

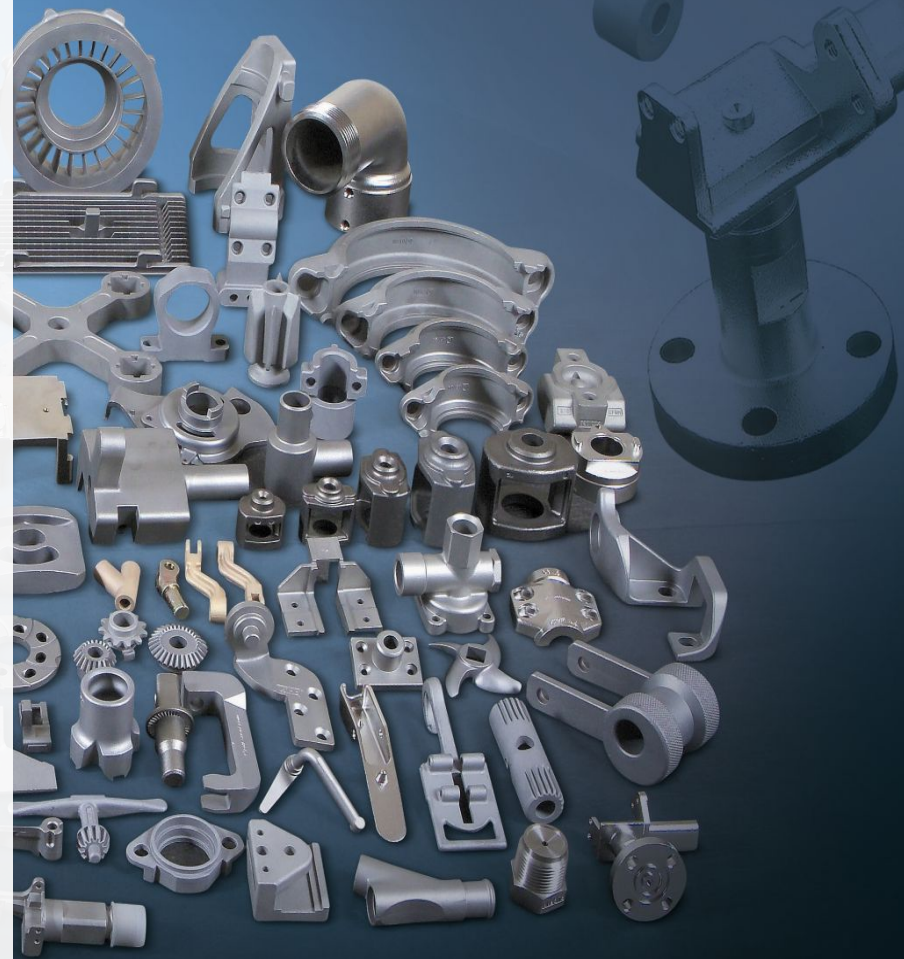
# Безопасность интернет-проектов: основные проблемы разработки и пути решений



# → Сайты сегодня – набор запчастей

Большая часть современных сайтов - набор запчастей

- низкий уровень стандартной разработки
- отсутствие единой концепции безопасности
- несколько аккаунтов для одного пользователя
- не обновляемое ПО, особенно после модификации



# О безопасности сайта думают в последнюю очередь!

- индивидуальные разработчики думают о безопасности сайтов в самую последнюю очередь
- клиенты не готовы платить за безопасность интернет-проектов
- подразумевается, что разработчик должен этим заниматься, но у него не остается ни времени, ни бюджета

## → Хостинг часто не защищен

- зачастую уровень администрирования серверов и хостинга *критически низкий*
- редко используются системы автоматического мониторинга

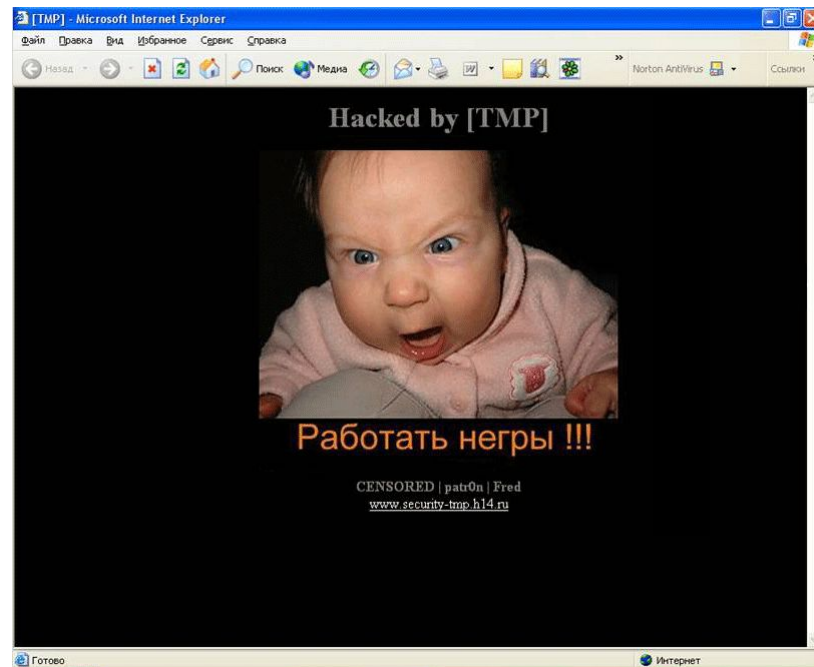


# Безопасность сайта

## → Веб-сайт - часть корпоративной инфраструктуры.

Взлом корпоративного сайта - это удар по репутации и имиджу компании. Очень неприятное в подобных событиях - огласка происшествия. Но потеря данных с сайта, информации о клиентах – это уже прямые убытки. И огласка таких происшествий происходит далеко не всегда.

Чем серьезнее компания и известнее ее имя и продукты, тем существеннее бывают риски и убытки от взлома корпоративного сайта.



**→ Платформа «1С-Битрикс» - это комплексное решение с единой системой безопасности:**

- единая политика безопасности
- единая система авторизации;
- единый бюджет пользователя для всех модулей
- трехуровневая система разграничения прав доступа
- независимость системы контроля доступа от бизнес-логики страницы
- смена пароля
- запомнить авторизацию
- возможность шифрования информации при передаче
- система обновлений SiteUpdate
- независимое журналирование выполняемых страниц в модуле Статистики
- политика работы с переменными и внешними данными
- методика двойного контроля критически опасных участков кода
- политика работы с пластиковыми картами

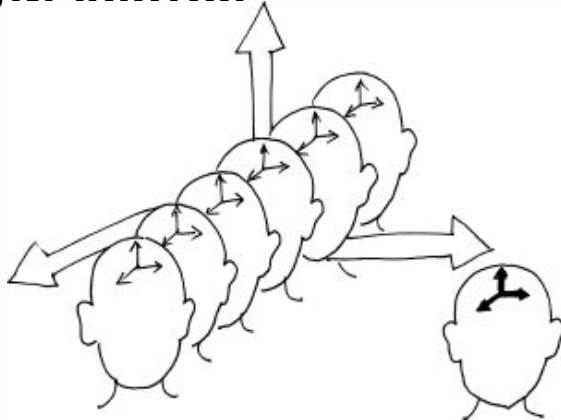
- Перед выпуском модуля идет обязательное тестирование разработчиками на внутренних серверах с разными базами данных, операционными системами и версиями РНР
- Отдел тестирования проверяет на соответствие бизнес-функциональности и наличие ошибок
- Отдел безопасности проверяет на наличие уязвимостей
- Модуль поступает в бета-тестирование клиентам и партнерам



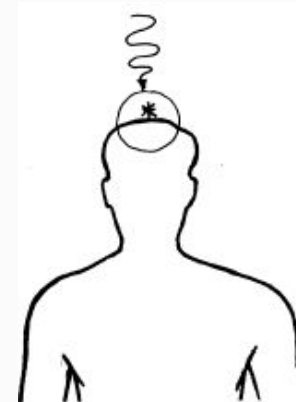
**Разработчики работают в компании по 5-8 лет, но все равно допускают ошибки в безопасности. Почему?**

# Психология хакера и разработчика

→ Психология хакера и разработчика принципиально отличаются



Как мыслит  
разработчик...



... и как мыслит  
хакер

Профессиональным веб-разработчик становится только через 3-5 лет и при активном контроле со стороны специалиста по веб-безопасности





# Категории

## хакеров

Студенты, ИТ специалисты  
начального уровня

- пробуют силы на первых попавшихся сайтах
- нет понимания последствий для жертвы
- нет осознания юридической личной ответственности
- редко зарабатывают на хакерстве как на бизнесе

## Профессиональные специалисты

- прекрасный технический багаж
- никогда не светятся в тусовках, не кривляются
- делают только на заказ и только за деньги
- активно работают на службы безопасности

**Соотношение разработчиков  
к хакерам 1:100**

# Платный аудит безопасности

- Индивидуальная проверка проектов специалистами по веб-безопасности
- Большой объем работы
- Постоянные изменения вносимые в интернет-проекты
- Нехватка специалистов
- Отсутствие сформированной практики аудитов

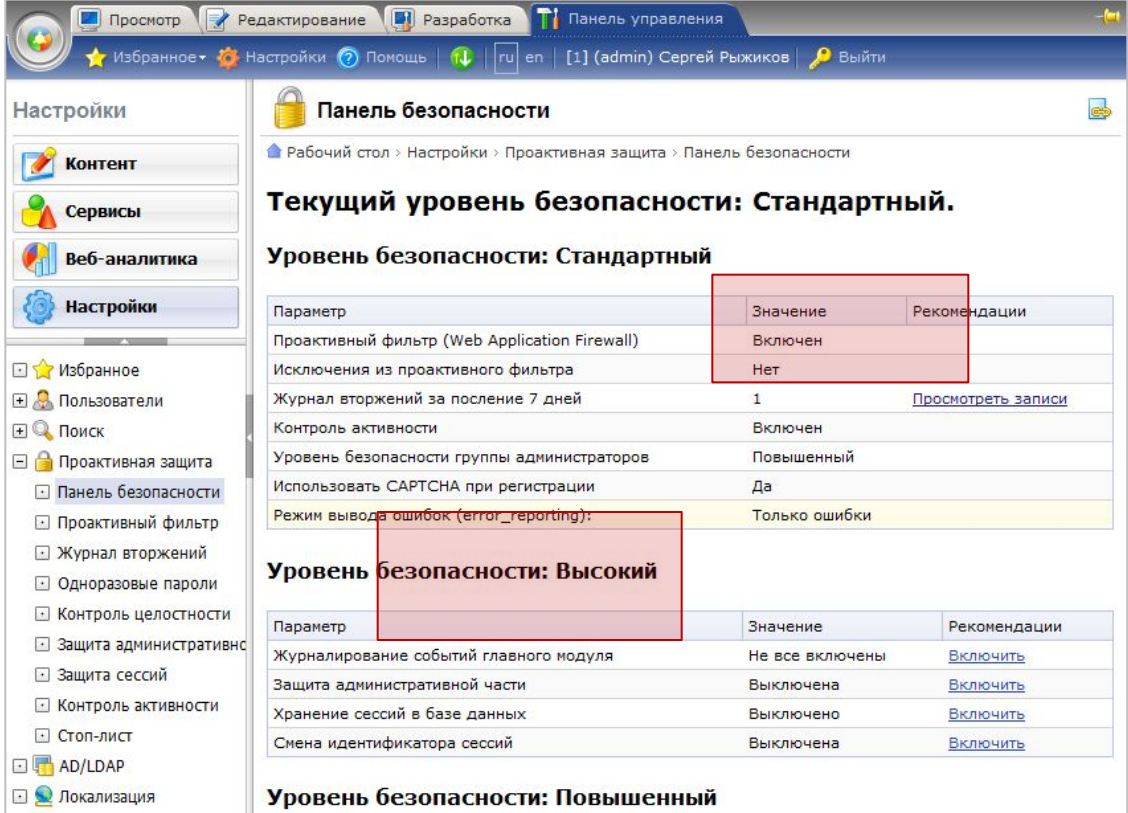
# Комплекс «Проактивная защита» Инструменты безопасности

- Web Application Firewall (Проактивный фильтр защиты от атак)
- Веб-антивирус
- Аутентификация и система составных паролей
- Технология защиты сессии пользователя
- Активная реакция на вторжение
- Контроль целостности системы
- Защита от фишинга
- Шифрование данных
- Групповые политики безопасности
- Защита при регистрации и авторизации



# Безопасность: Панель безопасности

→ Оценка уровней безопасности веб-проекта



**Панель безопасности**

Рабочий стол > Настройки > Проактивная защита > Панель безопасности

**Текущий уровень безопасности: Стандартный.**

**Уровень безопасности: Стандартный**

Параметр	Значение	Рекомендации
Проактивный фильтр (Web Application Firewall)	Включен	
Исключения из проактивного фильтра	Нет	
Журнал вторжений за последние 7 дней	1	<a href="#">Просмотреть записи</a>
Контроль активности	Включен	
Уровень безопасности группы администраторов	Повышенный	
Использовать CAPTCHA при регистрации	Да	
Режим вывода ошибок (error_reporting):	Только ошибки	

**Уровень безопасности: Высокий**

Параметр	Значение	Рекомендации
Журналирование событий главного модуля	Не все включены	<a href="#">Включить</a>
Защита административной части	Выключена	<a href="#">Включить</a>
Хранение сессий в базе данных	Выключено	<a href="#">Включить</a>
Смена идентификатора сессий	Выключена	<a href="#">Включить</a>

**Уровень безопасности: Повышенный**

# Проактивный фильтр Web Application FireWall

- Распознает большинство опасных угроз и блокирует вторжения на сайт
  - **XSS** - cross site scripting (CSS)
  - **SQL инъекции**
  - **PHP Including**
  - часть атак, связанных с обходом каталогов
- Экранирует приложение от наиболее активно используемых атак
- Фиксирует попытки атаки в журнале
- Информировывает администратора о случаях вторжения



# Технология одноразовых паролей

→ Технология одноразовых паролей (One Time Password - OTP) с использованием брелков Aladdin eToken PASS позволяет быть однозначно уверенным, что на сайте авторизуется именно тот человек, которому выдали брелок.

Корректность работы электронных ключей eToken PASS для системы «1С-Битрикс: Управление сайтом 8.0» подтверждается соответствующим **сертификатом компании Aladdin**, выданным на основании серии испытаний.

eToken™  
YOUR KEY TO SECURITY



Aladdin®  
SECURITY SOLUTIONS



# Технология защиты авторизованных сессий

- Сессия пользователя – это **ключевой объект атаки** на веб-сайт с целью получения сессии авторизованного пользователя
- В повышенных режимах безопасности сессия будет полностью меняться раз в несколько минут (в зависимости от настройки)
- Механизм хранения сессий в базе данных для исключения ошибок конфигурирования виртуального хостинга, ошибок настройки прав доступа в временным каталогам и ряда других проблем настройки операционной среды

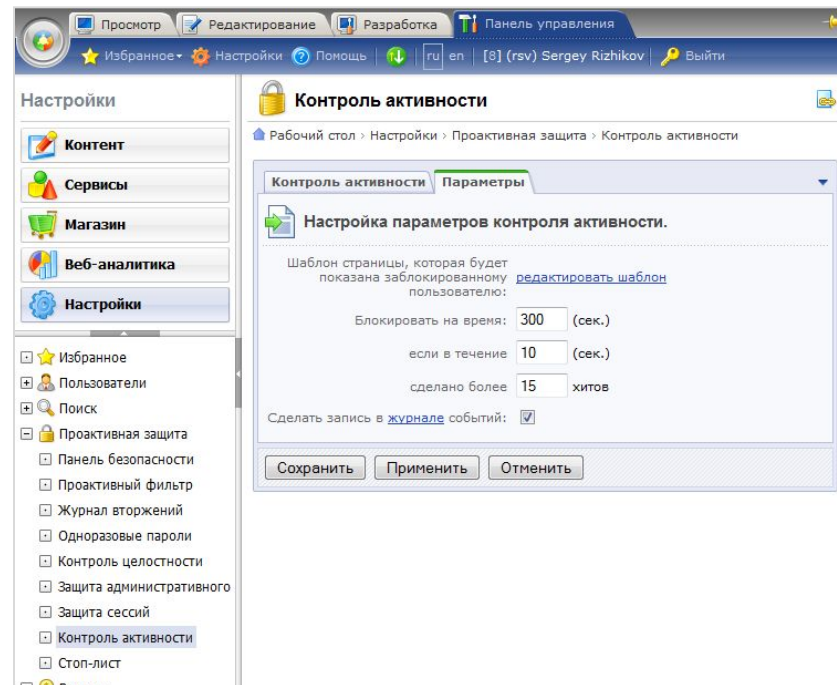


1С·БИТРИКС



# Контроль активности

→ Обеспечивает защиту от DDoS атак на веб-приложения, от автоматизированных роботов, которые извлекают контент, спамят и всячески подстраиваются под посетителей







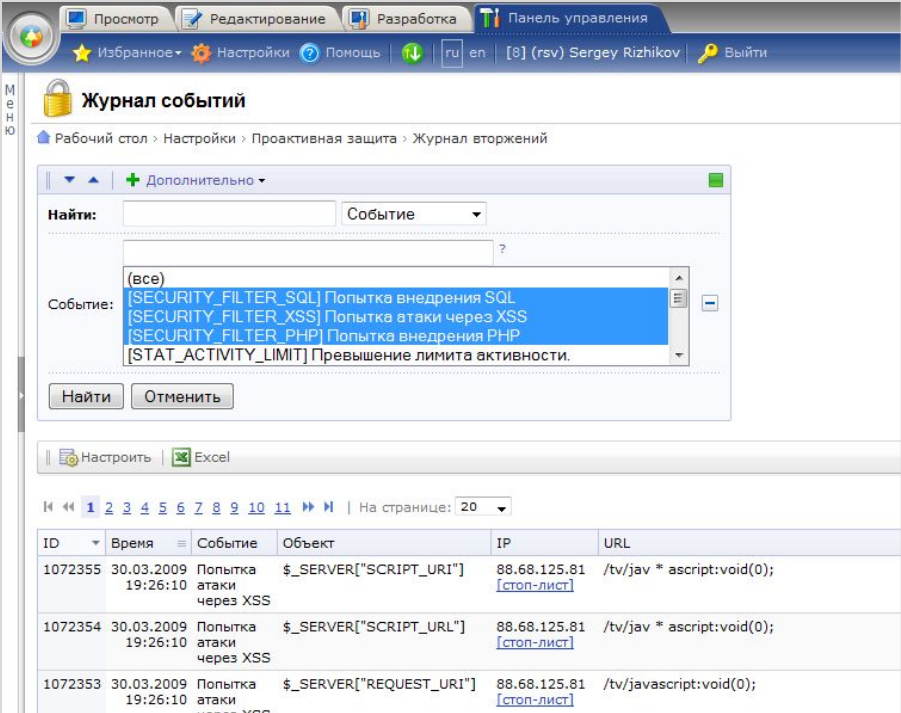
# Шифрование данных

- Полная поддержка работы по SSL.
- Один из ключевых вариантов обеспечения защищенности проекта – шифрование данных и сессионных значений при передаче между пользователем и сайтом.
- Зачастую разделяются режимы работы пользователей и администратора.
- Новые параметры позволяют использовать несколько режимов работы с сайтом для пользователей при установленном SSL сертификате.



# Журнал вторжений

➔ В журнале вторжений ведется запись попыток внедрения SQL, атак через XSS и внедрения PHP.



The screenshot shows the 'Журнал событий' (Event Journal) interface in 1C-Bitrix. The breadcrumb trail is: Рабочий стол > Настройки > Проактивная защита > Журнал вторжений. A search window is open with 'Событие' (Event) selected in the dropdown. The search results list several events, with the first one selected:

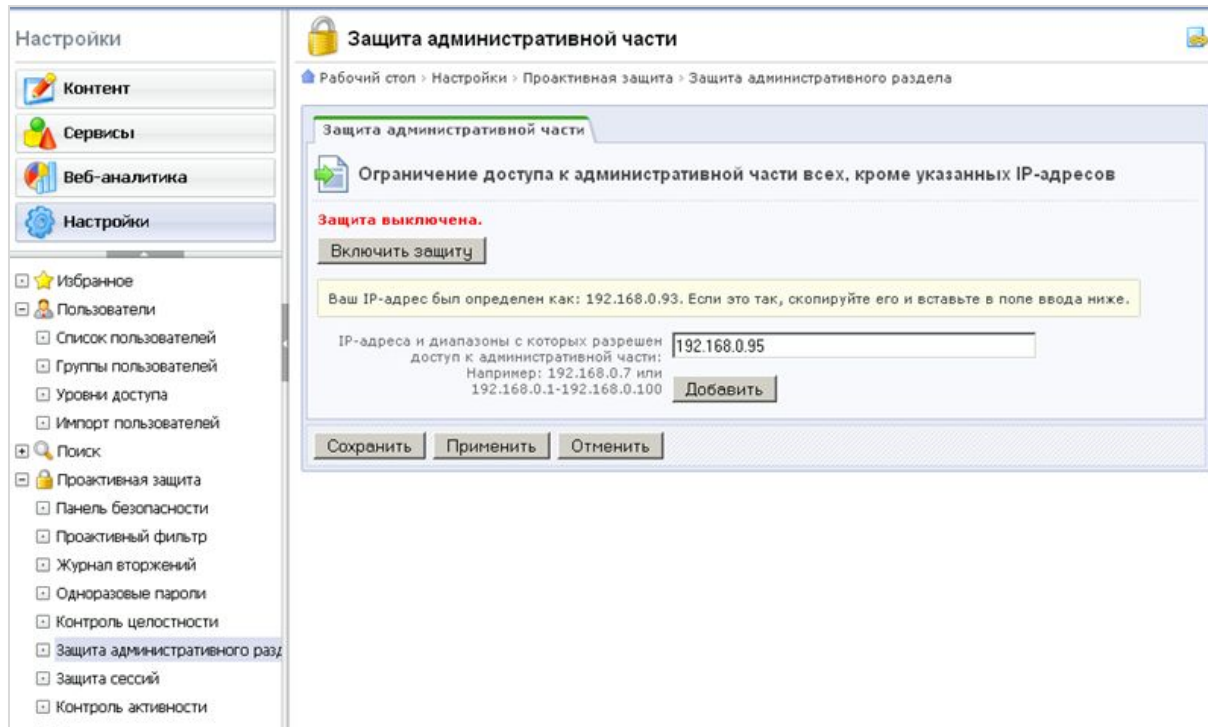
- Событие: [SECURITY\_FILTER\_SQL] Попытка внедрения SQL
- [SECURITY\_FILTER\_XSS] Попытка атаки через XSS
- [SECURITY\_FILTER\_PHP] Попытка внедрения PHP
- [STAT\_ACTIVITY\_LIMIT] Превышение лимита активности.

Below the search window, there are navigation controls and a table of events:

ID	Время	Событие	Объект	IP	URL
1072355	30.03.2009 19:26:10	Попытка атаки через XSS	\$_SERVER["SCRIPT_URI"]	88.68.125.81	/tv/jav * ascript:void(0); <a href="#">[стоп-лист]</a>
1072354	30.03.2009 19:26:10	Попытка атаки через XSS	\$_SERVER["SCRIPT_URL"]	88.68.125.81	/tv/jav * ascript:void(0); <a href="#">[стоп-лист]</a>
1072353	30.03.2009 19:26:10	Попытка атаки XSS	\$_SERVER["REQUEST_URI"]	88.68.125.81	/tv/javascript:void(0); <a href="#">[стоп-лист]</a>

# Защита административных разделов по IP

- ➔ Защита позволяет строго регламентировать сети, которые считаются безопасными и из которых сотрудникам разрешается администрировать сайт



Настройки

- Контент
- Сервисы
- Веб-аналитика
- Настройки

Избранное

- Пользователи
  - Список пользователей
  - Группы пользователей
  - Уровни доступа
  - Импорт пользователей
- Поиск
- Проактивная защита
  - Панель безопасности
  - Проактивный фильтр
  - Журнал вторжений
  - Одноразовые пароли
  - Контроль целостности
  - Защита административного раздела
  - Защита сессий
  - Контроль активности

Защита административной части

Рабочий стол > Настройки > Проактивная защита > Защита административного раздела

Защита административной части

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

**Защита выключена.**

Включить защиту

Ваш IP-адрес был определен как: 192.168.0.93. 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

192.168.0.95

Добавить

Сохранить Применить Отменить

➔ Стоп-лист ограничивает доступ посетителей к содержимому сайта. Все пользователи, которые попытаются зайти на сайт с IP адресами, включенными в стоп-лист, будут блокированы.

ID	Статус активности	Начало	Акт.	Сайт	IP адрес сети	Маска сети	Стат.
191	●	02.09.2011 11:48:38	Да	(все)			Да
189	●	25.07.2011 16:16:33	Да	(все)			Да
187	●	03.06.2011 10:22:56	Да	(все)			Да
183	●	17.05.2011 15:27:39	Да	(все)			Да
181	●	11.04.2011 15:23:33	Да	(все)			Да
179	●	30.03.2011 11:08:12	Да	(все)			Да
177	●	26.03.2011 19:23:36	Да	(все)			Да
175	●	23.03.2011 13:05:50	Да	(все)			Да
173	●	12.03.2011 15:38:47	Да	(все)			Да
171	●	12.03.2011 15:36:09	Да	(все)			Да
169	●	12.03.2011 15:33:34	Да	(все)			Да



# Контроль целостности системы

- Механизм расчета контрольных сумм всего проекта
- Раздельное вычисление для статических страниц и кода с возможностью видеть, когда менял обычный пользователь и когда менял веб-разработчик
- Пароль проверки не хранится на сайте
- Файл контрольных сумм можно отдельно сохранить у себя для проверки

**В любой момент вы можете проверить целостность ядра, системных областей, публичной части продукта**

- Фишинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, например, от имени социальных сетей (Facebook, ВКонтакте), банков (Ситибанк, Альфа-банк), прочих сервисов (Rambler, Mail.ru)
- Фишинг — одна из разновидностей социальной инженерии, основанной на незнании пользователями основ сетевой безопасности

При включенной защите все ссылки с сайта через редиректы защищаются дополнительным параметром индивидуальным для сайта и для этого перехода. Внешние переходы не будут работать



# Групповые политики безопасности

→ Выполняется проверка на длину пароля и на вхождение в пароль определенных групп символов (латинские буквы, цифры, знаки препинания)

Маска сети для привязки сохраненной авторизации:	<input checked="" type="checkbox"/> Не переопределять
	<input type="text"/>
Срок хранения авторизации, запомненной на компьютере пользователя (минут):	<input checked="" type="checkbox"/> Не переопределять
	<input type="text"/>
Срок действия контрольного слова для восстановления пароля (минут):	<input checked="" type="checkbox"/> Не переопределять
	<input type="text"/>
Минимальная длина пароля:	<input checked="" type="checkbox"/> Не переопределять
	<input type="text"/>
Пароль должен содержать латинские символы верхнего регистра (A-Z):	<input checked="" type="checkbox"/> Не переопределять
	<input type="checkbox"/>
Пароль должен содержать латинские символы нижнего регистра (a-z):	<input checked="" type="checkbox"/> Не переопределять
	<input type="checkbox"/>
Пароль должен содержать цифры (0-9):	<input checked="" type="checkbox"/> Не переопределять
	<input type="checkbox"/>
Пароль должен содержать знаки пунктуации (.,</?;:"'[]{} \ `~!@#\$%^&*()-_+=):	<input checked="" type="checkbox"/> Не переопределять
	<input type="checkbox"/>
Количество попыток ввода пароля до показа CAPTCHA:	<input checked="" type="checkbox"/> Не переопределять
	<input type="text"/>

# Регистрация и авторизация

- Подтверждение регистрации по email
- Поддержка авторизации OpenID и LiveID
- Детальная настройка CAPTCHA
- Вывод CAPTCHA после N неуспешных авторизаций

### Настройка параметров отображения CAPTCHA

Профиль:

Прозрачность текста в процентах от 0 до 100:

Нижняя граница случайного цвета фона:

Верхняя граница случайного цвета фона:

Количество кругов:

Нижняя граница случайного цвета круга:

Верхняя граница случайного цвета круга:

Линии поверх текста:

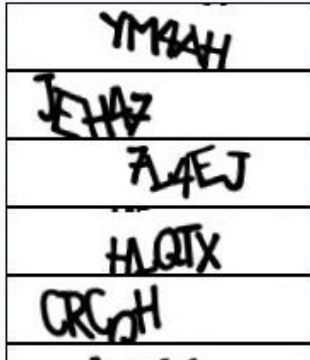
Количество линий:

Нижняя граница случайного цвета линии:

Верхняя граница случайного цвета линии:

Отступ текста слева:

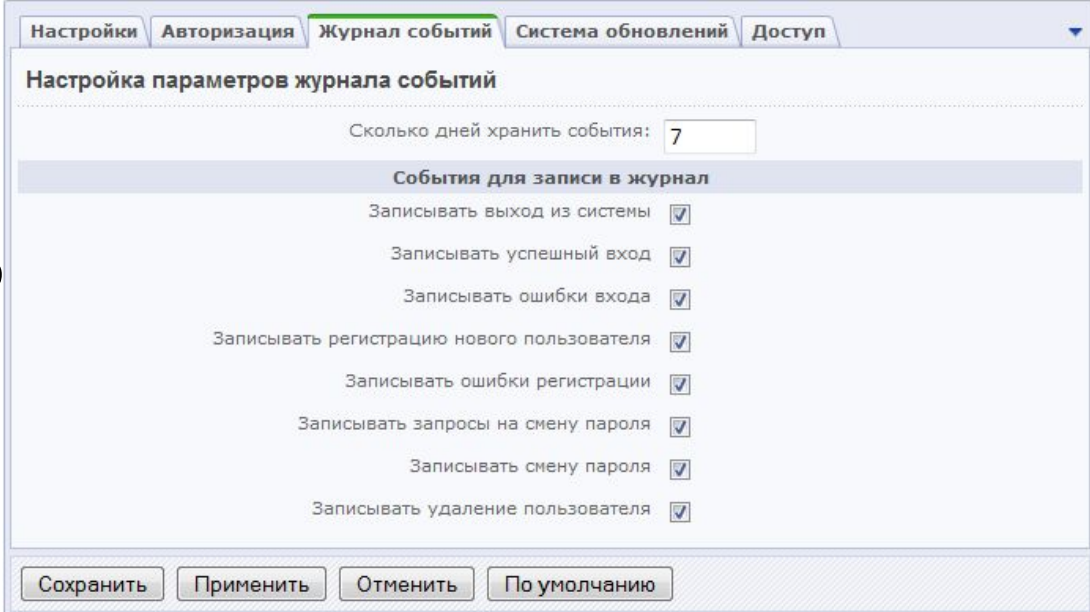
Размер шрифта:





# Журнал событий

→ В журнал заносятся события, связанные с авторизацией и регистрацией пользователей. Детально настраиваются фиксируемые события.



Настройки Авторизация **Журнал событий** Система обновлений Доступ

Настройка параметров журнала событий

Сколько дней хранить события:

**События для записи в журнал**

- 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

Сохранить Применить Отменить По умолчанию

# Модуль «Проактивная защита» включен в состав программных продуктов


- «1С-Битрикс: Управление сайтом» (все редакции, кроме «Старт»)
- Коробочная версия «1С-Битрикс24»





# Следите за

 [twitter.com/1C\\_Bitrix](https://twitter.com/1C_Bitrix)

 [facebook.com/1CBitrix](https://facebook.com/1CBitrix)

**Спасибо за внимание!**  
**Вопросы?**

