



1С-Битрикс: Управление сайтом

Курс «Администратор. Модули»





Содержание

Введение	3
Проактивная защита	4
Уязвимости	5
ОСНОВНЫЕ ПОНЯТИЯ	6
СТАНДАРТНЫЙ УРОВЕНЬ	7
Проактивный фильтр и исключения из него	7
Журнал вторжений	11
Контроль активности	12
Уровень безопасности группы администраторов	13
Использовать CAPTCHA при регистрации	14
Режим вывода ошибок	14
Показ ошибочных запросов базы данных	15
ВЫСОКИЙ УРОВЕНЬ	15
Журналирование событий главного модуля	16
Защита административной части	17
Хранение сессий и смена идентификатора	18
Защита редиректов от фишинга	20
ПОВЫШЕННЫЙ УРОВЕНЬ	22
Одноразовые пароли	22
Контроль целостности	25
Веб-антивирус	29
СТОП-ЛИСТ	33



Введение

Курс для пользователей, осуществляющих администрирование сайтов. Второй сертификат в линейке администрирования. Первый курс - Администратор. Базовый - дает базовые понятия по работе с системой "1С-Битрикс: Управление сайтом" и описывает работу модулей:

- Главный модуль,
- Управление структурой,
- Информационные блоки,
- Поиск.

Курс **Администратор. Модули** позволяет освоить методы выполнения расширенных задач по администрированию модулей, не относящихся к коммерческой деятельности.

Получаемые навыки:

- методы работы с модулями системы некоммерческого плана;
- работа с инструментами поисковой оптимизации и контроля за посещаемостью сайта;
- методы импорта пользователей с помощью сервера LDAP;
- организация документооборота и бизнес-процессов;
- работа с инструментами защиты сайта от несанкционированного доступа;
- работа с инструментами обеспечения жизнеспособности сайта при повышенной нагрузке;



Проактивная защита

В данной главе рассматриваются основные операции по настройке модуля **Проактивная защита**, который является важным дополнением к стандартной политике безопасности продукта и существенно повышает уровень защиты веб-проекта.

Защита от хакерских атак, взлома и кражи хранящейся на сайте информации — это достаточно важная задача для любого действующего проекта, даже если он не имеет доступа в Интернет.

***Хакерские атаки** - это использование некоторых неочевидных возможностей приложений для совершения нетипичных действий, возможность выполнения которых не подразумевалась явно разработчиком веб-приложения.*

Главная цель модуля **Проактивная защита** — уберечь сайт от возможных ошибок при доработке проекта сторонними разработчиками. Этот модуль реализует целый комплекс защитных мероприятий для сайта и сторонних приложений.

***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;
- веб-антивирус;
- шифрование данных.

Не секрет, что любая включенная функция — дополнительная нагрузка на сервер. Поэтому работа с модулем **Проактивная защита** — это вечный поиск компромисса между защитой от потенциальной опасности и реальной загруженностью сервера. Все настройки параметров Проактивной защиты, в том числе и страница **Панель безопасности**, расположены в разделе [Настройки > Проактивная защита](#).



Уязвимости

Уязвимости можно разделить на два основных типа:

- атаки собственно на систему;
- атаки на клиентов веб-приложений.

Атаки непосредственно на систему

Это атаки, осуществляемые на систему непосредственно, без всякого участия "сторонних" программ.

- **SQL-инъекция.** Классическая уязвимость, которая связана с недостаточной фильтрацией данных, используемых в SQL-запросах. Эта критическая уязвимость приводит к тому, что нападающий может выполнить произвольные SQL-запросы к базе данных. В рамках "философии программирования" в **Bitrix Framework** запрещено обращаться непосредственно к базе. Но разработчики сайтов иногда отходят от этого принципа.
- **Внедрение в имя файла.** Уязвимость связана с использованием в качестве части имени файла недостаточно фильтруемого значения, принятого от пользователя. Нападающий может изменить имя файла таким образом, чтобы включить и выполнить в контексте уязвимого сайта произвольный PHP-файл.
- **Внедрение в функцию system.** Уязвимость связана с недостаточной фильтрацией данных. Нападающий сможет выполнить произвольный код в системе.
- **Подбор реквизитов доступа.** Нападающий может подобрать простые пароли.
- **Логические ошибки в коде.** Данный тип ошибок особенно тяжело диагностируется и имеет наибольшее разнообразие. Логическая ошибка в коде возникает, когда при некоторых ситуациях код работает не так, как предполагается.

Атаки на клиентов веб-приложения

Это атаки на веб-систему, которые проходят через других пользователей веб-приложения. Например, через администраторов форума.

- **Межсайтовый скриптинг (XSS).** Уязвимость возникает тогда, когда данные, принятые от пользователя, выводятся в браузер без надлежащей фильтрации. Уязвимость может быть использована для изменения вида HTML-страниц уязвимого сайта в контексте браузера целевого пользователя, похищения **cookie** данных браузера целевого пользователя с последующим внедрением в его сессию под его учетной записью.
- **CSRF.** Если каким-либо образом заставить браузер пользователя сделать запрос к уязвимому серверу, браузер сделает этот запрос с текущими **cookie** данного пользователя.
- **Социальная инженерия.** Злоумышленник может представиться администратором сайта и попросить пароль у пользователя, или изменить пароль на какой-то заданный, или узнать "любимое блюдо" и т. п.
- **Фишинг.** Создается подставной веб-сайт, который повторяет дизайн целевого сайта и имеет похожий URL. Например, 1c-bitrix.ru (здесь первый символ — "эль", а не "один"), на него заманивается пользователь в надежде, что он введет свои логин и пароль, которые будут доступны злоумышленникам. Уязвимость может быть использована совместно с **XSS** и **CSRF**.



Основные понятия

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](#)).

Текущий уровень безопасности: Начальный.

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	Низкий	Включить 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	



Для каждого уровня приведена соответствующая таблица параметров и их значений, а также указаны, в случае необходимости, рекомендации по изменению значений параметров. Если для какого-то параметра установлено несоответствующее значение, то в поле **Рекомендации** будет отображено необходимое для выполнения действие.

Стандартный уровень

Для того чтобы защита веб-проекта осуществлялась на стандартном уровне безопасности, необходимо настроить должным образом все параметры данного уровня:

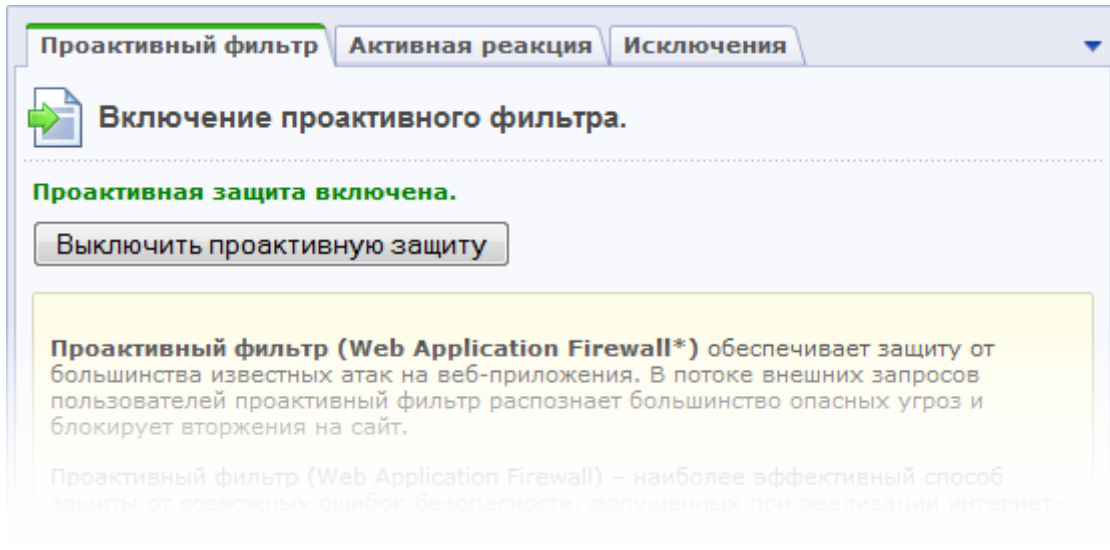
Уровень безопасности: Стандартный		
Параметр	Значение	Рекомендации
Проактивный фильтр (Web Application Firewall)	Включен	
Исключения проактивного фильтра	Нет	
Журнал вторжений за последние 7 дней	0	
Контроль активности	Включен	
Уровень безопасности группы администраторов	Повышенный	
Использовать CAPTCHA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

⚠ 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.

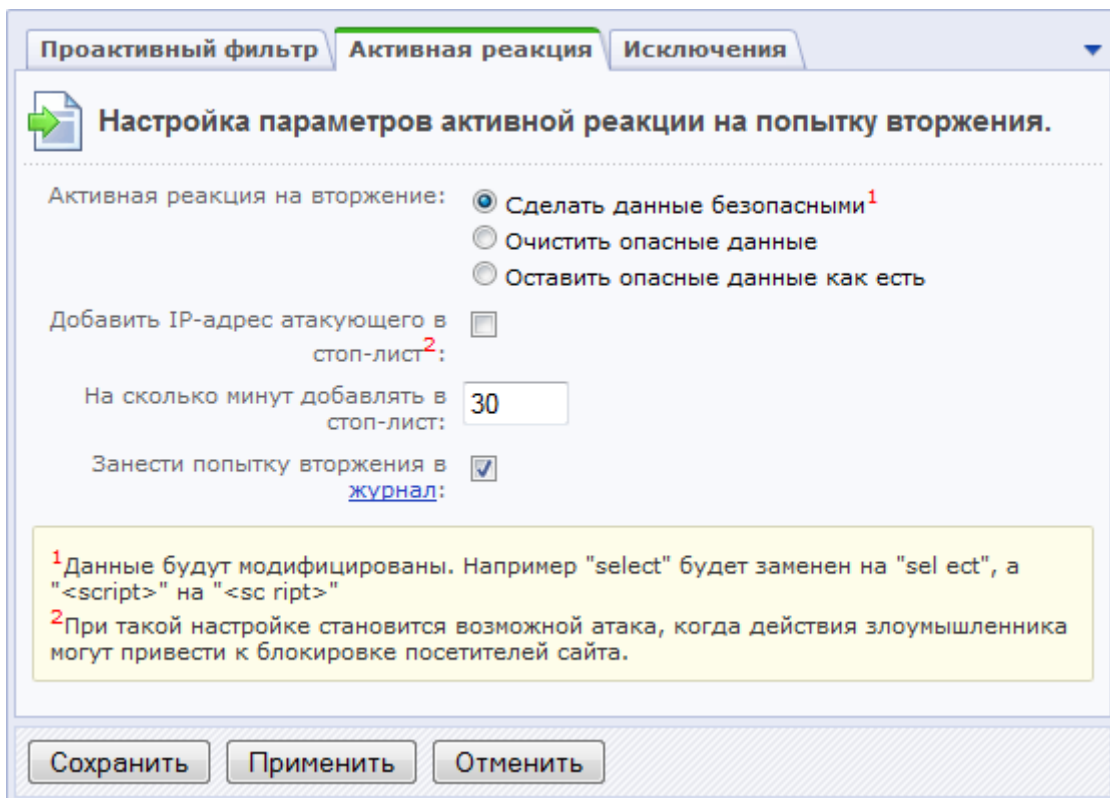
Проактивный фильтр и исключения из него

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**).



На закладке **Активная реакция** настраиваются действия системы при попытке вторжения на сайт:



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.

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.

Настроить работу фильтра можно по двум параметрам: по страницам и по пользователям.

Фильтр по страницам

- Перейдите на вкладку **Исключения** страницы [Настройки > Проактивная защита > Проактивный фильтр](#).
- В поле **Маски исключения** внесите нужные вам страницы. С помощью кнопки **Добавить** можно увеличить число полей для исключений.

Проактивный фильтр Активная реакция Исключения

К страницам подходящим к условиям фильтрация не будет применяться.

Маски исключения: для сайта:

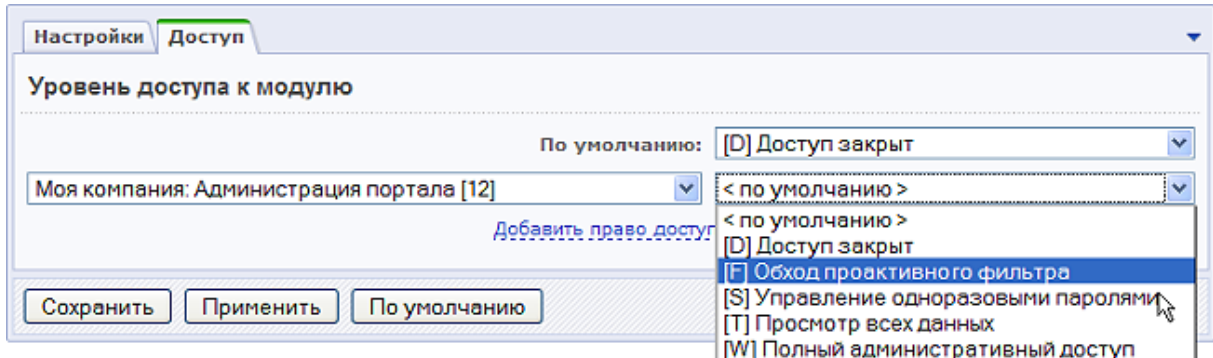
(например: /bitrix/* или */news/*)

Фильтр по пользователям

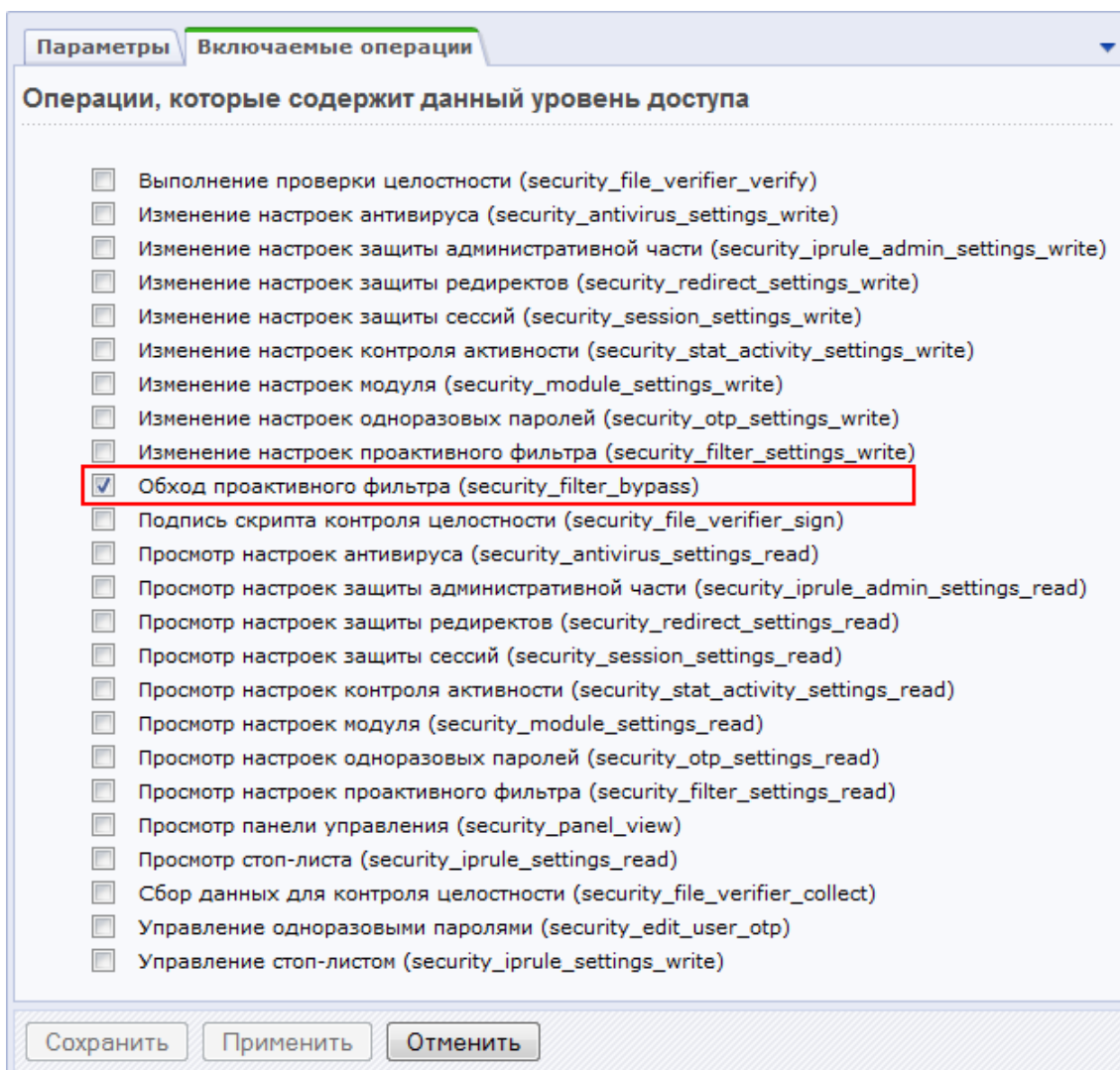
При необходимости можно настроить проактивный фильтр так, чтобы он не срабатывал на любых страницах, но для определенных групп пользователей. Эта настройка осуществляется на странице настроек параметров самого модуля **Проактивная защита**:



- Перейдите на вкладку **Доступ** страницы *Настройки > Настройки продукта > Настройки модулей > Проактивная защита*.
- Для нужных групп пользователей выберите уровень доступа: **[F] Обход проактивного фильтра**.



Примечание: проактивный фильтр не работает для тех групп пользователей, для которых в правах доступа к модулю **Проактивная защита** разрешена операция **Обход проактивного фильтра**. Определяется настройками уровня доступа (Настройки > Пользователи > Уровни доступа) к модулю проактивной защиты.





Журнал вторжений

Журнал вторжений (*Настройки > Проактивная защита > Журнал вторжений*) 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**.

В журнале представлена следующая информация о событии:

Журнал событий

Рабочий стол > Настройки > Проактивная защита > Журнал вторжений

Найти: Событие:

Событие: (все)
[SECURITY_FILTER_SQL] Попытка внедрения SQL
[SECURITY_FILTER_XSS] Попытка атаки через XSS
[SECURITY_FILTER_PHP] Попытка внедрения PHP
[SECURITY_REDIRECT] Попытка фишинга через редирект

Настроить | Excel

На странице: 20 | Записи 1 - 2 из 2

ID	Время	Событие	Объект	IP	URL	Пользователь	Описание
256	12.05.2010 16:11:53	Попытка внедрения SQL	\$_GET["q"]	192.168.0.61	/search/?q=select+*+from+abc	[473] Наталья Ломова	select * from abc
225	07.05.2010 12:12:03	Обнаружен вирус	UNKNOWN	127.0.0.1	/bitrix/admin/dump.php?lang=ru&dumping=Y&Next=Y&NS=8da6c6330136a31997c3677502341f83&stepped=Y&max_execution_time=30&d_pub=Y&d_ker=Y&skip_symlinks=Y&max_file_size=1048576&dump_base=Y&sessid=54c385416f9f3c827eed0d8bf350142		<script>document.getElementById("form_tbl_dump").action="/bitrix/admin/dump.php?mode=frame&lang=ru&dumping=Y&Next=Y&NS=8da6c6330136a31997c3677502341f83&stepped=Y&max_execution_time=30&d_pub=Y&d_ker=Y&skip_symlinks=Y&max_file_size=1048576&dump_base=Y&sessid=54c385416f9f3c827eed0d8bf350142";document.getElementById("form_tbl_dump").onsubmit();document.getElementById("form_tbl_dump").submit();</script>

Выбрано: 2

- 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.



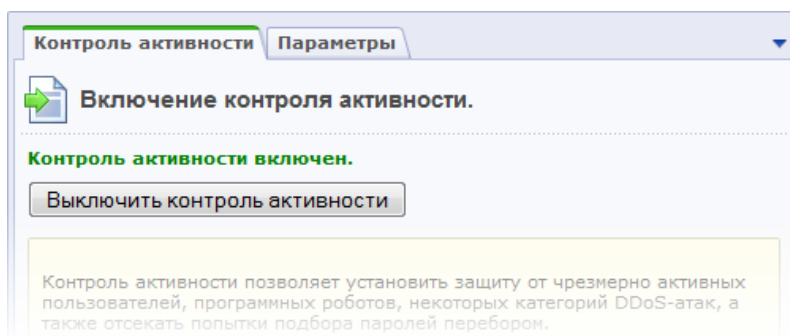
В журнале фиксируются события следующих типов:

- 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 отсекают 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**).



На закладке **Параметры** задаются параметры максимальной активности пользователей вашего сайта.



Контроль активности **Параметры**

Настройка параметров контроля активности.

Шаблон страницы, которая будет показана заблокированному пользователю: [редактировать шаблон](#)

Блокировать на время: (сек.)

если в течение (сек.)

сделано более хитов

Сделать запись в [журнале](#) событий:

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 вторично 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 отличен от повышенного, то необходимо выполнить следующее:

- На странице **Панель безопасности** нажмите ссылку **Включить повышенный**. Откроется форма редактирования группы на закладке **Безопасность**.

Параметры **Безопасность**

Настройки политики безопасности

Предопределенные настройки уровня безопасности: -- Выберите уровень --

Время жизни сессии (минут): -- Выберите уровень --

Маска сети для привязки сессии: Низкий

Повышенный

255.255.255.255

Максимальное количество компьютеров на которых может быть одновременно быть запомнена авторизация: Не переопределять

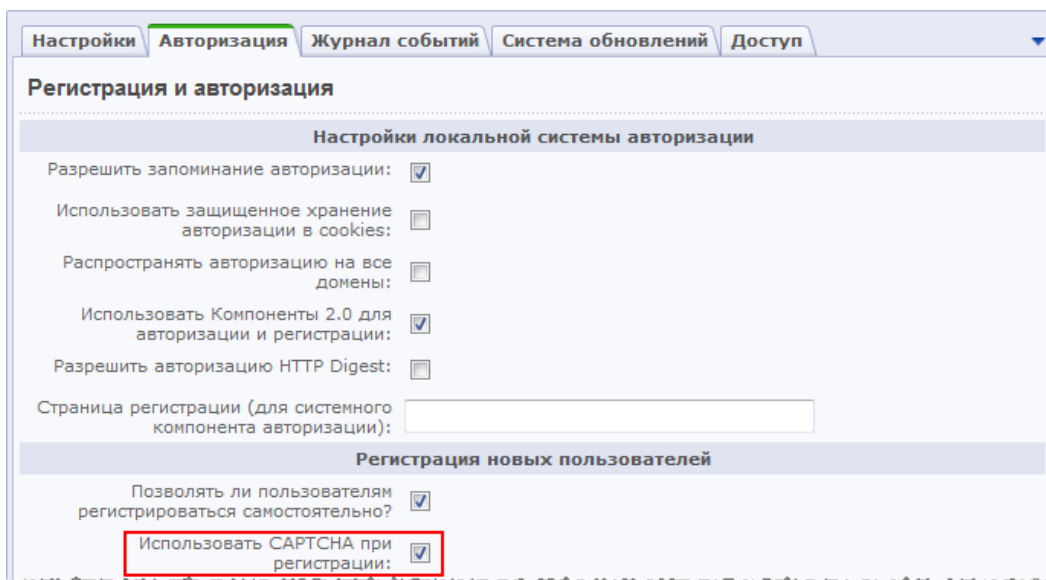
- В поле **Предопределенные настройки уровня безопасности** укажите **повышенный уровень**.



- 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**:



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**.



Настройка параметров модуля

Системные настройки

Язык по умолчанию для административной части: [ru] Russian

Название сайта: Моя компания

URL сайта (без http://): Например: www.mysite.com

Имя префикса для названия cookies (без точек и пробелов): BITRIX_SM

Распространять куки на все домены:

Посылать в заголовке статус 200 на 404 ошибку:

Режим вывода ошибок (error_reporting): Только ошибки

Использовать визуальный редактор для редактирования шаблонов сайта:

Почта

E-Mail адрес или список адресов через запятую на который будут дублироваться все исходящие сообщения:

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

- 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

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:

**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	

⚠ 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](#)):



Настройки Авторизация **Журнал событий** Система обновлений Доступ ▾

Настройка параметров журнала событий

Сколько дней хранить события:

События для записи в журнал

Записывать выход из системы	<input checked="" type="checkbox"/>
Записывать успешный вход	<input checked="" type="checkbox"/>
Записывать ошибки входа	<input checked="" type="checkbox"/>
Записывать регистрацию нового пользователя	<input checked="" type="checkbox"/>
Записывать ошибки регистрации	<input checked="" type="checkbox"/>
Записывать запросы на смену пароля	<input checked="" type="checkbox"/>
Записывать смену пароля	<input checked="" type="checkbox"/>
Записывать удаление пользователя	<input checked="" type="checkbox"/>
Записывать изменение групп пользователя	<input checked="" type="checkbox"/>
Записывать изменение политики безопасности группы	<input checked="" type="checkbox"/>
Записывать изменение доступа к модулю	<input checked="" type="checkbox"/>
Записывать изменение доступа к файлу	<input checked="" type="checkbox"/>
Записывать изменение уровня доступа	<input checked="" type="checkbox"/>

Чтобы защита сайта велась на высоком уровне, должны быть отмечены **все** опции секции **События для записи в журнал**. Даже если не будет отмечена только одна опция, 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**).



Защита административной части

Ограничение доступа к административной части всех, кроме указанных IP-адресов

Защита включена.

Выключить защиту

Ваш IP-адрес был определен как: 127.0.0.1. Если это так, скопируйте его и вставьте в поле ввода ниже.

IP-адреса и диапазоны с которых разрешен доступ к административной части:
Например: 192.168.0.7 или 192.168.0.1-192.168.0.100

127.0.0.1

Добавить

Сохранить Применить Отменить

⚠ 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 уже установленное ограничение по IP-адресам можно посредством создания специального файла, путь к которому задается в настройках модуля **Проактивная защита**. По умолчанию файл имеет имя следующего формата: `ipcheck_disable_<случайный_набор_из_32_символов>`:

Настройки Доступ

Настройка параметров модуля

Разрешать блокировать себя по IP (с показом предупреждения) :

Путь к файлу-флажку запрета блокировки по IP : /bitrix/modules/ipcheck_disable_ff7a38c6b2b5e8

Сохранить Применить Отменить По умолчанию

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:

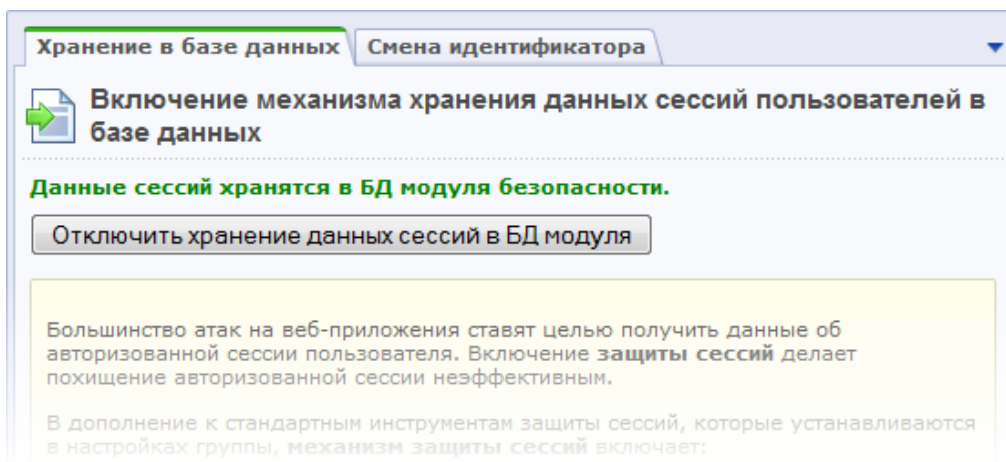
- Время жизни сессии (минут);
- Маска сети для привязки сессии.



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.

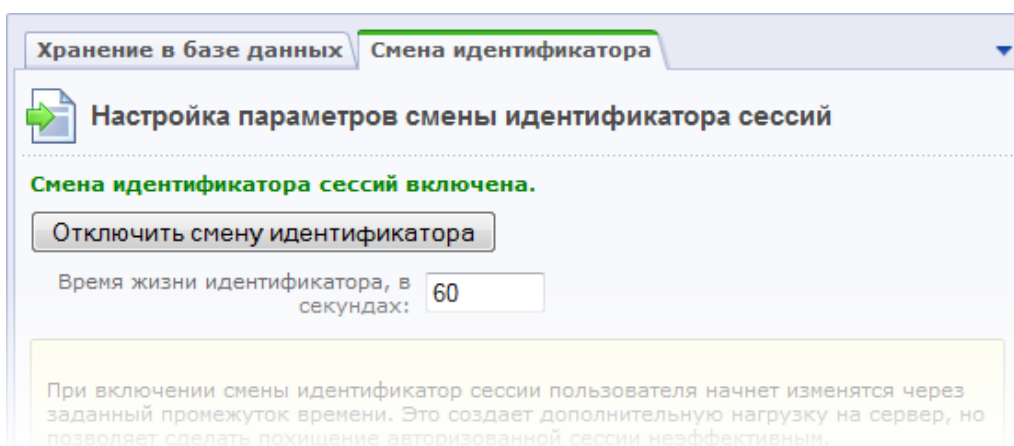
Включение (или отключение) механизма хранения данных сессий пользователей в базе данных выполняется на странице **Защита сессий** ([Настройки](#) > [Проактивная защита](#) > [Защита сессий](#)) с помощью кнопки **Включить хранение данных сессий в БД модуля** (или **Отключить хранение данных сессий в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



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.





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.

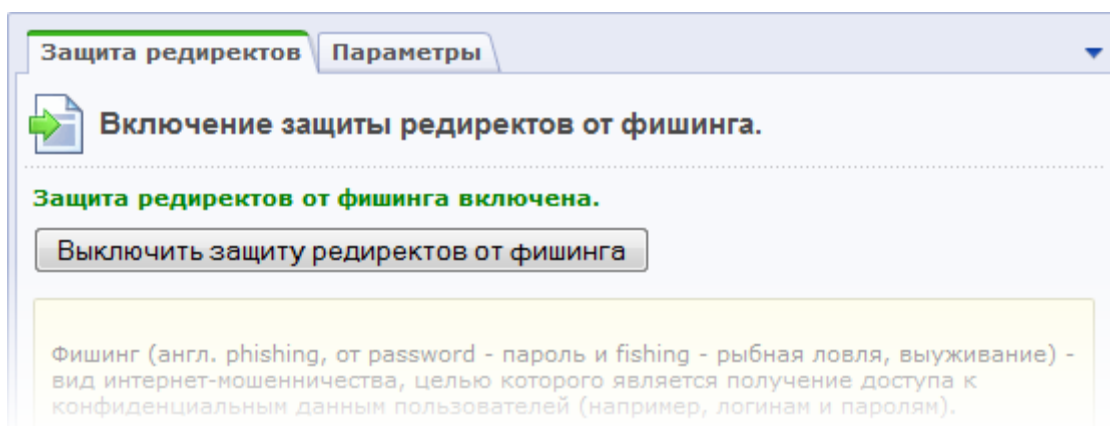
Защита редиректов от фишинга

Фишинг (англ. *phishing*, от *password* — "пароль" и *ishing* — "рыбная ловля, выуживание") - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (например, логинам и паролям).

Фишинг основан на незнании пользователями основ сетевой безопасности. Они воспринимают просьбы от якобы используемого ими сервиса сообщить свои учетные данные, пароль и др. как вполне легальные.

Такая мера получения несанкционированного доступа характерна для проектов с большой посещаемостью и большим числом пользователей, когда есть вероятность, что в общей «толпе» окажется достаточное количество некомпетентных пользователей.

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**).



Параметры защиты от фишинга настраиваются на закладке **Параметры**:



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 URL** 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 высоком уровне, защита редиректов от фишинга должна быть включена.

Повышенный уровень

Для того чтобы защита веб-проекта осуществлялась на повышенном уровне безопасности, сначала необходимо настроить защиту на **стандартном** и **высоком** уровне, а затем настроить параметры повышенного уровня:

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	

⚠ 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.

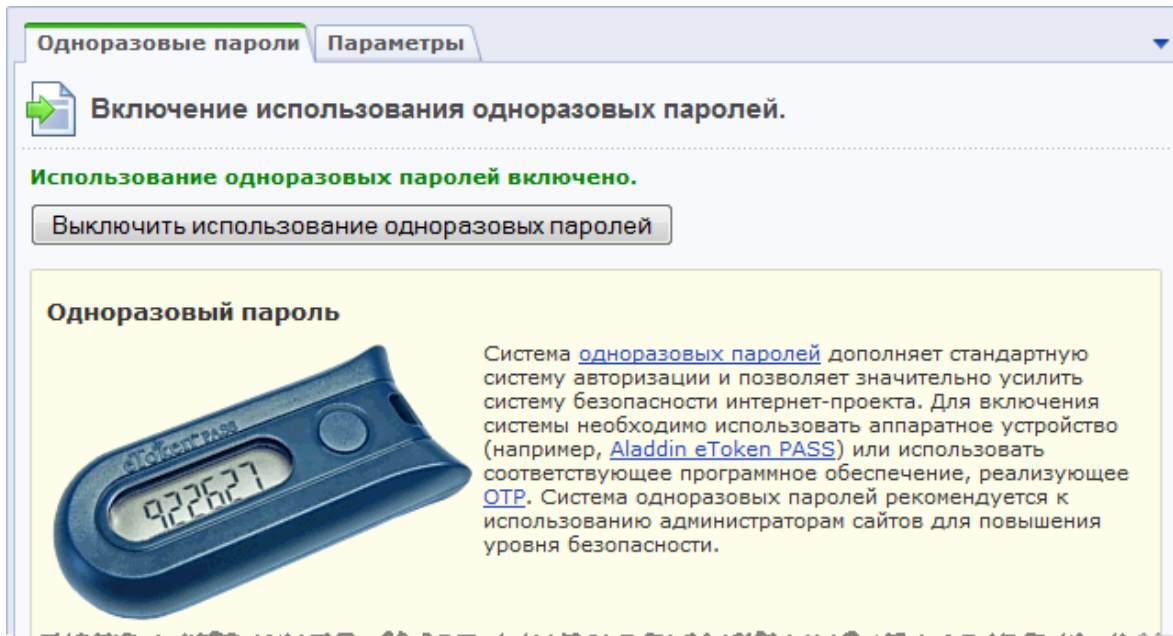
Одноразовые пароли

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.

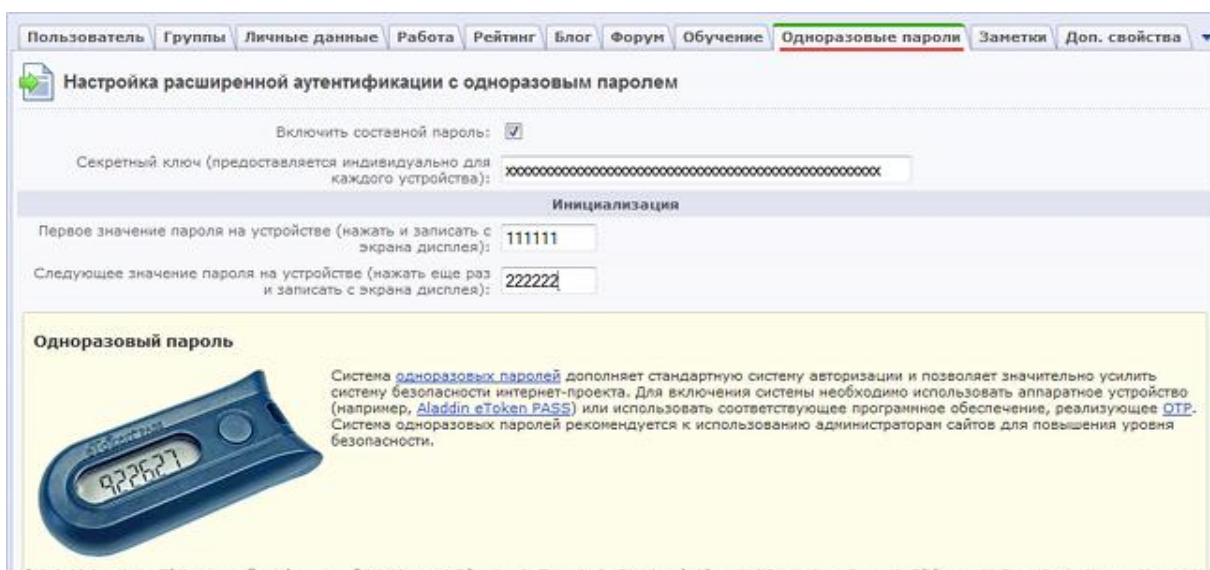
⚠ Примечание: для защиты проекта на повышенном уровне система использования одноразовых паролей должна быть включена.



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**).



Если использование одноразовых паролей включено, то в форме редактирования параметров пользователя (*Настройки > Пользователи > Список пользователей*) появляется дополнительная закладка **Одноразовые пароли**, т.е. механизм использования одноразового пароля настраивается отдельно для каждого 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).
- 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 рисунке ниже) вводится в поле **Пароль** стандартной формы авторизации на сайте сразу после обычного пароля (см. 1 на рисунке ниже) без пробелов.

Логин: admin

Пароль: [1] [2]

Запомнить меня на этом компьютере

[Забыли свой пароль?](#)

[Регистрация](#)

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**, произойдет нарушение синхронизации счетчика генерации, и пользователь не сможет выполнить вход на сайт.

Одноразовые пароли | Параметры

Настройка параметров одноразовых паролей.

Размер окна проверки паролей: 10

В этом случае необходимо выполнить повторную синхронизацию пользователя с устройством – привести значение на сервере в соответствие значению, хранящемуся в устрой-



стве. 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.

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

⚠ Примечание: *Кроме физических устройств для системы одноразовых паролей можно использовать программные средства. Существует разработанные компанией 1С-Битрикс приложения для **Apple iOS, Android OS**.*

Контроль целостности

Форма, расположенная на странице **Контроль целостности** ([Настройки > Проактивная защита > Контроль целостности](#)), служит для выполнения проверки целостности 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.



Контроль целостности скрипта Выбор действия

Целостность скрипта контроля

*Пароль: ●●●●●●●●

Придумайте и запомните пароль. Рекомендуется использовать пароль длиной не менее 10 символов, состоящий из латинских букв и цифр.

*Пароль еще раз: ●●●●●●●●

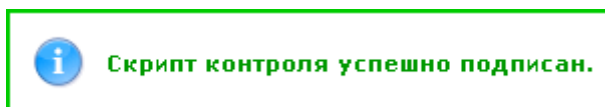
*Ключевое слово: bitrix

Произвольное слово, которое вы должны запомнить. Это слово должно отличаться от пароля. Если при следующем запуске кодовое слово будет отличаться от введенного вами, скрипт контроля файлов был изменен.

Далее >>

Нажмите кнопку **Далее**.

Если вы не ошиблись при подтверждении пароля, то отобразится 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:

Контроль целостности скрипта **Выбор действия**

Выбор действия

*Действие: Проверить файлы
 Собрать информацию по файлам

<< В начало Далее >>

- Нажмите кнопку **Далее**. Откроется форма сбора данных.



Контроль целостности скрипта | Выбор действия | **Сбор данных** | Отчет

Сбор данных

*Область сбора данных:

- ядро (/bitrix/modules)
- системная область (/bitrix)
- публичная часть

*Расширения файлов:

*Пароль для шифрования:

Время выполнения шага (сек):

<< В начало | Далее >>

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

Контроль целостности скрипта | Выбор действия | Сбор данных | **Отчет**

Отчет

Обработка файлов завершена

Успешно обработано файлов: 20233.
Для того, чтобы скачать файл с результатом, нажмите на [ЭТУ ССЫЛКУ](#).

<< В начало

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.



- Введите пароль, которым вы подписали скрипт контроля и нажмите кнопку **Далее**.

Контроль целостности скрипта Выбор действия


Целостность скрипта контроля

*Пароль: ●●●●●●●●

При проверке целостности введите тот пароль, с которым вы устанавливали ключ.

Далее >>

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

 Текущее ключевое слово 'bitrix'. Если это слово отличается от введенного вами ранее, файл скрипт контроля скомпрометирован.

⚠ 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 до более ранней версии модуля).

- На закладке **Выбор действия** отметьте опцию **Проверить файлы**.

Контроль целостности скрипта Выбор действия

Выбор действия

*Действие: Проверить файлы
 Собрать информацию по файлам

<< В начало Далее >>

- Нажмите кнопку **Далее**. Откроется форма выбора файла с верификационными данными.



The screenshot shows the 'Выбор файла' (File Selection) step. At the top, there are tabs: 'Контроль целостности скрипта', 'Выбор действия', 'Выбор файла' (active), 'Проверка данных', and 'Отчет'. Below the tabs, the title 'Выбор файла' is displayed. Underneath, there is a sub-section 'Выбор файла с верификационными данными' (File selection with verification data). A table lists files with columns: 'Дата' (Date), 'Регион' (Region), 'Расширения' (Extensions), and 'Действия' (Actions). One file is selected with a radio button. Below the table, there is a section 'Загрузка файла с верификационными данными' (Upload file with verification data) with a text input field and an 'Обзор...' (Browse...) button. At the bottom, there are navigation buttons: '<< В начало' and 'Далее >>'.

	Дата	Регион	Расширения	Действия
<input checked="" type="radio"/>	13.05.2010 12:17:46	ядро (/bitrix/modules) системная область (/bitrix) публичная часть	php, js	Удалить

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

The screenshot shows the 'Проверка данных' (Data Check) step. At the top, there are tabs: 'Контроль целостности скрипта', 'Выбор действия', 'Выбор файла', 'Проверка данных' (active), and 'Отчет'. Below the tabs, the title 'Проверка данных' is displayed. There is a field for '*Пароль для дешифрования:' (Password for decryption) with a masked input field. Below it, there is a field for 'Время выполнения шага (сек):' (Step execution time (sec)) with the value '30'. At the bottom, there are navigation buttons: '<< В начало' and 'Далее >>'.

- 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:

The screenshot shows the 'Отчет' (Report) step. At the top, there are tabs: 'Контроль целостности скрипта', 'Выбор действия', 'Выбор файла', 'Проверка данных', and 'Отчет' (active). Below the tabs, the title 'Отчет' is displayed. The main content area shows 'Обработка файлов завершена' (File processing completed) and 'Отличия не найдены' (No differences found). At the bottom, there is a navigation button: '<< В начало'.

Веб-антивирус

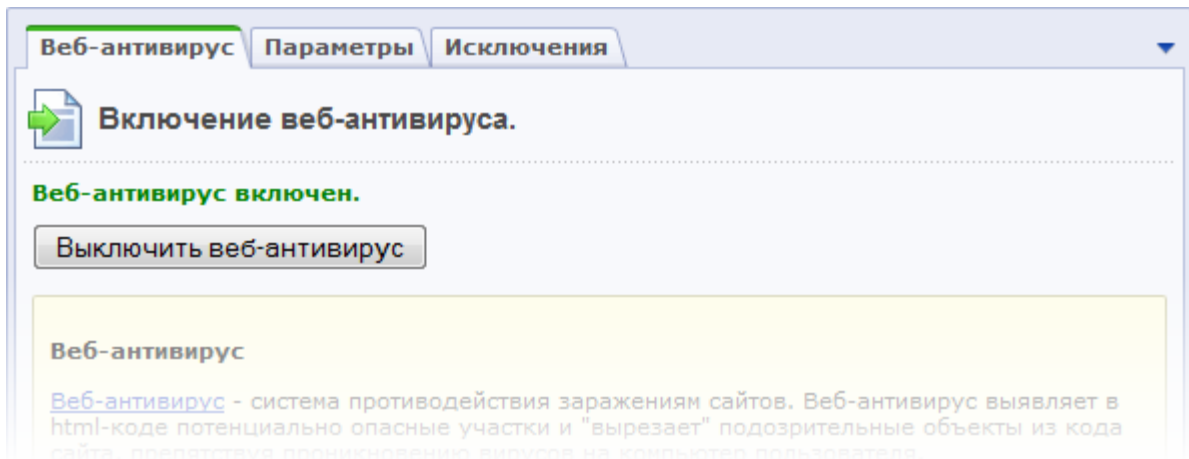
Веб-антивирус - система противодействия заражениям сайтов. Веб-антивирус выявляет в html-коде потенциально опасные участки и "вырезает" подозрительные объ-



екты из кода сайта, тем самым препятствуя проникновению вирусов на компьютер пользователя.

⚠ Внимание! 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**).



По умолчанию веб-антивирус всегда включен. Отключая его, вам необходимо понимать, что вы снижаете контроль за безопасностью своего сайта. Не смотря на ограничения доступа из Всемирной сети, корпоративный проект можно инфицировать.

О времени заражения вашего проекта никто вас заранее не предупредит. С целью уменьшения нагрузки на сервер веб-антивирус не проводит автоматически проверку с заданной периодичностью, а проверяет код непосредственно в момент его отдачи браузеру. Вирус будет обнаружен именно в этот момент, а уведомления об обнаруженном вирусе администратор сайта будет получать в интервале, заданном в настройках веб-антивируса. Прежде всего настроим периодичность оповещения и параметры реакции антивируса на обнаруженный подозрительный код.

Перейдите на страницу [Настройки](#) > [Проактивная защита](#) > [Веб-антивирус](#), на вкладку **Параметры**. Откроется форма настройки параметров реагирования на угрозы.

В поле **Интервал оповещения (минуты)** можно изменить периодичность, с которой производится уведомление администратора, если модуль обнаружит вирус. Значение можно оставить по умолчанию.

Вне зависимости от выбранного режима работы (только **Оповестить** или **Вырезать**) пользователь не получает сообщения. Но в первом случае система выдает посетителю сайта вместе с кодом запрошенной страницы код подозрительного объекта (и компьютер сотрудника тоже может заразиться вирусом). Во втором случае подозрительный код вырезается из отдаваемой пользователю страницы. В любом случае администратор получает уведомление (на почту и в **Журнал вторжений**).



Веб-антивирус Параметры Исключения

Настройка параметров оповещения о заражении.

Действия при обнаружении вируса: Вырезать из кода сайта
 Только занести в журнал и оповестить администратора

Интервал оповещения (минуты):

Сохранить Применить Отменить

⚠ Примечание: Строго говоря, вирус не присутствует на сайте. На нем есть ссылка на связку скриптов и вирус, которыми заражаются посетители проекта. Заражение может реализоваться двумя способами:

- **Первый:** на каком-либо сайте выставляется ссылка на вирус. Задача вируса — заразить посетителей. Если этот сайт посещает некоторый человек с устаревшим браузером, то связка скриптов (эксплоитов) пробивает браузер и заражает посетителя. Компьютер посетителя пополняет армию ботов в какой-нибудь зомби-сети.
- **Второй:** на этот сайт заходит не просто посетитель, а администратор другого сайта и тоже заражается. В этом случае вирус не просто пополняет зараженным компьютером армию ботов, а находит на компьютере сохраненные пароли от серверов, обслуживаемых этим администратором. Пароли передаются автору вируса, который заходит на сайты с помощью похищенных паролей и добавляет на них ссылки на свой вирус.

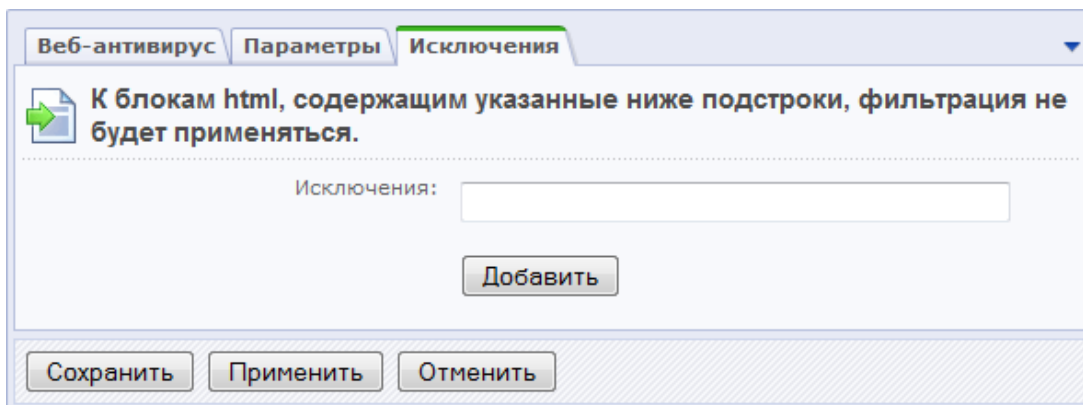
С полем **Действия** при обнаружении вируса нужно быть внимательными. Проблема заключается в том, что любая система может допускать ложные срабатывания. Количество ложных срабатываний веб-антивируса минимально, но, к сожалению, они все же встречаются. Иными словами, если вы выберете параметр **Вырезать** из кода сайта, то в случае ошибки можете нанести ущерб самим себе.

Как отличить ошибку от ложного срабатывания?

Работа веб-антивируса основана на эвристическом анализе потенциально опасных блоков в HTML-коде. В целом распознавание "вирусных" и легитимных блоков может быть сложной задачей даже для человека, а не только для программы.

Ключевое отличие блоков, действительно содержащих ссылки на вирусы, от ложных срабатываний — это то, что ошибочно принятые за вирус блоки были явно добавлены вашим программистом. Кто добавил "вирусные" блоки и откуда они взялись, вы не знаете.

Если вы уверены, что блок, на который срабатывает веб-антивирус, легитимный и не содержит ссылки на загрузку вирусов, то данное срабатывание антивируса является ложным. В этом случае вам необходимо взять некоторую строку из этого блока (достаточно длинную и достаточно уникальную) и добавить ее в исключения веб-антивируса на одноименной вкладке страницы **Веб-антивирус**. В результате антивирус перестанет срабатывать на любые обрабатываемые им блоки, содержащие указанную строку.



Маска исключений должна быть достаточно уникальной, но при этом покрывать все блоки данного типа (если они генерируются динамическими). Вероятность того, что при добавлении достаточно длинной строки (содержащей, например, имена нормальных переменных или функций из корректного блока) случайно будет разрешен вирус, невелика.

Если срабатывание антивируса не ложное, то все будет намного сложнее. Удалить обнаруженный код — дело несложное. Нужно понять, как он оказался на вашем сайте. Почти со стопроцентной уверенностью можно утверждать, что "вирусный" блок был помещен злоумышленником с помощью пароля, похищенного через компьютер какого-либо сотрудника, имеющего доступ на сервер через FTP (SSH, SFTP и т. п.). Этот компьютер заражен вирусом, укравшим пароль от сервера.

При обнаружении вируса на сайте

- необходимо проверить все компьютеры людей, имеющих доступ к сайту (в том числе к **Панели администрирования**), с помощью персонального антивирусного программного обеспечения;
- после того как все такие компьютеры были вылечены, нужно сменить все пароли от вашего сервера всем пользователям;
- только после этого можно вычищать весь сторонний код на сервере. При вычищении кода обратите внимание на сроки обнаружения заражения и сроки создания резервной копии (бэкапа) сайта. Если по каким-то причинам резервное копирование делалось после даты заражения, бэкапом пользоваться нельзя.

Для отслеживания изменившихся файлов рекомендуется использовать инструмент **Контроль целостности**. Если же вы не используете данный инструмент, то в общем случае поиск всех изменений, оставленных хакером, может быть таким:

- поиск по всем файлам на сервере, содержащем строки из блока, на который сработал веб-антивирус;
- поиск и ручная проверка всех недавно изменившихся файлов;
- анализ логов HTTP сервера.

При этом остается надеяться, что хакер оказался не слишком хитрым, ограничился внедрением JavaScript со ссылками на вирус и не оставил за собой скрытых бэкдоров (что, в общем-то, бывает достаточно редко).



⚠ 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"
```

Стоп-лист

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

Активность	Сортировка	Название	Маски путей	Маски исключений	IP-адреса	IP-адреса исключений
Да	100	Запрет на доступ к сайту	/*		192.168.0.55	
Да	200	Запрет на доступ к административной части	/bitrix/admin/*		192.168.0.100-192.168.0.255	192.168.0.200

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 в качестве активной реакции на вторжение выбрано **Добавить IP-адрес атакующего в стоп-лист на <количество> минут**).



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

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

- 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.