



**1С-БИТРИКС:**  
Управление сайтом



СИСТЕМА УПРАВЛЕНИЯ ИНТЕРНЕТ-ПРОЕКТАМИ

# Актуальные вопросы информационной безопасности веб-приложений

**Сергей Рыжиков**  
генеральный директор  
компании «1С-Битрикс»



## 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**



*Разработчики интернет-приложений зачастую не задумываются о безопасности.*



## **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





## Web-приложения и анализ рисков

- Анализ рисков. Где статистика?
- В 2006 году впервые количество обнаруженных Web-уязвимостей превысило «стандартные» проблемы  
*MITRE, анализ списка CVE*
- **Больше 7% Web-сайтов может быть «взломано» автоматически**
- **При экспертном анализе вероятность обнаружения критической уязвимости превышает 60%**  
*Web Application Security Consortium*

*По данным компании Positive Technologies*



# Исследование уязвимости Web-приложений, 2008 г.

- Объем исследования:
  - В автоматическом режиме – около 10000 узлов
  - Детальный анализ – около 1000 узлов

## Результаты исследования:

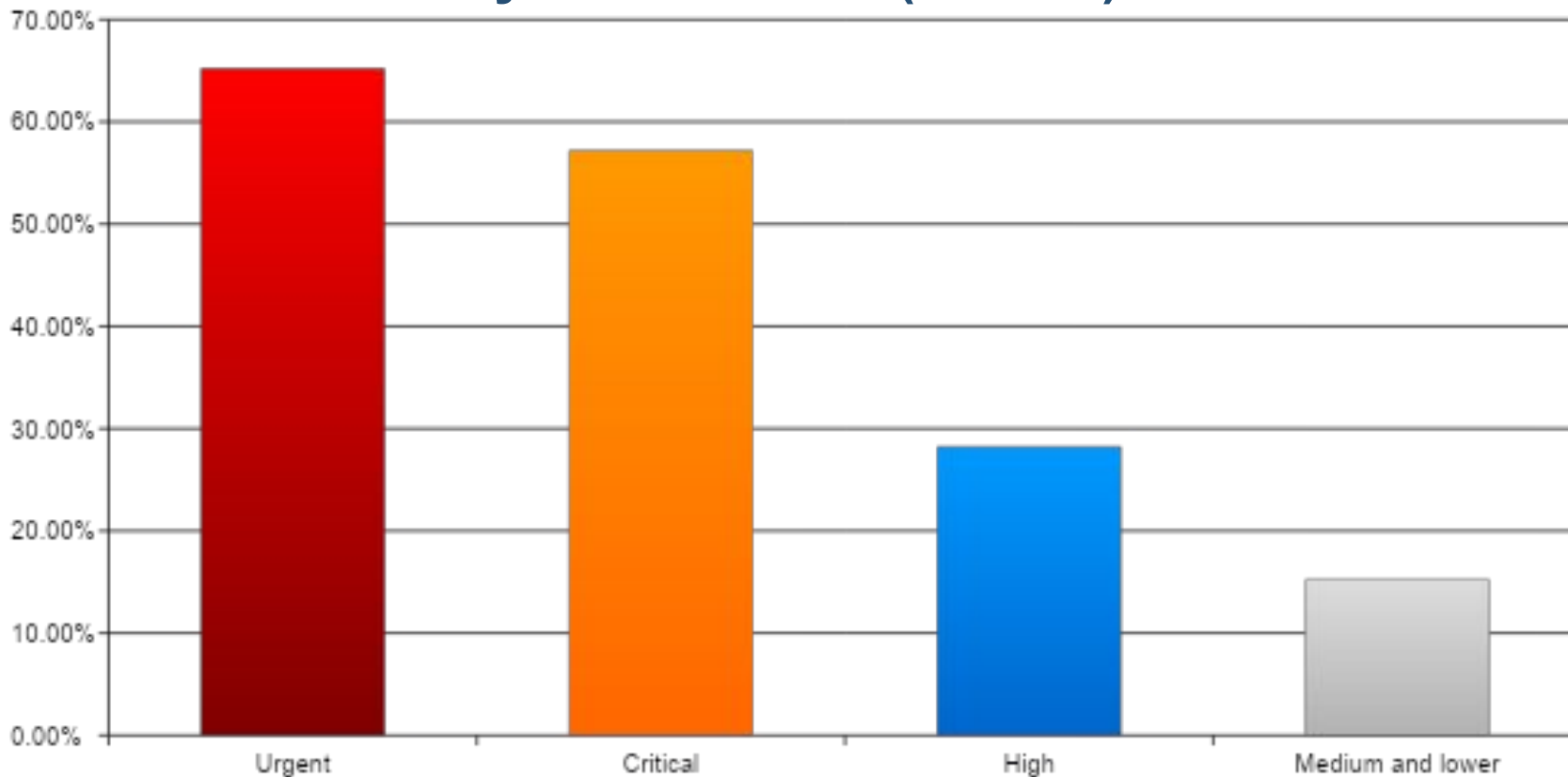
- Низкий уровень защищенности большинства Web-сайтов
- Автоматизация методов выявления и эксплуатации уязвимостей

Web Application Security Consortium  
предварительные данные

*По данным компании Positive Technologies*



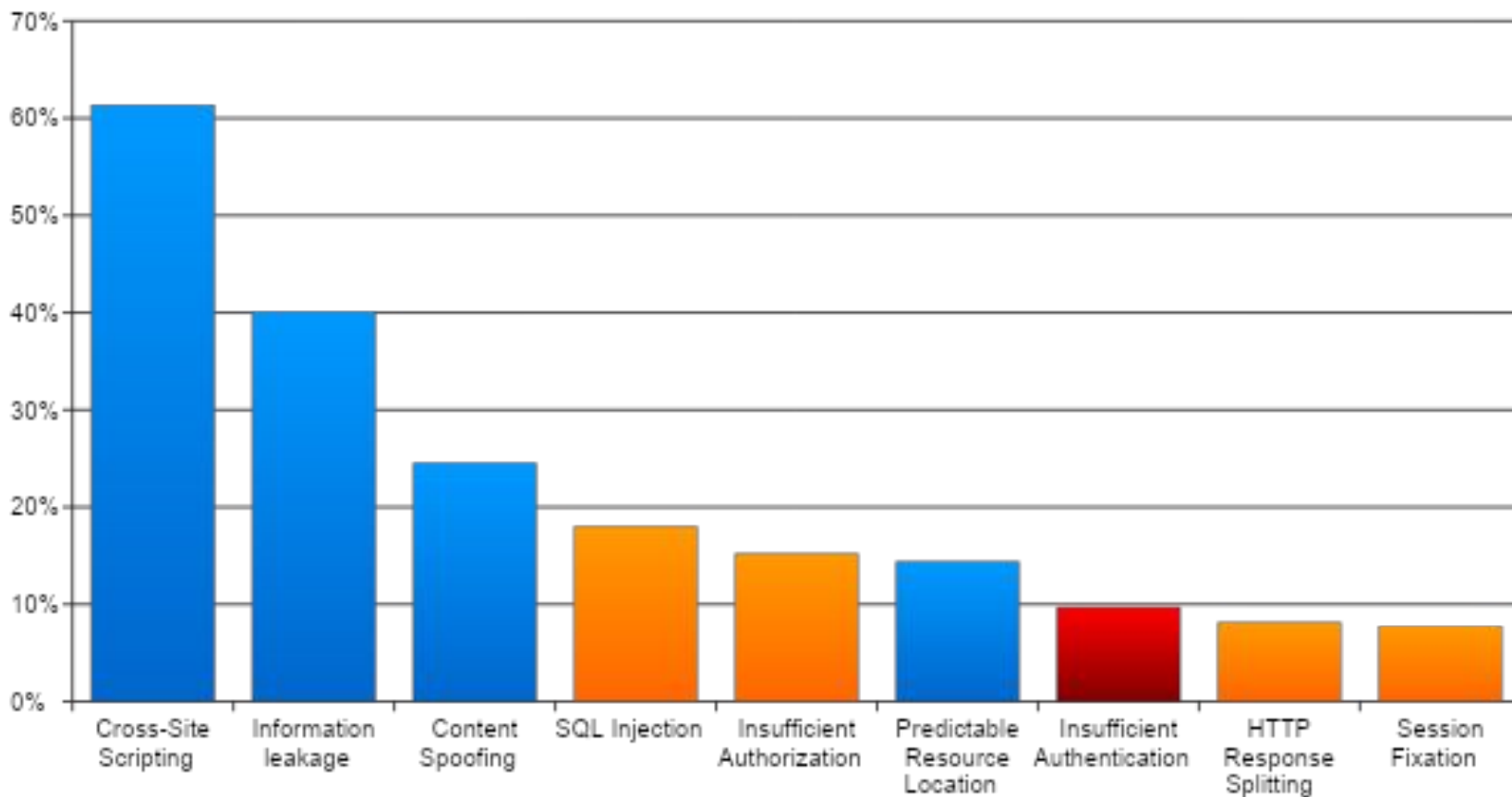
## Распределение веб-сайтов по уровню найденных уязвимостей (2008 г.)



*По данным компании Positive Technologies*



## Наиболее распространенные уязвимости

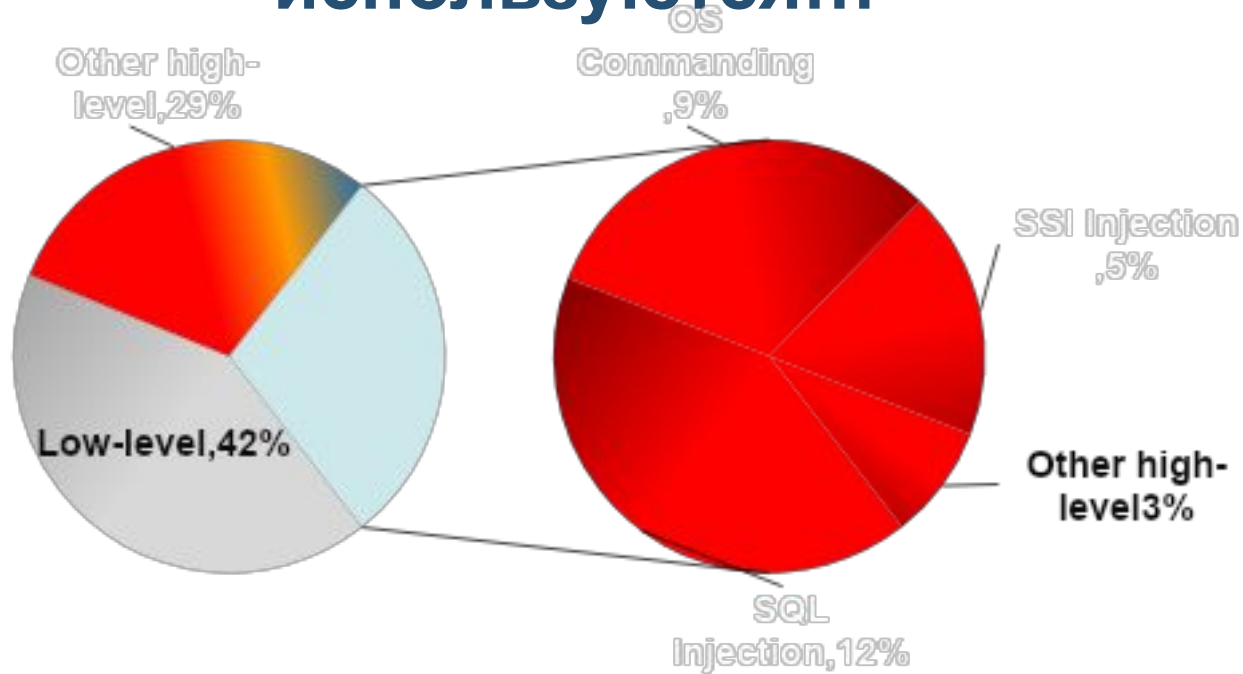


По данным компании Positive Technologies





## Для атаки на Web-сайт обычно используются...

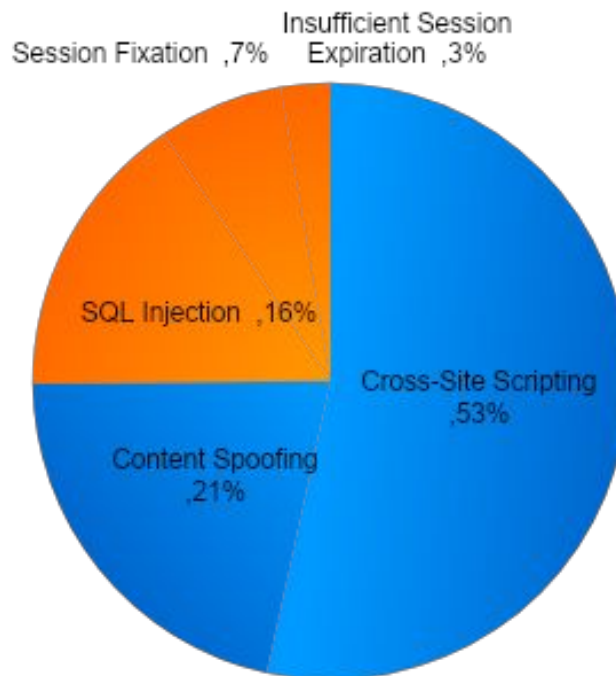


При анализе скомпрометированного Web-сайта обнаруживается “букет” уязвимостей, треть из которых могла быть использована нарушителем для атаки

*По данным компании Positive Technologies*



## Для атаки на пользователей Web-сайта обычно используются...



*По данным компании Positive Technologies*



## А как оперативно устраняются эти проблемы?

Class of Attack	% resolved	severity
Information Leakage	50%	urgent
Insufficient Authorization	42%	urgent
SQL Injection	66%	urgent
HTTP Response Splitting	83%	urgent
Directory Traversal	31%	urgent
Insufficient Authentication	26%	critical
Cross-Site Scripting	55%	critical
Abuse of Functionality	41%	critical
Cross-Site Request Forgery	48%	critical
Session Fixation	11%	critical
Brute Force	8%	high
Content Spoofing	26%	high
HTTP Response Splitting	31%	high
Information Leakage	34%	high
Predictable Resource Location	31%	high

Whitehat Security

По данным компании Positive Technologies



## Нашли «дыру»... Взломали... Что делать?

- Всех уволить!
- Найти эту дыру и закрыть ее!
- Проверить другие приложения
- Осознать проблему и заняться безопасностью



## Осознали... Что дальше?

- Периодический аудит
- Развитие внутренних компетенций
- Внедрение дополнительных средств защиты
- Создание собственных средств защиты



## Что дает проактивная защита?

- Страховка от возможных ошибок
- Безопасность сторонних разработок
- Своевременное обнаружение атак
- Соответствие PCI DSS



## 1С-Битрикс: Framework

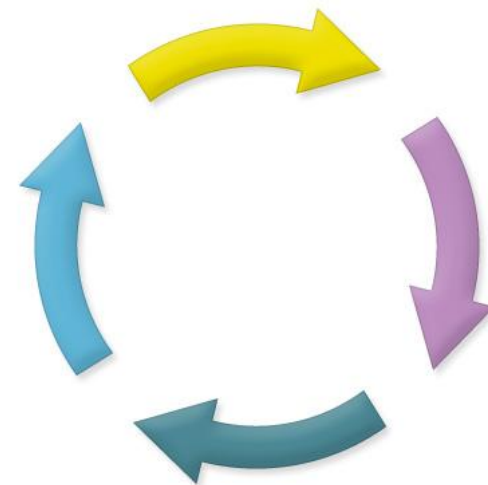
**Платформа «1С-Битрикс» - это комплексное решение с единой системой безопасности:**

- **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.**



## Цикл разработки

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



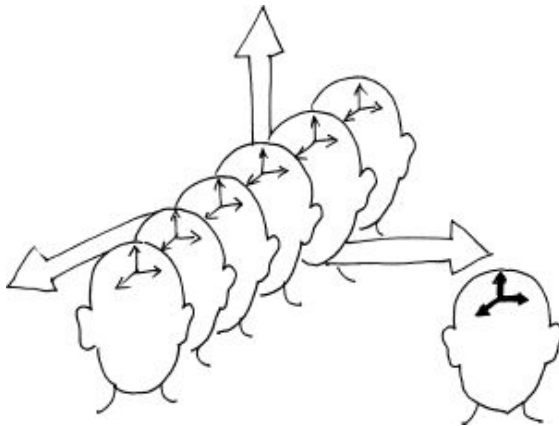
**Разработчики работают в компании по 5-8 лет, но все равно допускают ошибки в безопасности. Почему?**



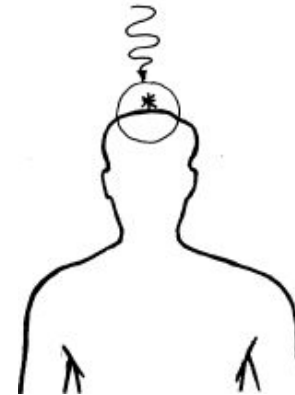


# Психология хакера и разработчика

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 крупных компаний

***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**

*Аудит профессиональными компаниями - такими как Positive Technologies - услуга комплексная, сложная и зачастую не подходит для массового рынка.*



## Новый подход к концепции веб-безопасности

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

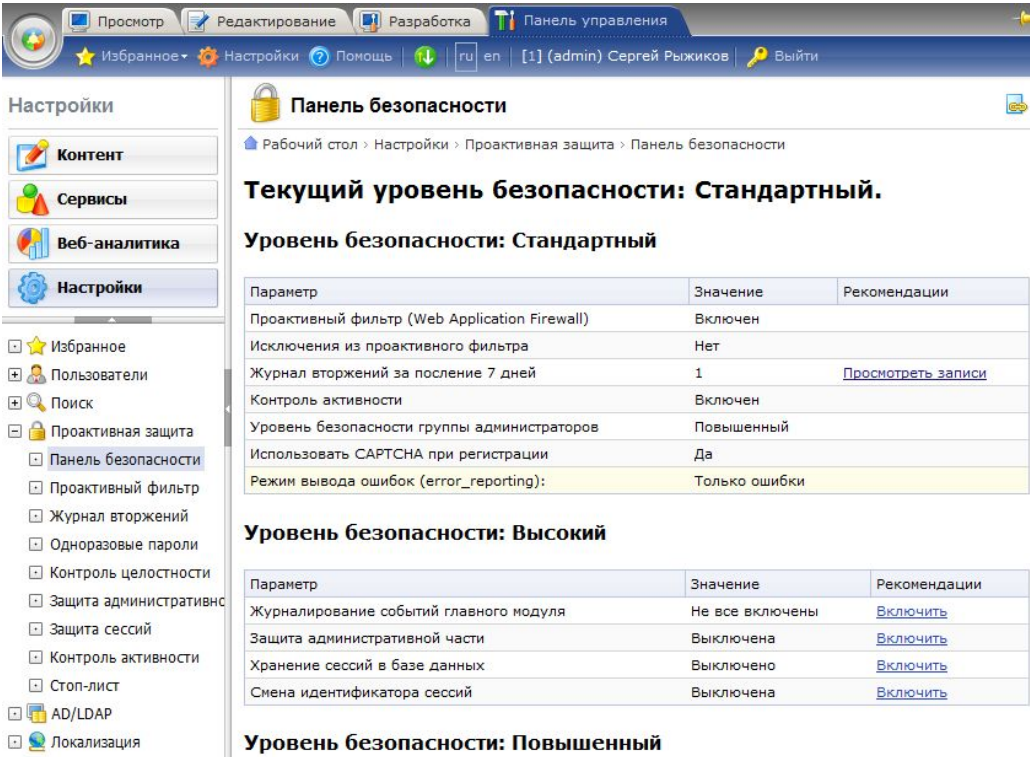
- **Панель безопасности**
- **Проактивный фильтр (Web Application FireWall)**
- **Технология одноразовых паролей (OTP)**
- **Защита авторизованных сессий**
- **Контроль активности**
- **Шифрование канала передачи через SSL**
- **Журнал вторжений**
- **Защиту административных разделов по IP**
- **Стоп-листы**
- **Контроль целостности**
- **Рекомендации по настройке безопасности**
- **Защиту редиректов от фишинга**
- **Монитор обновлений**
- **Внешний контроль информационной среды**



*Проактивная  
защита*



## Панель безопасности



The screenshot shows the 'Панель безопасности' (Security Panel) in the 1C-Bitrix administration interface. The interface is in Russian and includes a navigation menu on the left with options like 'Настройки' (Settings), 'Контент' (Content), 'Сервисы' (Services), and 'Веб-аналитика' (Web Analytics). The main content area displays the current security status and a list of security parameters.

**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**

### Оценка уровней безопасности веб-проекта



## Проактивный фильтр Web Application FireWall

Проактивный фильтр 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 сессии

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.





## Контроль активности

The screenshot shows the 1C-Bitrix administration interface. The top navigation bar includes 'Просмотр', 'Редактирование', 'Разработка', and 'Панель управления'. The left sidebar contains a 'Настройки' menu with options like 'Контент', 'Сервисы', 'Магазин', 'Веб-аналитика', and 'Настройки'. The main content area is titled 'Контроль активности' and shows the 'Параметры' tab. The settings include: 'Шаблон страницы, которая будет показана заблокированному пользователю' (with a link to 'редактировать шаблон'), 'Блокировать на время: 300 (сек.)', 'если в течение 10 (сек.)', 'сделано более 15 хитов', and 'Сделать запись в журнале событий: '. At the bottom are buttons for 'Сохранить', 'Применить', and 'Отменить'.

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 позволят использовать несколько режимов работы с сайтом для пользователей при установленном SSL сертификате.



## Журнал вторжений

Меню

Панель управления

Избранное Настройки Помощь [8] (rsv) Sergey Rizhikov Выйти

### Журнал событий

Рабочий стол > Настройки > Проактивная защита > Журнал вторжений

Дополнительно

Найти: Событие

Событие:

- (все)
- [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.

Найти Отменить

Настроить Excel

На странице: 20

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 через XSS	\$_SERVER["REQUEST_URI"]	88.68.125.81	/tv/javascript:void(0); <a href="#">[стоп-лист]</a>

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



## Защита административных разделов по IP

The screenshot shows the 'Настройки' (Settings) section of the 1C-Bitrix administration interface. The left sidebar contains a menu with 'Настройки' selected, and a sub-menu for 'Проактивная защита' (Proactive protection) with 'Защита административного раздела' (Administrative section protection) selected. The main content area is titled 'Защита административной части' (Administrative section protection) and shows the status 'Защита выключена.' (Protection is disabled). A yellow box contains the text: 'Ваш IP-адрес был определен как: 192.168.0.93. Если это так, скопируйте его и вставьте в поле ввода ниже.' (Your IP address was determined as: 192.168.0.93. If this is the case, copy it and paste it into the input field below). Below this, there is a text input field containing '192.168.0.95' and a 'Добавить' (Add) button. At the bottom of the settings area are buttons for 'Сохранить' (Save), 'Применить' (Apply), and 'Отменить' (Cancel).

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



## Стоп-листы

<input type="checkbox"/>		ID	Статус активности	Начало	Акт.	Сайт	IP адрес сети	Маска сети	Стат.
<input type="checkbox"/>		72		25.01.2006 19:57:33	Да	(все)	200.79.200.200	200.200.200.200	Нет
<input type="checkbox"/>		74		26.01.2006 16:58:56	Да	(все)	200.79.200.200	200.200.200.0	Нет
<input type="checkbox"/>		70		16.12.2005 16:52:12	Да	(все)	200.200.200.79	200.200.200.200	Нет
<input type="checkbox"/>		2		13.02.2004 18:58:15	Да	(все)	200.200.200.200	200.200.200.200	Нет

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



## Контроль целостности системы

Контроль целостности системы управления и страниц сайта:

- 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.



## Защита от фишинга

### Защита редиректов с сайта от фишинга

**Фи́шинг** (англ. Фи́шинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — вид интернетФи́шинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — вид интернет-мошенничества) Фи́шинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинамФи́шинг (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 путём проведения массовых рассылокФи́шинг (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 путём проведения массовых рассылок электронных писемФи́шинг (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 путём проведения массовых рассылок электронных писем от имени популярных брендовФи́шинг (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 путём проведения массовых рассылок электронных писем от имени популярных брендов, например, от имени социальных сетейФи́шинг (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 путём проведения массовых рассылок электронных писем от имени популярных брендов, например, от имени социальных сетей Фи́шинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к



## 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

- 1) Подтверждение регистрации по email
- 2) Поддержка авторизации OpenID и LiveID
- 3) Детальная настройка CAPTCHA
- 4) 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:

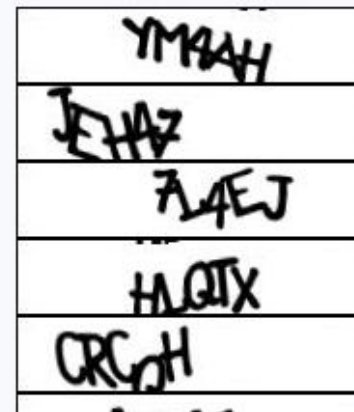
Количество линий:

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



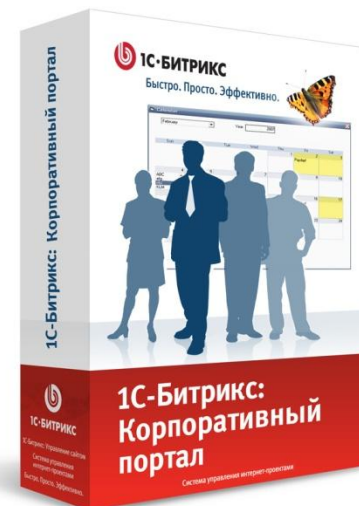
# 1С-БИТРИКС: Управление сайтом



СИСТЕМА УПРАВЛЕНИЯ ИНТЕРНЕТ-ПРОЕКТАМИ

**Модуль «Проактивная защита» включен в состав программных продуктов:**

- «1С-Битрикс: Управление сайтом» (все редакции, кроме «Старт»)
- «1С-Битрикс: Корпоративный портал»





# 1С-БИТРИКС: Управление сайтом



СИСТЕМА УПРАВЛЕНИЯ ИНТЕРНЕТ-ПРОЕКТАМИ

**Спасибо за внимание! Вопросы?**

**Сергей Рыжиков**  
**[rsv@1c-bitrix.ru](mailto:rsv@1c-bitrix.ru)**

**[www.1c-bitrix.ru](http://www.1c-bitrix.ru)**