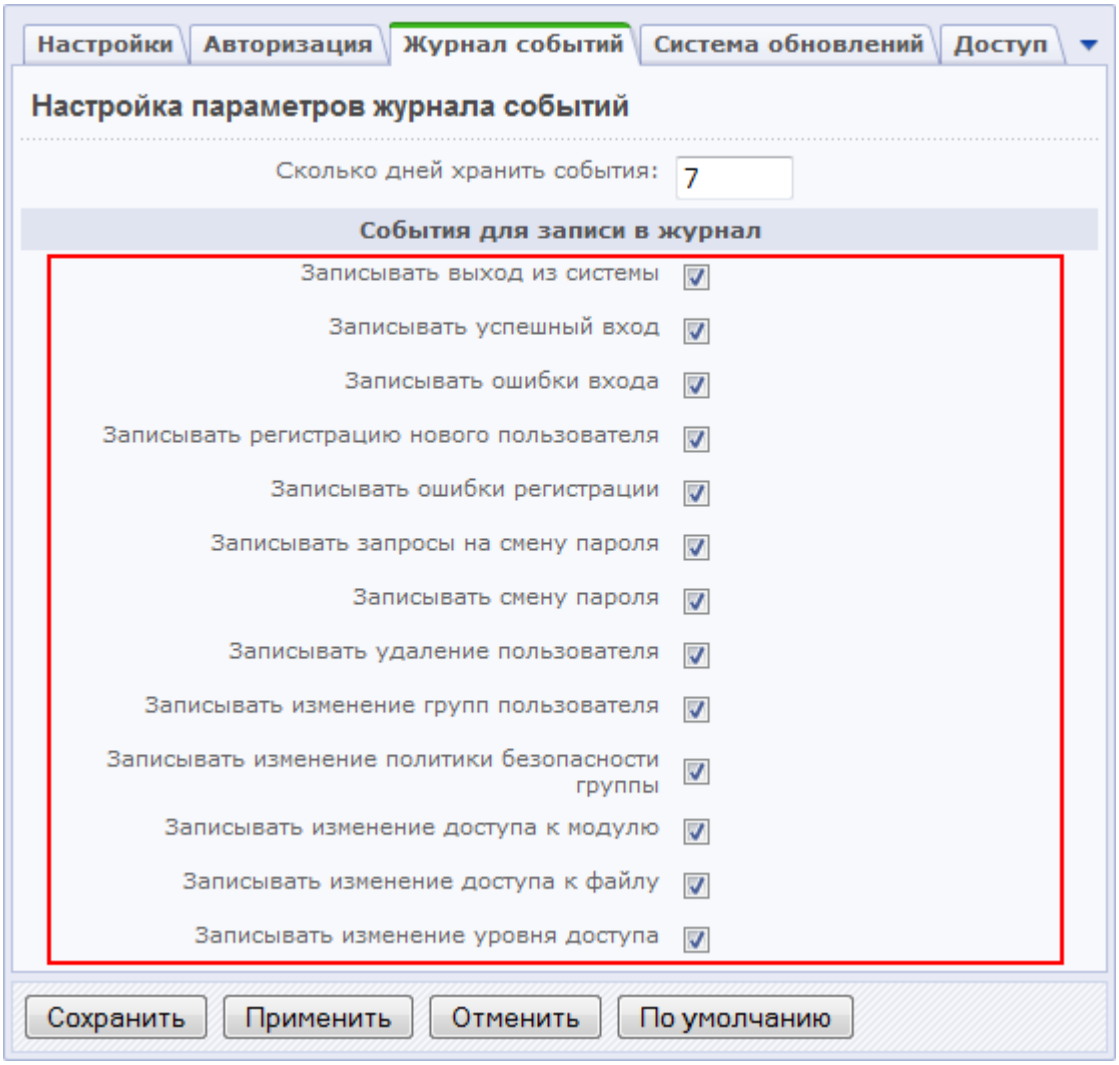

Рис. 1.13 Настройка журналирования событий

Чтобы защита сайта велась на высоком уровне, должны быть отмечены следующие события:

- Записывать выход из системы;
- Записывать успешный вход;
- Записывать ошибки входа;
- Записывать регистрацию нового пользователя;
- Записывать ошибки регистрации;
- Записывать запросы на смену пароля;
- Записывать смену пароля;
- Записывать удаление пользователя;
- Записывать изменение групп пользователя;
- Записывать изменение политики безопасности группы;
- Записывать изменение доступа к модулю;
- Записывать изменение доступа к файлу;
- Записывать изменение уровня доступа.

Даже если не будет отмечена только одна из вышеперечисленных обязательных опций, то считается, что параметр **Журналирование событий главного модуля** принимает несоответствующее значение, и защита сайта будет осуществляться на стандартном (или начальном) уровне безопасности.

Защита административной части

Защита административной части сайта осуществляется с помощью ограничения доступа со всех, кроме указанных в настройках IP-адресов. Включение или отключение защиты выполняется на странице **Защита административного раздела** (*Настройки > Проактивная защита > Защита административного раздела*) с помощью кнопки **Включить защиту** (или **Выключить защиту**) (Рис. 1.14).

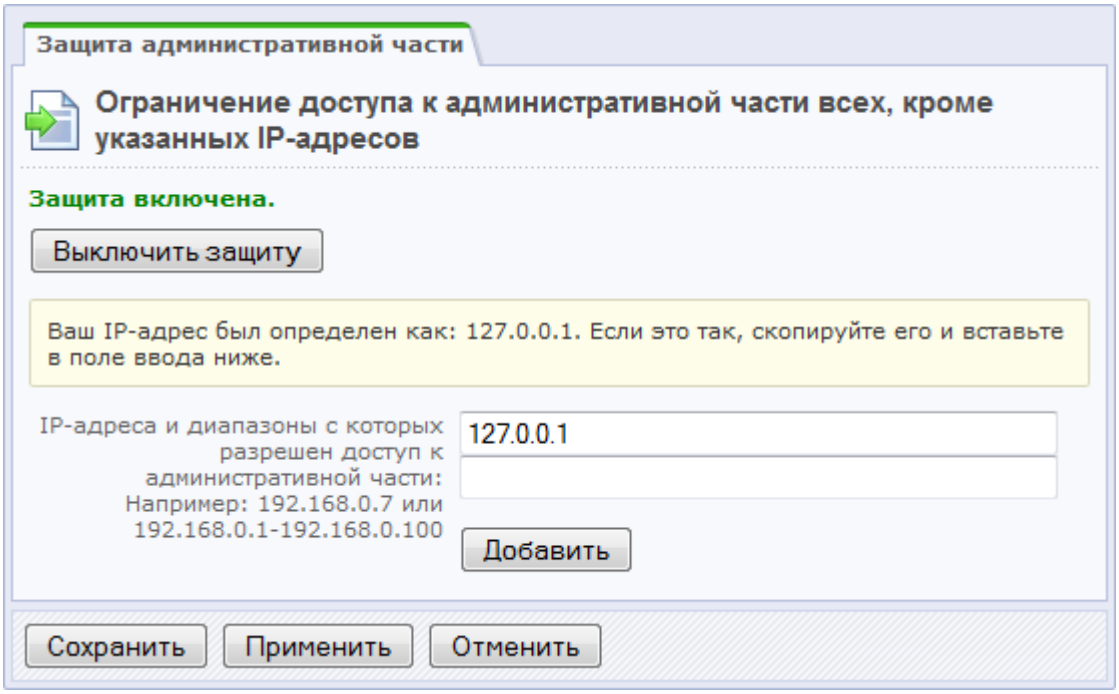

Рис. 1.14 Защита административного раздела

⚠ ***Внимание:*** *перед включением защиты административной части необходимо внести в список* ***IP-адреса и диапазоны, с которых разрешен доступ к административной части*** *свой IP-адрес и дополнительные адреса (или диапазоны), с которых разрешен доступ.*

⚠ ***Примечание:*** *чтобы защита вашего веб-проекта осуществлялась на высоком уровне, защита административного раздела должна быть включена.*

⚠ ***Примечание:*** *снять ограничение по IP-адресам можно посредством создания специального файла, путь к которому задается в настройках модуля* ***Проактивная защита*** *(Рис. 1.15). По умолчанию файл имеет имя следующего формата:* ***ipcheck_disable_<случайный_набор_из_32_символов>****.*

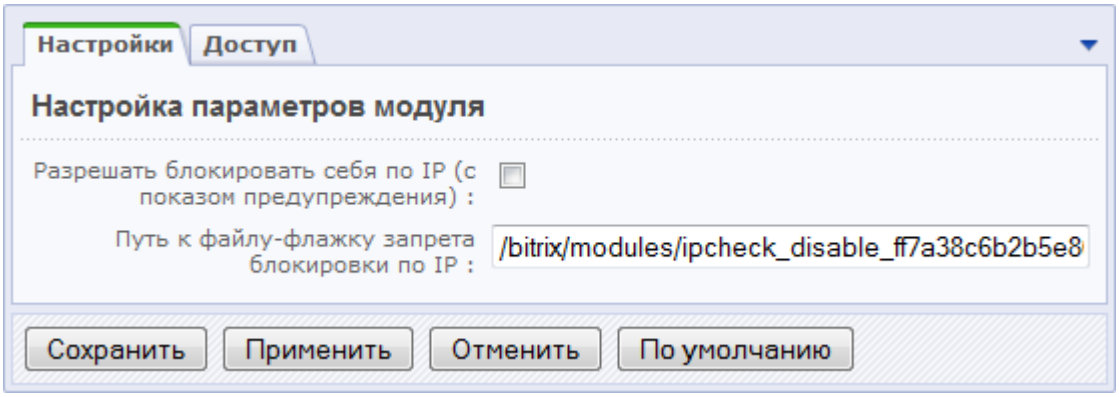

Рис. 1.15 Настройки модуля Проактивная защита

Хранение сессий и смена идентификатора

Сессия пользователя - это ключевой объект атаки на веб-сайт с целью похищения сессии авторизованного пользователя и в особенности администратора. В базовой поставке продукта защита сессий настраивается в политике безопасности каждой группы пользователей с помощью параметров:

- Время жизни сессии (минут);
- Маска сети для привязки сессии.

Но такие строгие настройки не всегда получается ввести, например в силу того, что пользователи могут работать с разных IP-адресов. Модуль **Проактивная защита** позволяет выполнить защиту сессий с помощью следующих инструментов:

- хранение сессий в базе данных модуля безопасности;
- смена идентификатора сессий через указанное время.

Включение (или отключение) механизма хранения данных сессий пользователей в базе данных выполняется на странице **Защита сессий** (*Настройки* > *Проактивная защита* > *Защита сессий*) с помощью кнопки **Включить хранение данных сессий в БД модуля** (или **Отключить хранение данных сессий в БД модуля**) (Рис. 1.16).

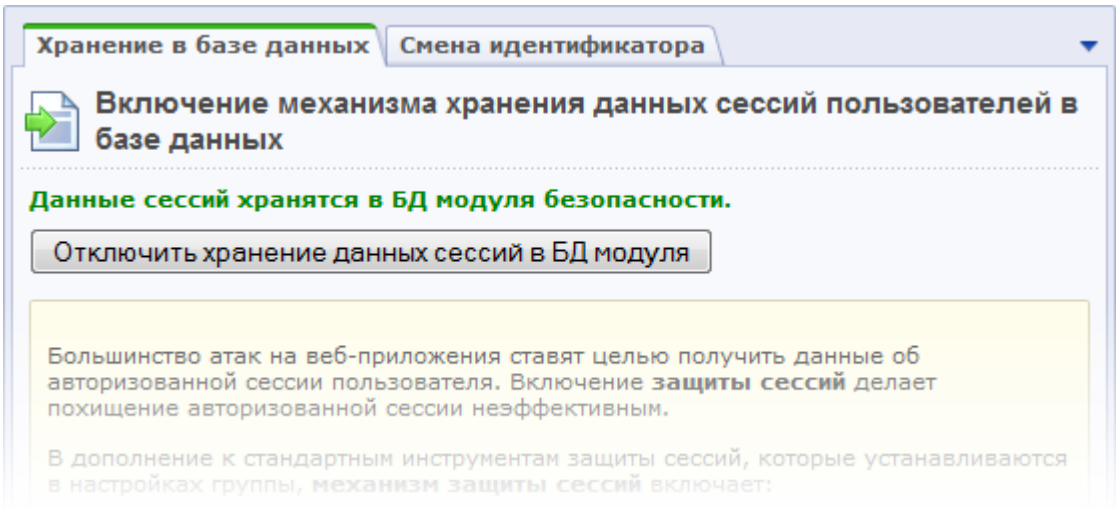

Рис. 1.16 Хранение сессий в базе данных модуля

Хранение данных сессий в таблице модуля **Проактивная защита** позволяет избежать чтения этих данных через скрипты других виртуальных серверов, исключив ошибки конфигурирования виртуального хостинга, ошибки настройки прав доступа во временных каталогах и ряд других проблем настройки операционной среды. Кроме того, это разгружает файловую систему, перенося нагрузку на сервер базы данных.

⚠ ***Внимание!*** *При переключении режима хранения сессий все пользователи потеряют авторизацию (данные сессий будут уничтожены).*

Настройка механизма смены идентификатора сессий выполняется на закладке **Смена идентификатора** формы настройки защиты сессий (Рис. 1.17).

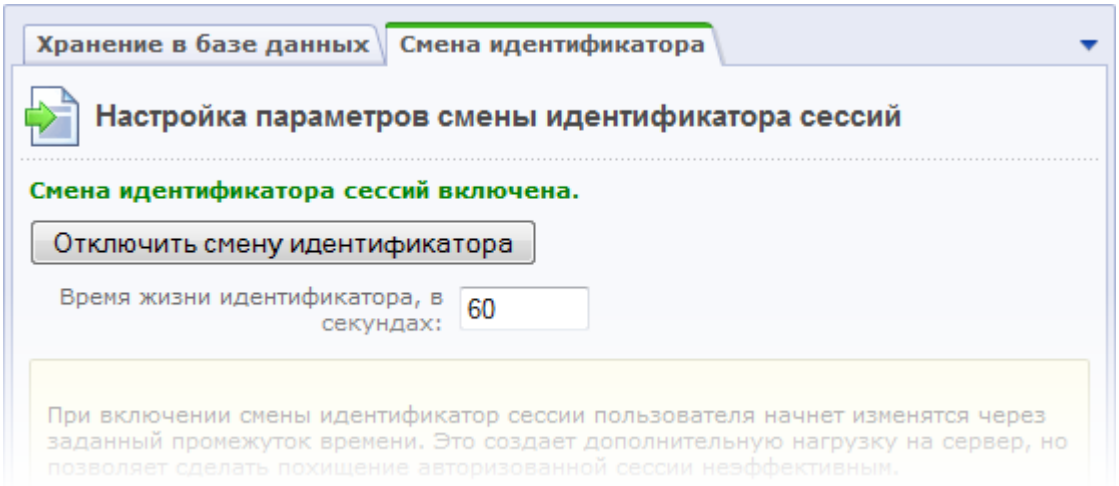

Рис. 1.17 Смена идентификатора сессий

Чтобы выполнялась смена идентификатора, необходимо:

- указать **Время жизни идентификатора, в секундах**, т.е. через какой промежуток времени будет измениться идентификатор сессий;
- Нажать кнопку **Включить смену идентификатора**.

Смена идентификатора создает дополнительную нагрузку на сервер, но позволяет сделать похищение авторизованной сессии неэффективным.

⚠ ***Примечание:*** *для защиты вашего веб-проекта на высоком уровне безопасности должны быть включены оба механизма защиты сессий.*

Защита редиректов от фишинга

Включение или отключение защиты редиректов от фишинга выполняется на странице **Защита редиректов** (*Настройки > Проактивная защита > Защита редиректов*) с помощью кнопки **Включить защиту редиректов от фишинга** (или **Выключить защиту редиректов от фишинга**) (Рис. 1.18).

Рис. 1.18 Защита редиректов от фишинга

Параметры защиты от фишинга настраиваются на закладке **Параметры** (Рис. 1.19):

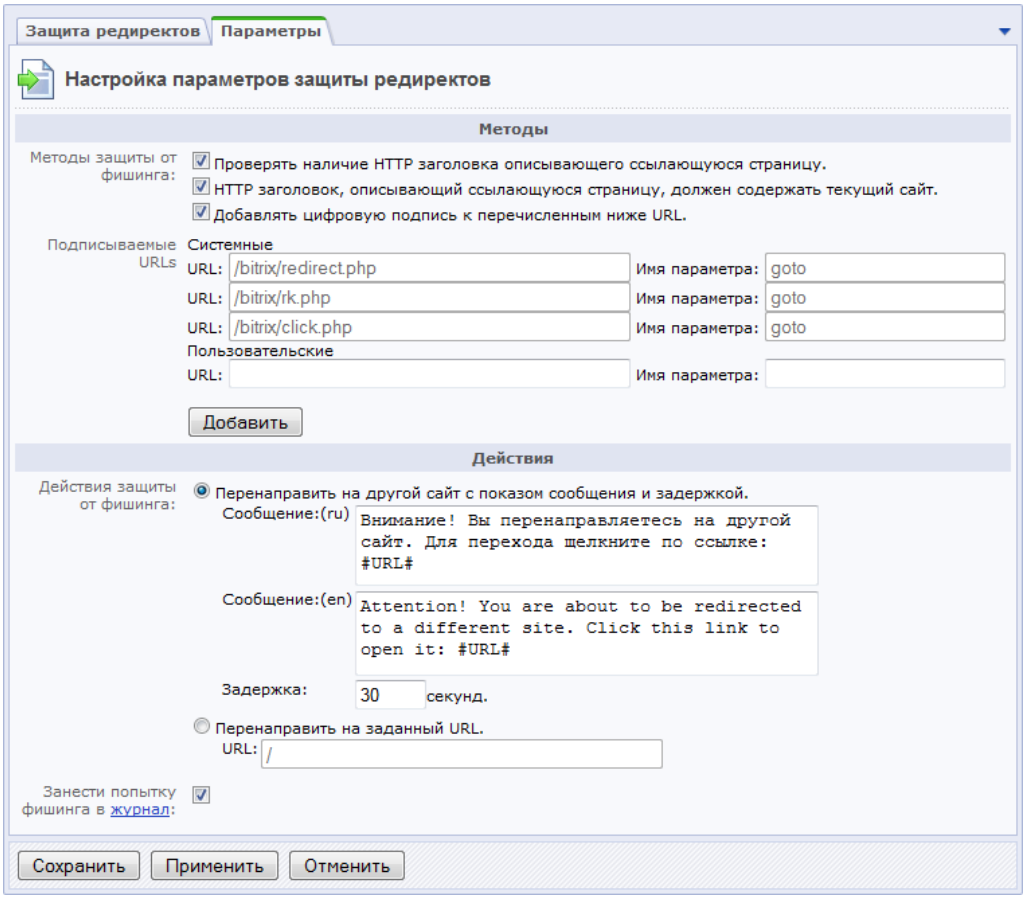

Рис. 1.19 Настройка параметров защиты редиректов

Защита редиректов от фишинга может осуществляться:

- Проверкой наличия HTTP заголовка, описывающего страницу;
- Проверкой наличия в HTTP заголовке записи о текущем сайте, который описывает ссылающуюся страницу;
- Добавлением цифровой подписи к ссылкам, генерируемым на сайте.

При включенной защите все системные ссылки обязательно подписываются дополнительным параметром индивидуальным для сайта и для этого перехода. Кроме

того, можно защитить пользовательские ссылки перенаправлений, добавив их в поле **Подписываемые URLs** в секции **Пользовательские** (добавление полей ввода осуществляется с помощью кнопки **Добавить**).

Защита редиректов может выражаться одним из следующих действий:

- Перенаправлением на другой сайт с показом соответствующего сообщения и выполнением задержки на несколько секунд.

  Текст сообщения задается с помощью поля **Сообщение**, а период задержки пользователя – в поле **Задержка**.

или

- Перенаправлением на заведомо безопасный адрес, например, на главную страницу сайта.

  В этом случае необходимо задать адрес страницы сайта с помощью поля **URL**.

Для фиксирования попыток фишинга через редирект необходимо отметить опцию **Занести попытку фишинга в журнал**.

⚠ ***Примечание:*** *для того чтобы защита сайта осуществлялась на стандартном уровне, защита редиректов от фишинга должна быть включена.*

Повышенный уровень безопасности

Для того чтобы защита веб-проекта осуществлялась на повышенном уровне безопасности, сначала необходимо настроить защиту на стандартном и высоком уровне, а затем выполнить настройку параметров повышенного уровня (Рис. 1.20):

Уровень безопасности: Повышенный

Параметр	Значение	Рекомендации
Одноразовые пароли	Включены	
Контроль целостности	Выполнен	
Веб-антивирус	Включен	
Действия при обнаружении вируса	Вырезание из кода сайта	
Исключения веб-антивируса	Нет	
Журнал заражений за последние 7 дней	0	

Рис. 1.20 Повышенный уровень безопасности

⚠ ***Примечание:*** *если хотя бы один параметр повышенного уровня безопасности принимает несоответствующее значение, то защита сайта будет осуществляться на том уровне, который настроен полностью, но при этом будут учтены настройки параметров всех уровней.*

Одноразовые пароли

Система одноразовых паролей дополняет стандартную систему авторизации и позволяет значительно усилить систему безопасности интернет-проекта. Для включения системы необходимо использовать аппаратное устройство (например, Aladdin eToken PASS) или использовать соответствующее программное обеспечение, реализующее OTP (One-Time Password). Рекомендуется использование системы одноразовых паролей администраторам сайта для повышения уровня безопасности.

⚠ ***Примечание:*** *для защиты проекта на повышенном уровне система использования одноразовых паролей должна быть включена.*

Включение или отключение системы использования одноразовых паролей выполняется на странице **Одноразовые пароли** (*Настройки > Проактивная защита > Одноразовые пароли*) с помощью кнопки **Разрешить использование одноразовых паролей** (или **Выключить использование одноразовых паролей**) (Рис. 1.21).

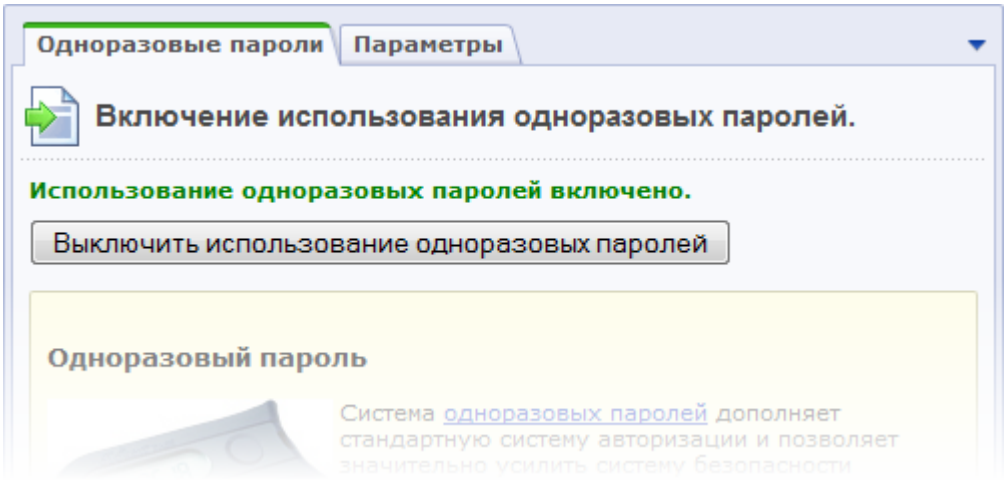

Рис. 1.21 Одноразовые пароли

Если использование одноразовых паролей включено, то в форме редактирования параметров пользователя появляется дополнительная закладка **Одноразовые пароли** (Рис. 1.22), т.е. механизм использования одноразового пароля настраивается отдельно для каждого пользователя.

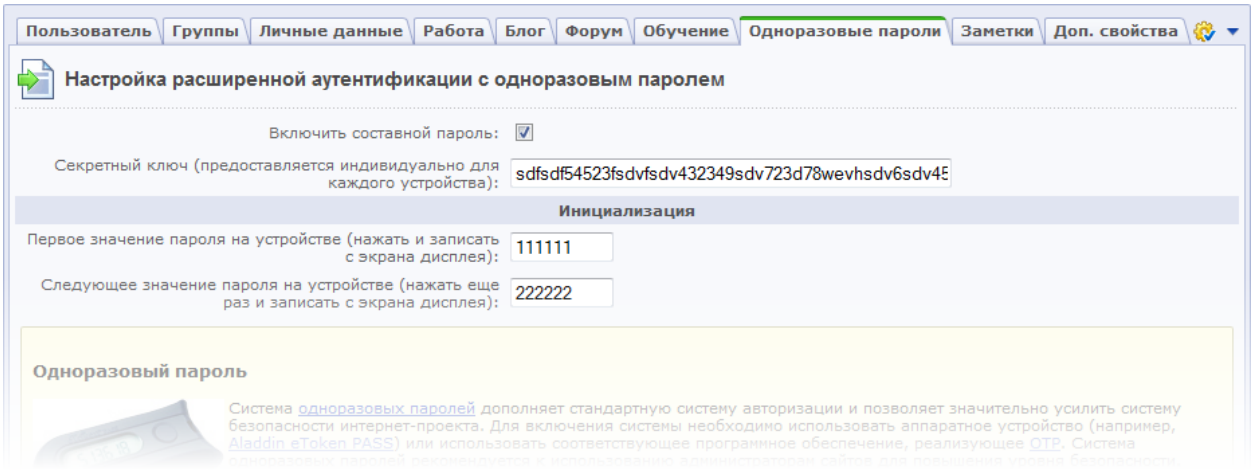

Рис. 1.22 Настройка аутентификации пользователя

Чтобы аутентификация пользователя выполнялась с использованием одноразовых паролей, выполните следующие действия:

- Отметьте опцию **Включить составной пароль**.
- В поле **Секретный ключ** введите секретный ключ, который поставляется вместе с устройством OTP.
- Выполните инициализацию устройства, т.е. введите два последовательно сгенерированных одноразовых паролей, полученных с устройства (например, 111111 и 222222, см. Рис. 1.22).
- Сохраните внесенные изменения.

Теперь пользователь сможет авторизоваться только с использованием логина и составного пароля, состоящего из своего пароля и одноразового пароля устройства.

Одноразовый пароль (см. 2 на Рис. 1.23) вводится в поле **Пароль** стандартной формы авторизации на сайте сразу после обычного пароля (см. 1 на Рис. 1.23) без пробелов.

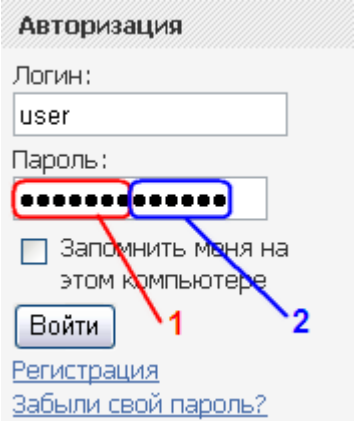

Рис. 1.23 Форма авторизации

Система авторизации с использованием одноразовых паролей разработана в рамках инициативы OATH. Реализация основана на алгоритме HMAC и хэш-функции SHA-1. Для расчета значения OTP принимаются два входных параметра - секретный ключ (начальное значение для генератора) и текущее значение счетчика (количество необходимых циклов генерации). Начальное значение хранится как в самом устройстве, так и на сайте после инициализации устройства. Счетчик в устройстве увеличивается при каждой генерации OTP, на сервере - при каждой удачной аутентификации по OTP.

Таким образом, если на устройстве была нажата кнопка несколько раз (например, случайно), но не было выполнено ни одной удачной аутентификации по OTP, то при превышении числа нажатий значения, заданного в параметре **Размер окна проверки паролей** (Рис. 1.24), произойдет нарушение синхронизации счетчика генерации, и пользователь не сможет выполнить вход на сайт.

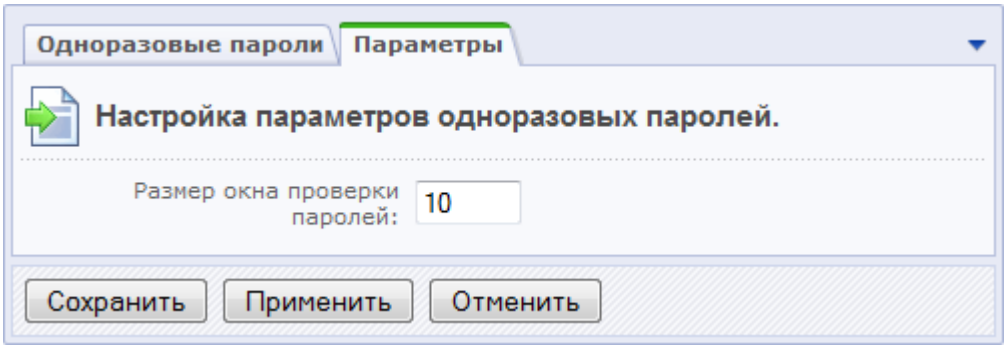

Рис. 1.24 Настройка параметра проверки одноразовых паролей

В этом случае необходимо выполнить повторную синхронизацию пользователя с устройством – привести значение на сервере в соответствие значению, хранящемуся в устройстве. Для этого администратор системы или сам пользователь (при наличии соответствующих разрешений) должен сгенерировать два последовательных значения одноразовых паролей и ввести их в форму редактирования параметров пользователя (Рис. 1.22).

Чтобы избежать нарушений синхронизации, можно увеличить значение параметра **Размер окна проверки паролей**, например, указать 100 или 1000.

Контроль целостности

Форма, расположенная на странице **Контроль целостности** (*Настройки* > *Проактивная защита* > *Контроль целостности*), служит для выполнения проверки целостность ядра, системных областей, публичной части продукта.

Для защиты веб-проекта на повышенном уровне безопасности необходимо регулярно (примерно раз в неделю) выполнять проверку целостности системы. Кроме того, проверку целостности следует выполнять перед установкой обновлений системы, а после установки обновлений необходимо собрать новую информацию по файлам.

⚠ ***Примечание:*** *некоторые обновления модуля могут потребовать переподписания скрипта контроля.*

Первый запуск проверки целостности

- Введите и запомните пароль, состоящий из латинских букв и цифр, длиной не менее 10 символов.
- Подтвердите его в поле **Пароль еще раз**.
- Задайте **Ключевое слово**, отличное от пароля, и запомните его.

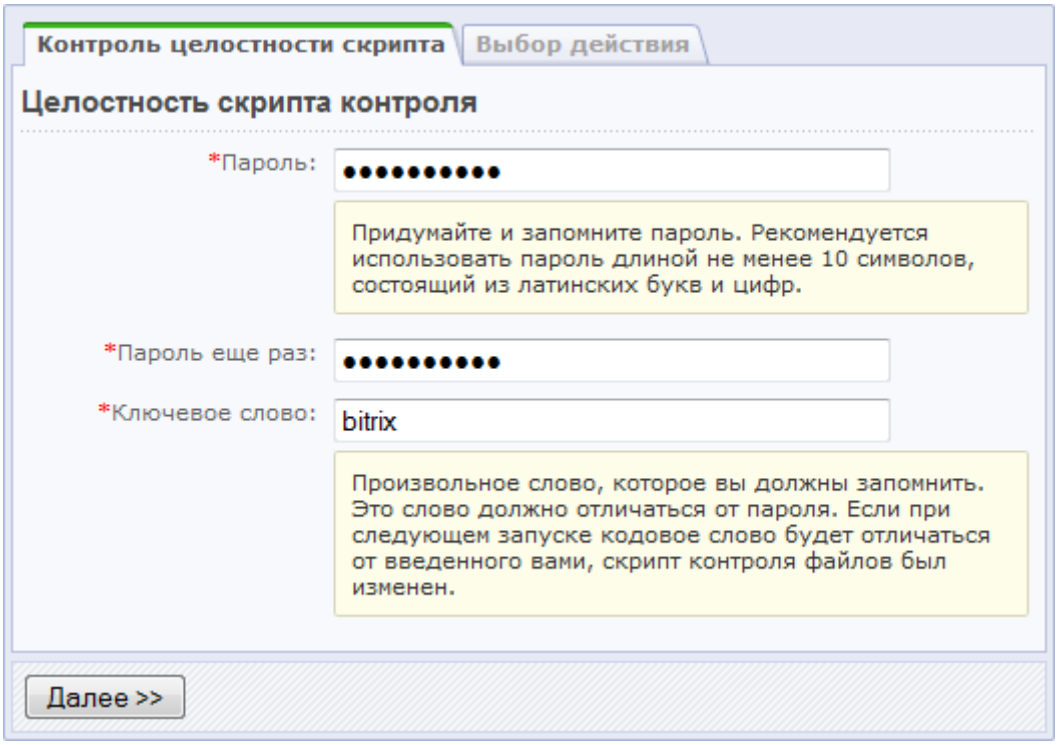

Рис. 1.25 Подписание скрипта контроля

- Нажмите кнопку **Далее**.

Если вы не ошиблись при подтверждении пароля, то отобразится сообщение об успешном подписании скрипта (Рис. 1.26).

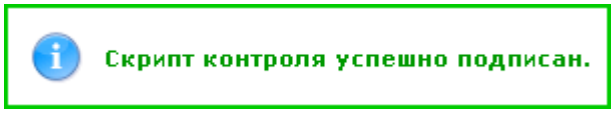

Рис. 1.26 Сообщение об успешном подписании скрипта

Теперь можно приступать к сбору информации по файлам, чтобы в дальнейшем выполнить проверку целостности системы.

Сбор информации по файлам:

- На закладке **Выбор действия** отметьте опцию **Собрать информацию по файлам** (Рис. 1.27):

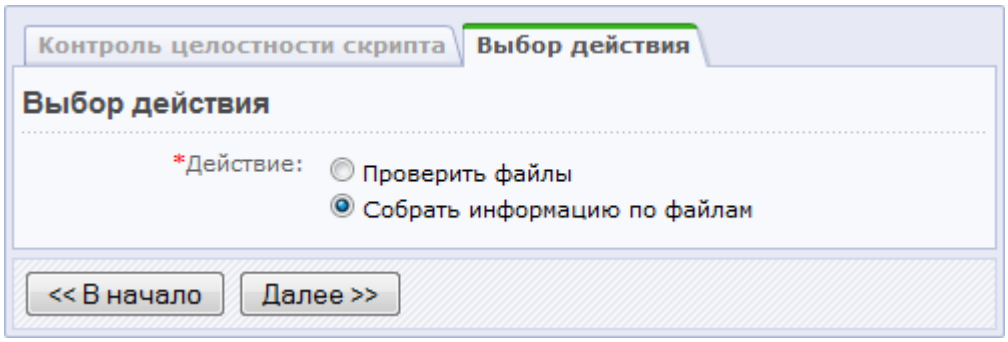

Рис. 1.27 Выбор действия

- Нажмите кнопку **Далее**. Откроется форма сбора данных (Рис. 1.28).

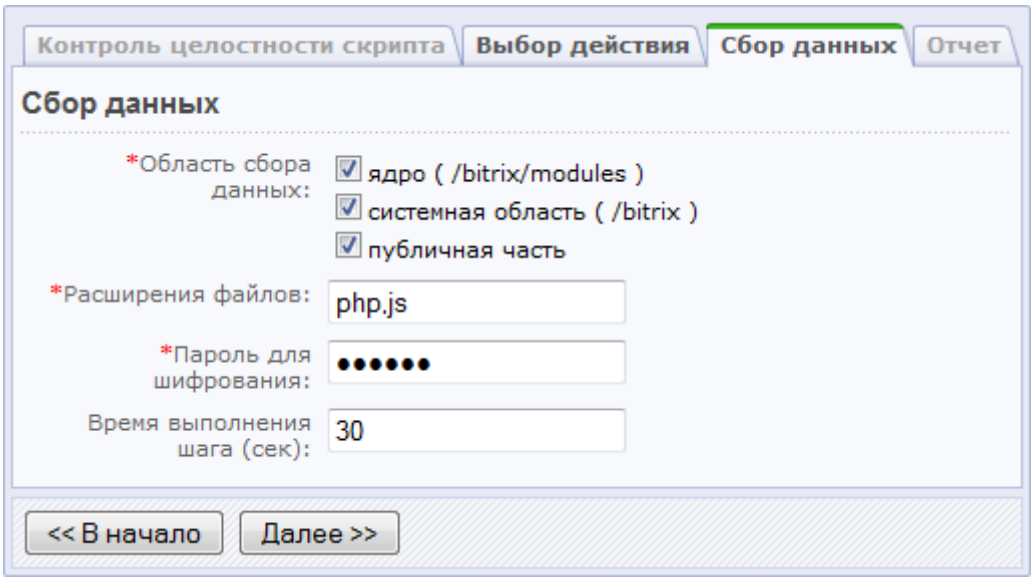

Рис. 1.28 Сбор данных

- Задайте параметры для сбора информации:

  - **Область сбора данных** – отметьте необходимые для обработки папки системы.

- **Расширения файлов** – укажите расширения файлов, по которым должна быть собрана информация. Расширения файлов указываются через запятую без пробелов.
- **Пароль для шифрования** – введите и запомните пароль, который будет использоваться для шифрования и последующего дешифрования собранного верификационного файла.
- **Время выполнения шага** – укажите количество секунд для выполнения одного шага сбора данных.

Ø Нажмите кнопку **Далее**. Начнется процесс сбора данных, по окончании которого в целях безопасности рекомендуется скачать файл с данными на локальный компьютер (Рис. 1.29).

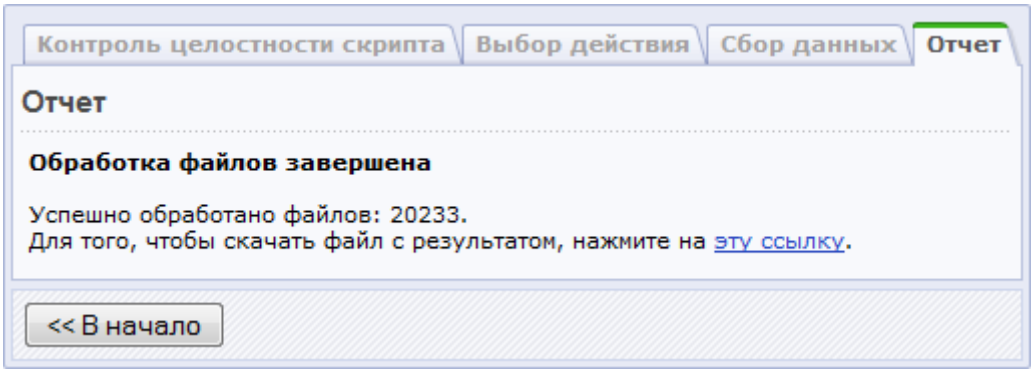

Рис. 1.29 Окончание обработки файлов

Файл с верификационными данными собран, теперь можно выполнить проверку целостности системы.

Проверка целостности системы

При любом (кроме первого) запуске проверки целостности системы сначала проверяется сам скрипт контроля на наличие в нем изменений.

Ø Введите пароль (Рис. 1.30), которым вы подписали скрипт контроля (Рис. 1.25) и нажмите кнопку **Далее**.

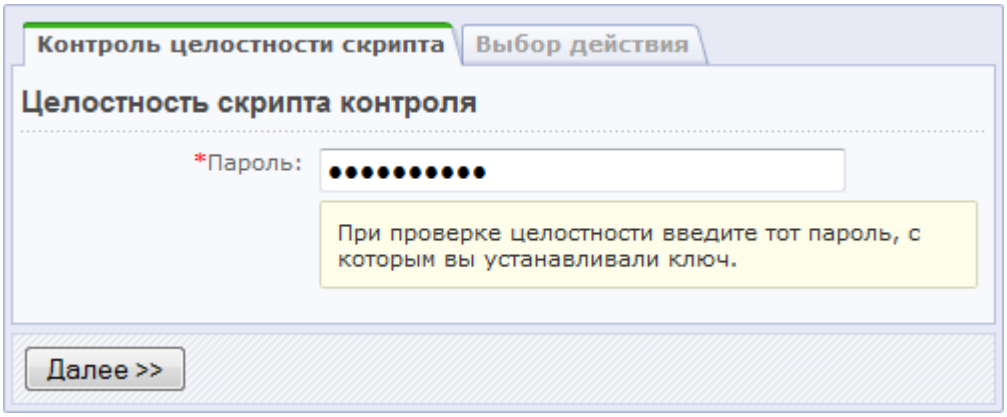

Рис. 1.30 Проверка скрипта контроля

В сообщении о результатах проверки скрипт должен указать кодовое слово, которое вы ввели в момент подписания (Рис. 1.31).

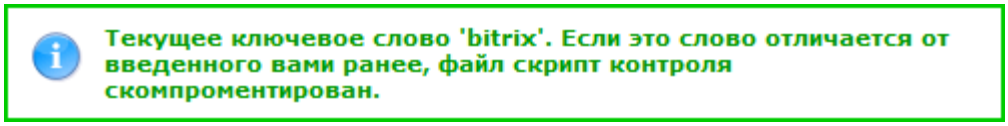

Рис. 1.31 Сообщение о результате проверки

⚠ ***Примечание:*** *если вы не увидели своего кодового слова в сообщении о результатах проверки, то скрипт контроля целостности файлов скомпрометирован (т.е. он был изменен и его результатам доверять нельзя). В этом случае необходимо заменить скрипт контроля целостности системы (например, можно сделать откат версии модуля до 8.0.0).*

- На закладке **Выбор действия** отметьте опцию **Проверить файлы** (Рис. 1.32).

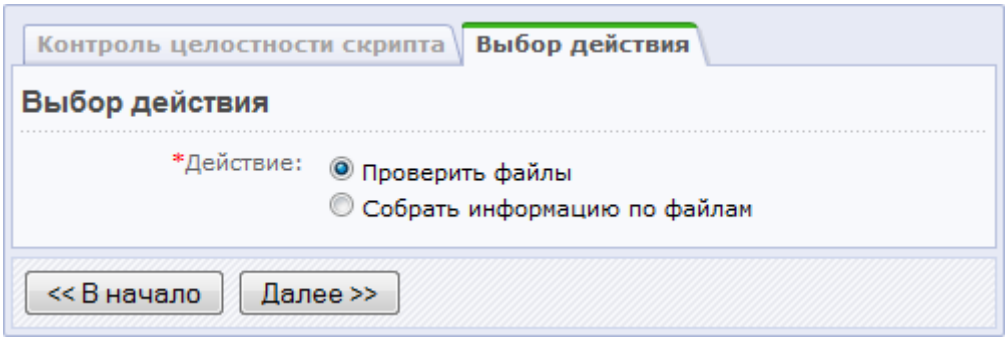

Рис. 1.32 Выбор действия

- Нажмите кнопку **Далее**. Откроется форма выбора файла с верификационными данными (Рис. 1.33).

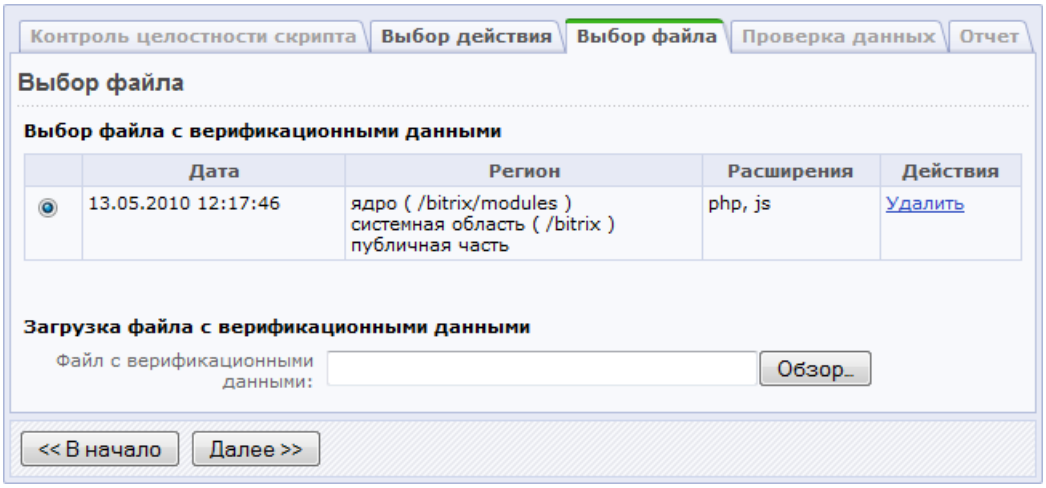

Рис. 1.33 Выбор файла

- Выберите один из лог-файлов, хранящихся в системе, либо загрузите лог-файл с вашего компьютера с помощью кнопки **Обзор**. Откроется форма проверки данных (Рис. 1.34).

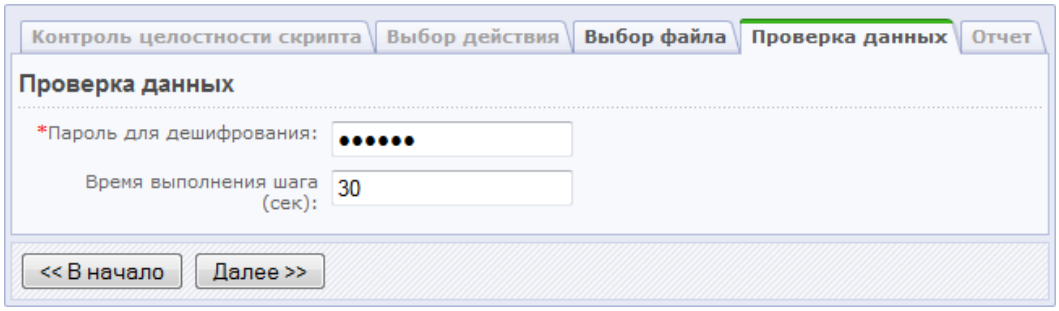

Рис. 1.34 Проверка данных

- В поле **Пароль для дешифрования** укажите пароль, который вы задавали при создании файла с верификационными данными.
- Укажите время выполнения одного шага проверки (чем меньше время выполнения одного шага, тем больше нагрузка на сервер).
- Нажмите кнопку **Далее**. Начнется процесс проверки целостности системы, по окончании которого будет выведен отчет (Рис. 1.35):

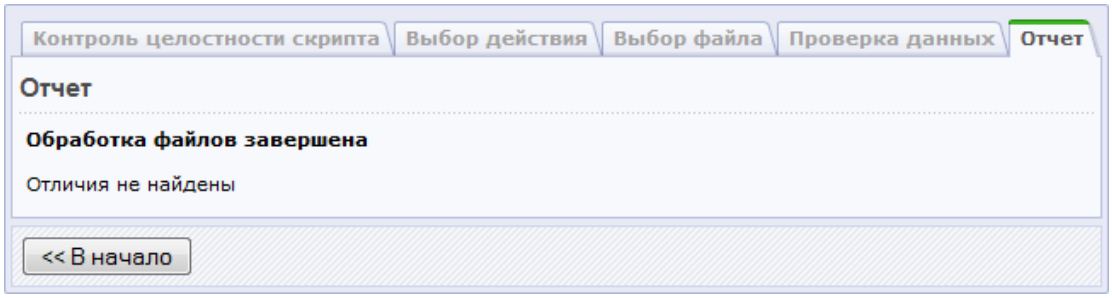

Рис. 1.35 Отчет по проверке файлов системы

Веб-антивирус и исключения из него

Веб-антивирус - система противодействия заражениям сайтов. Веб-антивирус выявляет в html-коде потенциально опасные участки и "вырезает" подозрительные объекты из кода сайта, тем самым препятствуя проникновению вирусов на компьютер пользователя.

⚠ ***Примечание:*** *веб-антивирус не является заменой обычного антивируса.*

Включение или отключение веб-антивируса выполняется на странице **Веб-антивирус** (*Настройки > Проактивная защита > Веб-антивирус*) с помощью кнопки **Включить веб-антивирус** (или **Выключить веб-антивирус**) (Рис. 1.36).

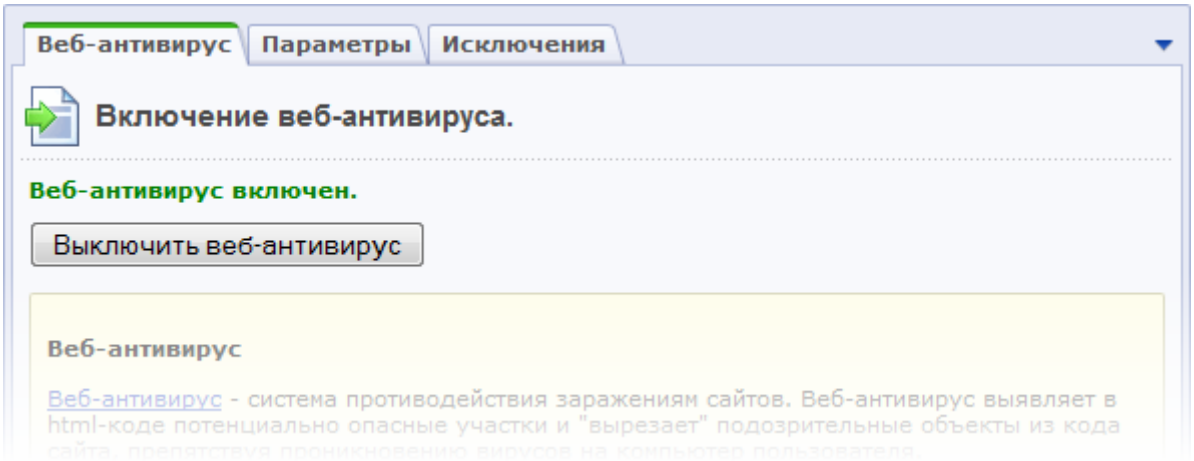

Рис. 1.36 Веб-антивирус

⚠ ***Примечание:*** *для детектирования вирусов, внедренных до старта буферизации вывода, необходимо задать*

- *либо в* ***php.ini****:*

  auto_prepend_file = /www/bitrix/modules/security/tools/start.php
- *или в файле* ***.htaccess****:*

  php_value auto_prepend_file "/www/bitrix/modules/security/tools/start.php"

Действия системы, выполняемые при обнаружении вируса, задаются на закладке **Параметры** (Рис. 1.37).

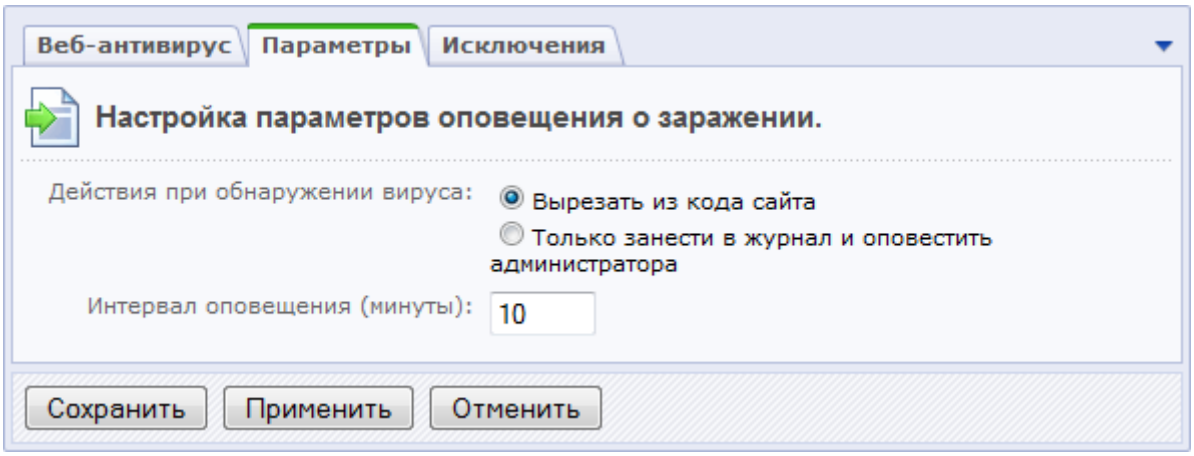

Рис. 1.37 Настройка параметров оповещения о заражении

- **Вырезать из кода сайта** - опасные данные будут вырезаны из кода сайта;
- **Только занести в журнал и оповестить администратора** - запись об обнаружении вируса будет занесена в **Журнал событий**. Администратору будут посылаться оповещения по e-mail через интервал времени, заданный в поле **Интервал времени**.

Закладка **Исключения** (Рис. 1.38) позволяет настроить исключения для веб-антивируса, т.е. веб-антивирус не будет применяться к блокам html-кода, указанным на данной закладке.

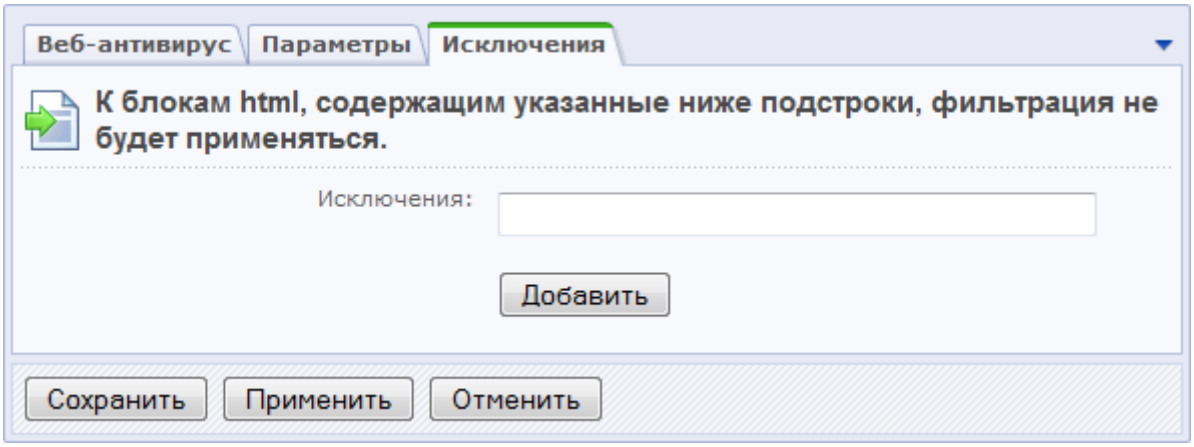

Рис. 1.38 Исключения веб-антивируса

⚠ ***Примечание:*** *чтобы защита сайта осуществлялась на повышенном уровне веб-антивирус должен быть включен.*

Глава 2. Дополнительные настройки

Стоп-лист

Модуль **Проактивная защита** имеет собственный **Стоп-лист** (*Настройки* > *Проактивная защита* > *Стоп-лист*) (Рис. 2.1), отличный от стоп-листа модуля **Веб-аналитика**.

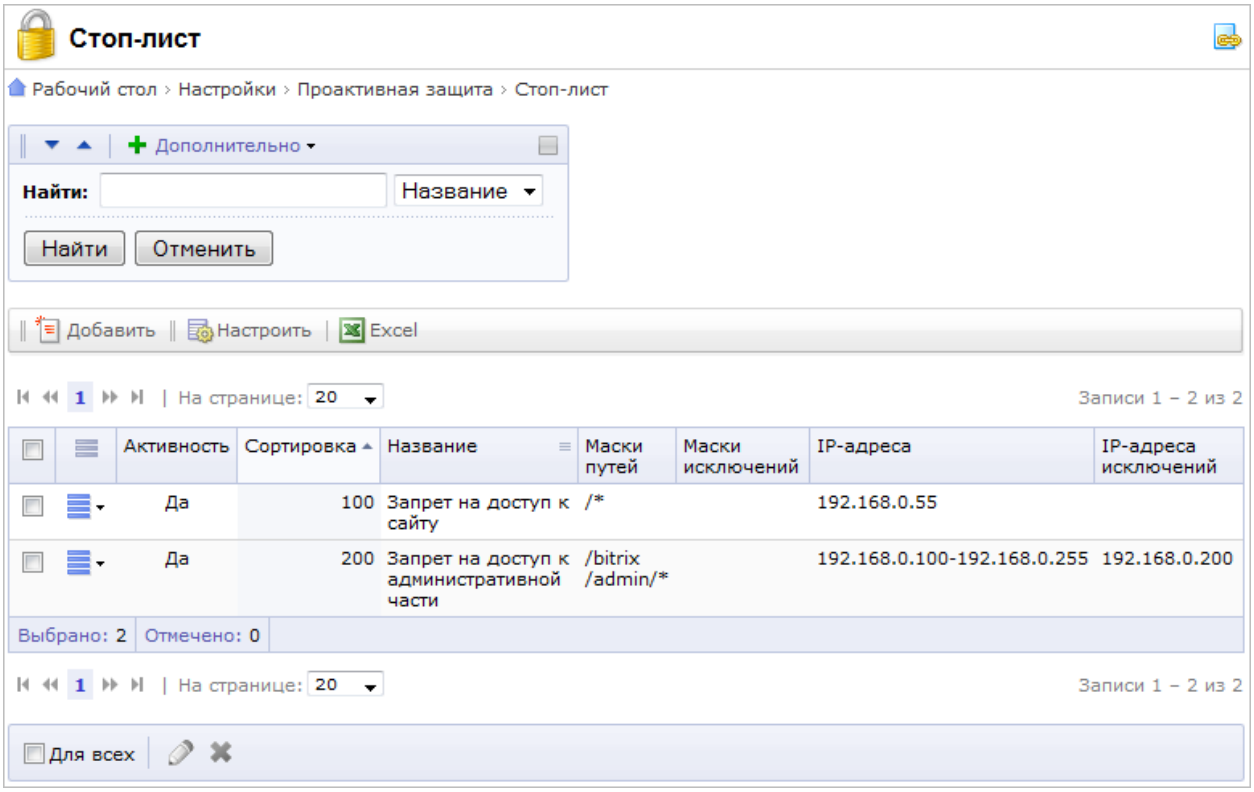

Рис. 2.1 Стоп-лист модуля Проактивная защита

На странице **Стоп-лист** представлена информация о правилах блокировки доступа к вашему сайту или некоторым его разделам с определенных IP-адресов, причем если активность обозначена зеленым цветом, то правило действует на данный момент, а если красным, то срок действия правила истек.

Записи о блокировке доступа создаются либо вручную, либо автоматически. Правило создается автоматически в следующих случаях:

- при включении механизма защиты административной раздела;
- при срабатывании проактивного фильтра на вторжении (если отмечена опция **Добавить IP-адрес атакующего в стоп-лист**) (Рис. 1.4).

Чтобы создать правило блокировки вручную, например, на основе анализа журнала вторжений, выполните следующее:

Ø Нажмите на кнопку **Добавить**, расположенную на контекстной панели страницы стоп-листа проактивной защиты. Откроется форма создания (редактирования) правила блокировки доступа к сайту (Рис. 2.2).

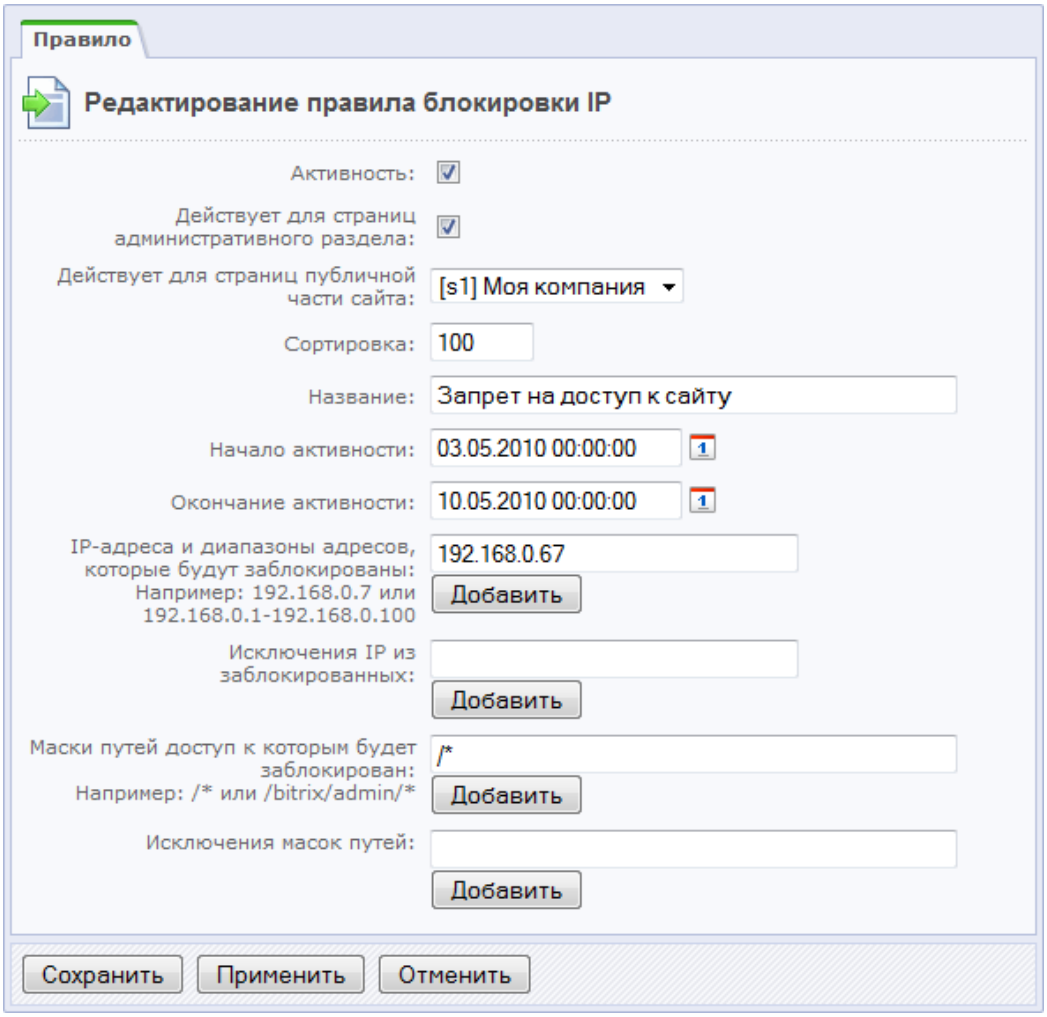

Рис. 2.2 Создание правила блокировки доступа

- Заполните поля формы необходимым вам образом.

  Вы можете заблокировать доступ как к административной, так и к публичной части сайта, указав при этом IP-адреса или диапазоны адресов, которые будут заблокированы. Вы можете заблокировать доступ не ко всему сайту, а только к некоторым его разделам и страницам, для этого необходимо задать маски путей, доступ к которым необходимо заблокировать. Исключения в правиле задаются как по IP-адресам, так и по маскам путей.

  ⚠ ***Примечание:*** *каждый IP-адрес или маска пути задается в отдельном поле, которое добавляется по кнопке* ***Добавить****. Диапазон IP-адресов указывается с помощью тире, например, 192.168.0.1-192.168.0.100.*

- Сохраните внесенные данные.

В результате, если пользователь, для IP-адреса которого имеется правило блокировки доступа, попытается зайти на сайт, то ему будет выдана ошибка HTTP 403 – доступ запрещен.

Заключение

Изучив руководство, вы получили представление об использовании модуля **Проактивная защита** для обеспечения безопасности вашего веб-проекта.

Вопросы можно задавать на форуме сайта компании "1С-Битрикс":

http://dev.1c-bitrix.ru/community/forums/

или решать в рамках технической поддержки компании "1С-Битрикс":

http://dev.1c-bitrix.ru/support/