



## Как защитить веб-ресурс

с пользовательскими данными и финансами  
от взлома, кражи денег и информации  
без раздутого бюджета

Кейс крупнейших высоконагруженных  
интернет-проектов рунета



**Котова Юлия**  
CEO сканера уязвимостей  
PHP Scan

# Какую бизнес задачу мы решали?

GO·GET·LINKS    Оптимизаторам    Вебмастерам    База знаний

## GoGetLinks - научите свой сайт приносить доход!

✓ Лидирующая на рынке биржа ссылок: вечные ссылки и их усиление, многоуровневые, крауд-ссылки.

[Начни работать](#) и получи [приветственный бонус](#)

### Оптимизаторам

Рост поискового трафика за счет ссылочного продвижения

№ 1  
№ 2  
№ 3

### Вебмастерам

Пассивный доход сайта за счет ручного размещения ссылок

**KWORK**  
ФРИЛАНС МАРКЕТПЛЕЙС

Найти услуги [Найти](#)

Пользователей онлайн: 2  
Последний заказ: 21 сек. н

Дизайн    Разработка и IT    Тексты и переводы    SEO и трафик

## Покупайте фриланс-услуги В ОДИН КЛИК

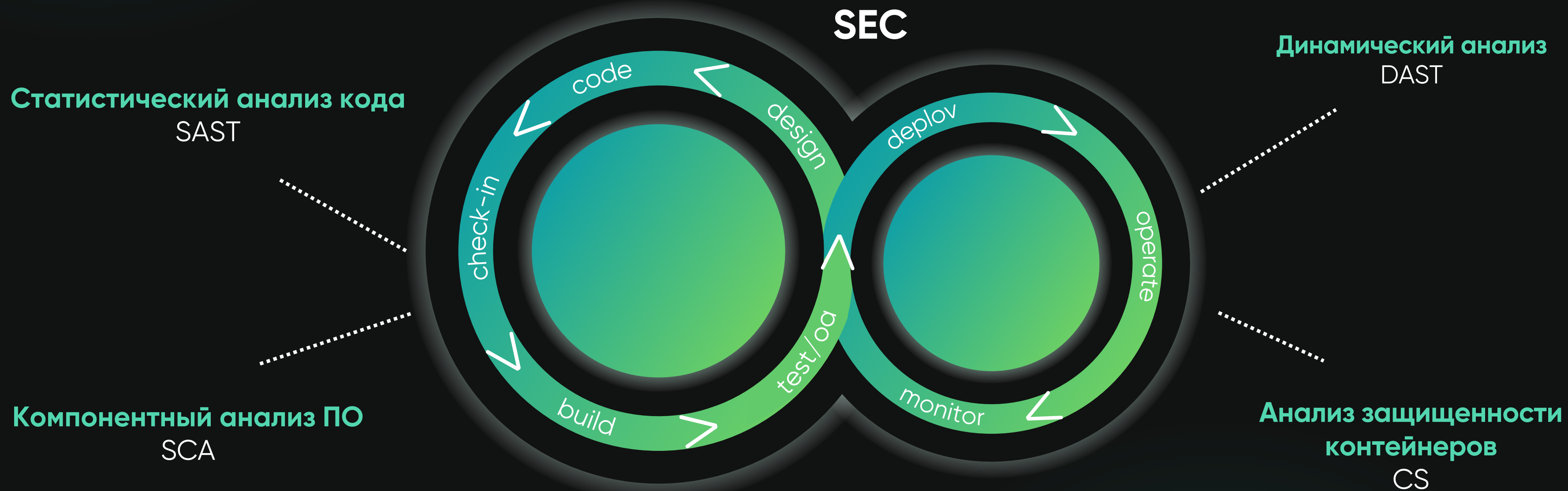
Создать сайт на wix [Найти](#)

Популярное: [Веб дизайн](#)   [Логотипы](#)   [Дизайн соцсетей](#)   [Wordpress](#)

**0,4 млн** пользователей  
в месяц

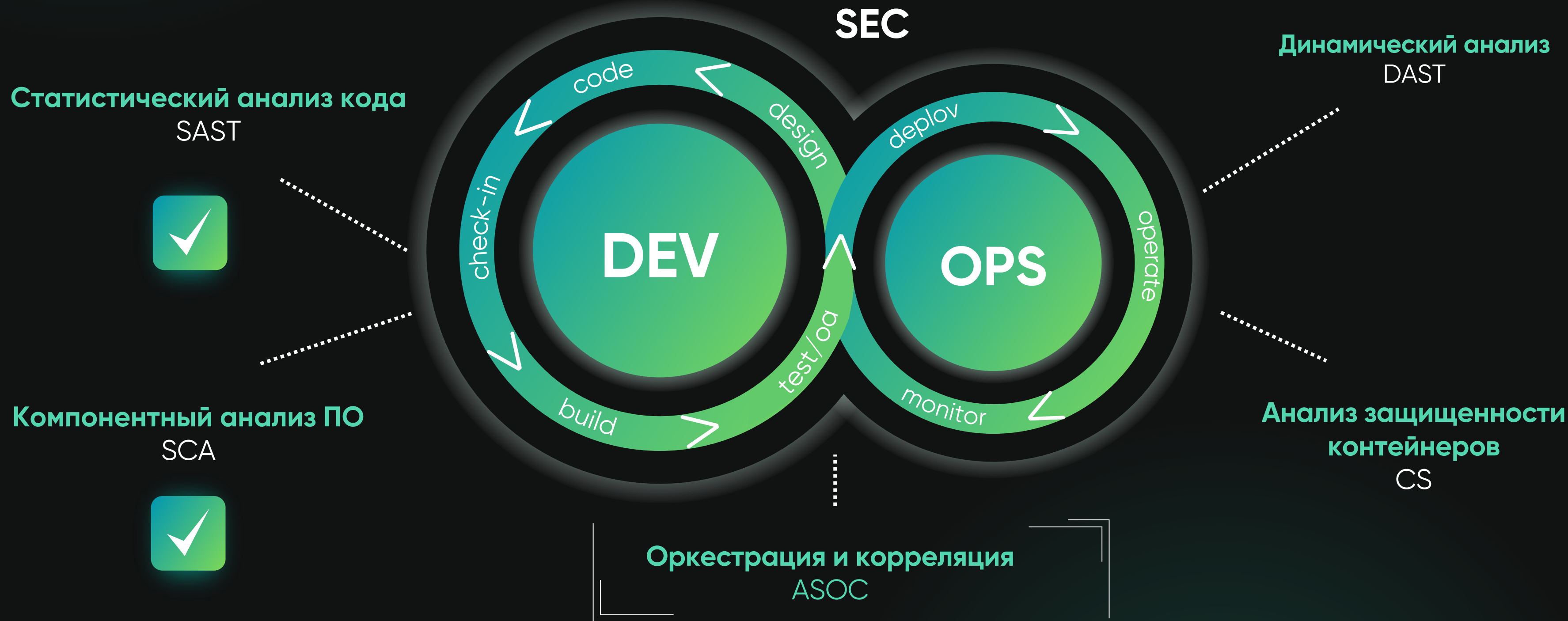
**4,1 млн** пользователей  
в месяц

# Составляющие безопасности для веб-ресурса





# Внедренные решения для безопасности веб-ресурсов



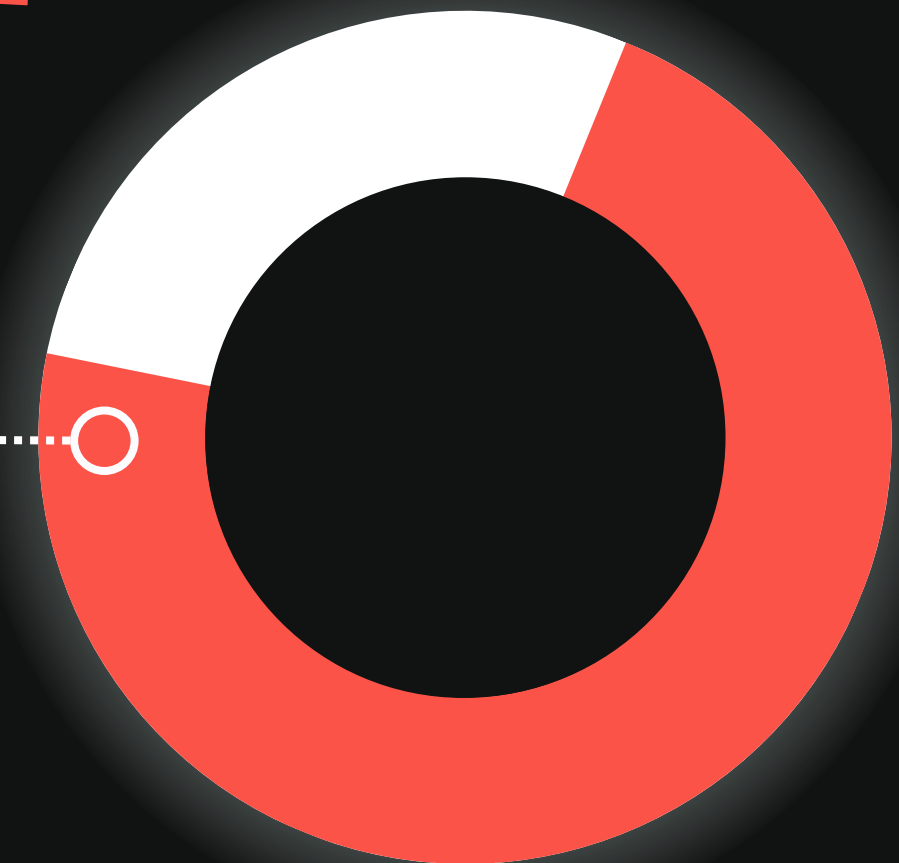
Ежедневно  
**взламывают**  
30 000 сайтов



**98%** веб-приложений  
**уязвимы**

*\*по данным исследований  
Positive Technologies в 2020-2021*

**72%** всех найденных  
уязвимостей **связаны**  
**с ошибками в коде**



# Как избежать серьезных угроз?

- Нужно использовать **SAST решение**  
(анализатор статического кода)

## **ЦЕЛЬ:**

**выявлять недостатки безопасности кода  
на ранних этапах** в процессе разработки

# Какой сканер для проверки кода **лучший** в мире?

*Мы проанализировали рынок сканеров уязвимостей.*

Критерии выбора лучших решений для проверки PHP кода:

**Цена**

**Качество  
проверок  
PHP кода**

(соотношение найденных  
и пропущенных  
уязвимостей)

**Поддержка  
интеграции  
с Git**

# Мировые SAST РЕШЕНИЯ для проверки PHP кода

Часть известных сканеров НЕ рассматривали ввиду:

└ Принадлежности к DAST

└ Дорогостоящих проверок

└ Отсутствия возможности протестировать

SAST сканеры, не вошедшие в тестирование на качество проверки кода:

Название	Оценка компании	Трафик по SimilarWeb	Цена, средняя	Возможность протестировать
Veracode	\$2.5 млрд	177 К	760 000-800 000 руб в мес	Через запрос и созвон
Checkmarx	\$1.15 млрд	142 К	Через запрос	Через запрос и предпродажные скрипты
Mend.IO	\$0.75 млрд	124 К	от 1 600 000 руб в мес	
CAST AIP	\$0.05 млрд	108 К	от 9 000 000 руб в мес	



# Мировые SAST РЕШЕНИЯ

для проверки PHP кода

Название	Оценка компании	Трафик по SimilarWeb
Sonarsource (Sonarqube)	\$4.7 млрд	1 М
Snyk	\$3.3 млрд	1.4 М
Sonatype	\$0.13 млрд	0.5 М
Semgrep	–	0.1 М
CloudDefense.ai	–	0.08 М
Aikido.dev	–	0.01 М
Application security от GitLab	–	–
PHP Scan	new	new

*\*Для сравнения  
взяты популярные в  
мире анализаторы  
статического кода*

# Проверка сканеров на качество сканирования кода

1

**ЭТАП**  
**Подготовка**  
**тестов**



**Мы сформировали**  
**225 ТЕСТОВ**

реальные фрагменты кода под каждый тип уязвимостей с разными вызовами функций, получением данных



**Учли**

разные версии php и разные конструкции, которые там используются

# Проверка сканеров на качество сканирования кода

2

ЭТАП

Проверка кода  
всеми сканерами

3

ЭТАП

Расчет качества  
сканирования

True Positive (TP)	False Positive (FP)
False Negative (FN)	True Negative (TN)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

# Пример результатов тестирования

\* Тестовый код, а также подробные результаты сканирования по каждому сканеру могут быть высланы по запросу.

Сравнение php SAST

Файл Правка Вид Вставка Формат Данные Инструменты Расширения Справка

100% р. % .0 .00 123 По ум... - 10 + B I A

B55  $f(x) = (B54+C54)/(B54+C54+D54+E54)$

	A	B	C	D	E	F	G	H	I	J
1	Группа тестов	True Posivite	True Negative	False Positive	False Negative	Что и где он нашел				
32	escaped_sql	1	9	0	10	src_interval_scope/wp-includes/taxonomy.php - в строках 5071				
33	extend_pdo	1	1	0	2	src_literal_empty_string/index.php - в строках 9, 18				
34	extract	0	1	0	2	src_multi_extends/index.php - в строках 14				
35	extract_unknown_taint	1	1	0	0	src_mysql_escape_string/index.php - в строках 22				
36	fallthrough_context	0	2	0	1	src_mysql_query/index.php - в строках 4				
37	fallthrough_is_numeric	1	1	0	0	src_pdo/run.php - в строках 13				
38	fallthrough_not_intval	1	0	2	0	src_php82/Input.php - в строках 32, 41, 49				
39	headers	1	0	0	0	src_php82/readonly.php - в строках 13				
40	instanse_of	2	0	0	0	src_property/T.php - в строках 14				
41	internal_safe_type	0	1	0	1	src_short_open_tag/index.php - в строках 5				
42	interval_scope	2	0	0	0	src_source_details/index.php - в строках 6, 13, 28, 35, 42, 51				
43	literal_empty_string	0	1	2	1	src_switch_const/index.php - в строках 18, 26				
44	multi_extends	1	0	0	0	src_test1/m_test_db.php - в строках 30, 31, 34				
45	mysql_escape_string	1	2	0	2	src_test2/m_test_db.php - в строках 13				
46	mysql_query	1	0	0	0	src_test2_1/m_test_db.php - в строках 30				
47	pdo	1	1	0	2	src_test3/z-ele-custom-skin.php - в строках 29				
48	pdo_1	0	1	0	3	src_test4/test_db.php - в строках 46				
49	pdo_2	0	1	0	3	src_unary_op/index.php - в строках 45, 46, 47, 48, 49				
50	php82	4	2	0	2	src_interval_scope/wp-includes/functions.php - в строках 4064				
51	preg_reddos	2	0	0	0	src_xss_printf/index.php - в строках 5				
52	property	1	0	0	0	src_unserialize/index.php - в строках 4				
53	session	0	0	0	1	src_preg_reddos/index.php - в строках 5, 9				
54	Summary	34	63	13	55					
55	Accuracy	58,79%								
56										

+ Summary PhpSecure SonarQube Snyk Semgrep aikido CloudDefense/GitLab/SonaType



# Сравнение сканеров по качеству

Название	Точность сканирования
Sonatype	7%
Application security от GitLab	7%
CloudDefense.ai	7%
Aikido.dev	41%
Semgrep	43%
Snyk	53%
Sonarsource (Sonarqube)	59%
PHP Scan - <b>NEW</b>	95%

\*Данные на январь  
2024 года



# Сравнение сканеров

по качеству, цене, поддержки ci/cd

Название	Точность сканирования	Цена, в месяц	Интеграция с Git
Sonatype	7%	16 500 руб	✓
Application security от GitLab	7%	Бесплатно	✓
CloudDefense.ai	7%	По запросу	✓
Aikido.dev	41%	80 000 руб	✓
Semgrep	43%	100 000 руб	✓
Snyk	53%	62 500 рублей	✓
Sonarsource (Sonarqube)	59%	35 000 рублей	✓
PHP Scan - NEW	95%	Бесплатно	✓

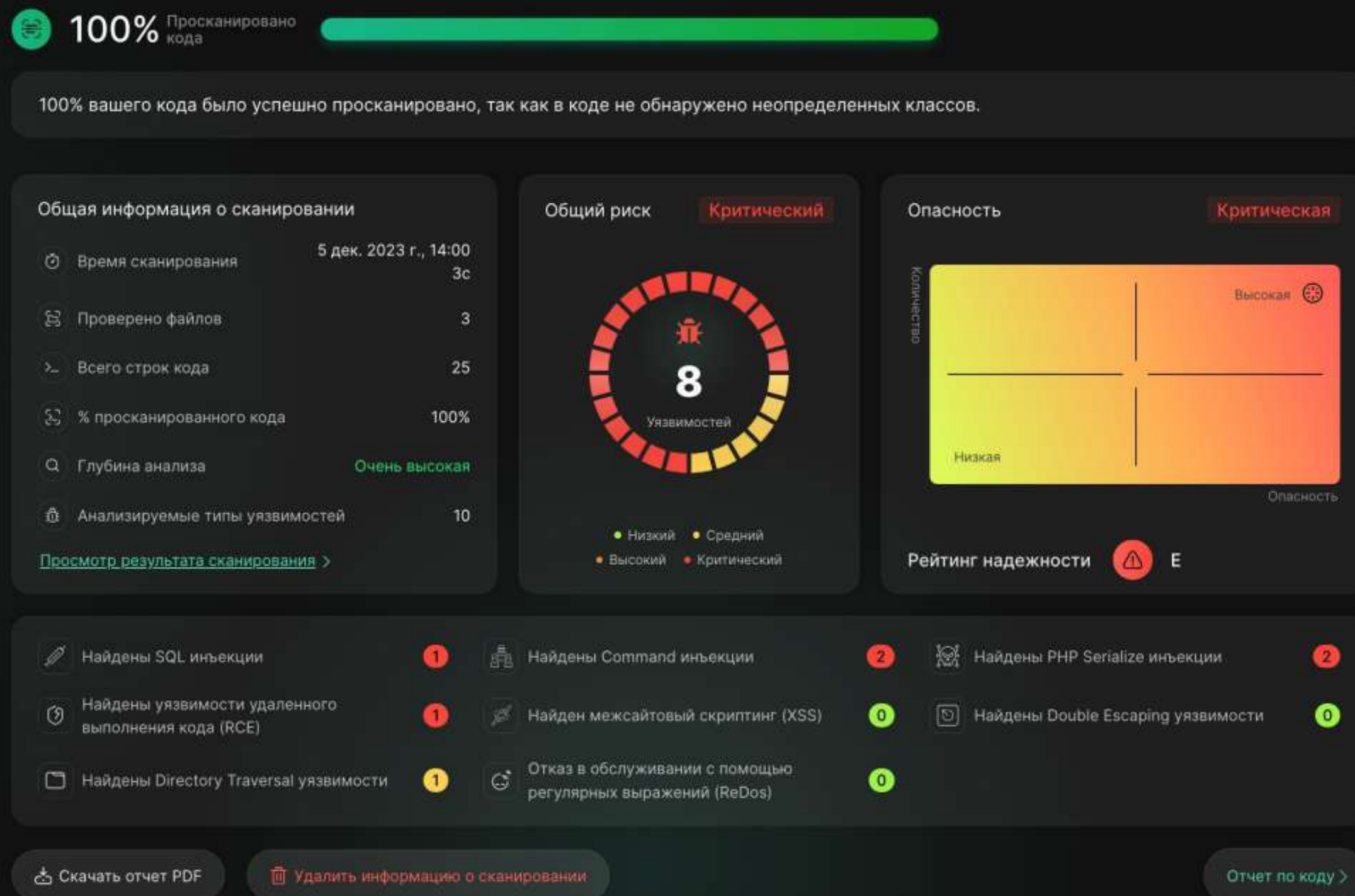
Расчет цены на примере проекта, в котором:

**~ 1 млн строк,  
25 разработчиков**

\*Данные на январь 2024 года

# Лучшее SAST решение

для проверки PHP кода



PHP Scan обнаруживает:

- ✓ SQL инъекции
- ✓ Command инъекции (Shell)
- ✓ Cross-Site Scripting (XSS)
- ✓ PHP Serialize инъекции
- ✓ Удаленное выполнение кода (RCE)
- ✓ Directory Traversal
- ✓ Отказ в обслуживании с помощью регулярных выражений (ReDos)



**PHP Scan**  
online code scanner



**Перейти на сайт**  
[www.phpscan.com](http://www.phpscan.com)

site</title>  
<meta http-equiv="<br>  
<meta name="keywords">  
<meta name="description">  
<meta name="language">  
<link rel="stylesheet">  
<link rel="shortcut icon">  
<div style="background-color: "#ffffff">  
<div style="float: left; width: 50%; padding-right: 10px;>  
<div style="float: right; width: 50%; padding-left: 10px;>



# Лучшее SAST решение

для проверки PHP кода

PHP scan дает:

Детальный отчет о найденных уязвимостях кода

Пояснения, почему это уязвимость

Откуда идет уязвимость

The screenshot displays a SAST tool interface with a sidebar on the left and a main content area on the right. The sidebar, titled "Данные об уязвимостях", shows a summary of 3 vulnerabilities, all marked as "Открыт" (Open). It also lists risk levels (Critical, High, Medium, Low) and vulnerability types (SQLi, Command Injection, PHP Serialize Injection, RCE, XSS, Double Escaping, Directory Traversal, ReDoS).

The main content area shows two vulnerability details:

- Command инъекция:** Located in `builds/test1570636/test-many-vulns/command_-_shell.php`. The code snippet shows `exec($_GET["cmd"]);` on line 3. A detailed explanation in Russian states: "Обнаружена командная инъекция. Измените этот код, чтобы он больше не передавал небезопасные данные, предоставленные пользователем." (Command injection detected. Change this code so it no longer passes unsafe data provided by the user.)
- XSS:** Located in `builds/test1570636/test-many-vulns/XSS.php`. The code snippet shows `printf("Hello, %s", $login);` on line 5.

Each vulnerability entry includes a "Где уязвимость?" (Where is the vulnerability?) tab, a "Как эксплуатировать уязвимость?" (How to exploit the vulnerability?) tab, a "Почему это уязвимость?" (Why is this a vulnerability?) tab, and a "Как исправить?" (How to fix it?) tab. Action buttons like "Игнорировать" (Ignore), "Отметить как на исправлении" (Mark as fixed), and "Путь уязвимости" (Vulnerability path) are also visible.

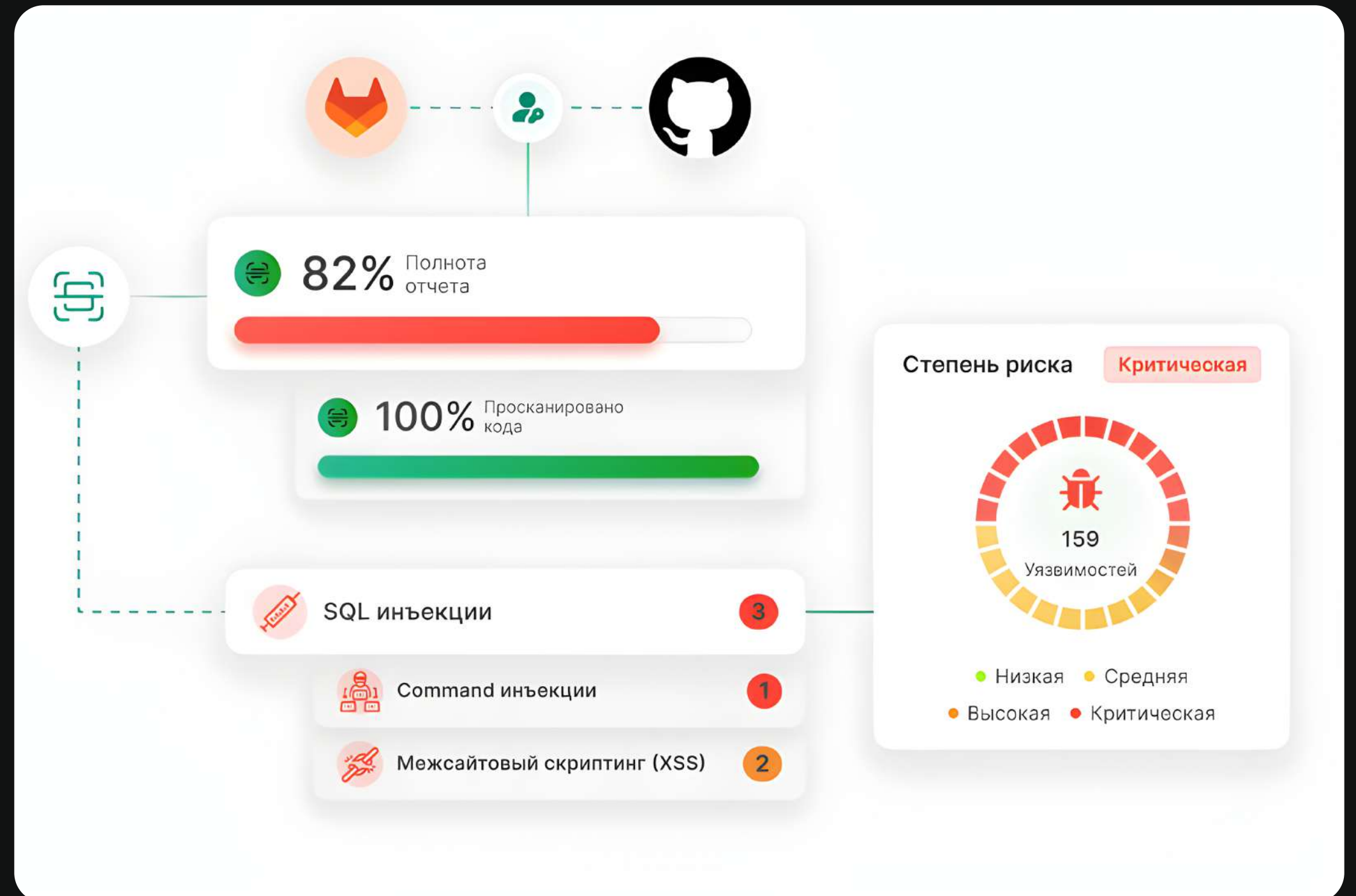




# Автоматическое сканирование кода

✓ Полная поддержка по внедрению сканирования кода в CI/CD Pipeline от наших специалистов

интегрируйте сканер в ваш Git репозиторий



# Снижение рисков взлома

В сеть выложили 99 млн строк базы данных клиентов "Спортмастера"

"Яндекс" подтвердил утечку исходного кода своих сервисов

Утечка данных 97 млн пользователей сервиса электронных книг "ЛитРес"



"Ашан" подтвердил утечку данных покупателей, около 8 млн записей

"Магнит" подтвердил утечку персональных данных сотрудников магазинов "Дикси"

"Почта России" и Минцифры расследуют утечку данных

\*Данные Tadvise, Лаборатории Касперского, сервиса DLBI

# Резюме: Снижение рисков потери денег и убытков от взлома



₽ 1 000 000 000

Максимальные убытки  
от утечки



₽ 27 700 000

Средние убытки  
от утечки



₽ 10 500 000

Средние ожидаемые  
убытки от утечки

# Резюме: Снижение рисков штрафов



## Защита от взлома,

утечки конфиденциальных данных и финансов, парализации бизнес-процессов или полного уничтожения проекта.



## Сокращение рисков получить штраф до 500 млн.руб.

от регулирующих органов

<title>web site</title>  
<meta http-equiv=<br><meta name="keywo<br><meta name="descri<br><meta name="langua<br><meta name="style&



# Бесплатное сканирование PHP Scan



Введите название ваш...

Начни сканирование бесплатно!



**Бесплатное и безлимитное  
сканирование кода,**

когда иные продукты по безопасности  
стоят ~ 100 000 руб в месяц.

php



Laravel



Drupal™



Joomla!

Bitrix  
24<sup>Ⓜ</sup>



# Высокое качество кода и удобство разработки



**Консультация по исправлению  
найденных уязвимостей**

от специалистов по безопасности PHP Scan



**Учет пожеланий по доработке сканера**

исходя из ваших бизнес задач и процессов  
разработки

# Как будет храниться и использоваться загруженный вами код?

PHP Scan гарантирует **полную конфиденциальность** вашего кода и отчетов об уязвимостях.

## **Сканер полностью зашифрован**

PHP Scan не использует и не передает загружаемый код кому бы то ни было.

## **Максимальная безопасность данных**

- Сразу после загрузки и сканирования кода он безвозвратно удаляется с сервера.
- Чтобы повторить сканирование, нужно повторно загрузить свой код или указать путь к GIT-хранилищу.

# Планы на будущее по PHP Secure

Мы работаем над постоянным усовершенствованием сканера, чтобы предоставлять **комплексное решение по безопасности**

**30+**

языков  
программирования

**Проверка на полный  
спектр угроз,**

в том числе ошибки  
конфигурации, уязвимости  
во вспомогательном ПО

**Эволюция сканера из SAST  
в IAST решение, которое  
будет анализировать:**

- потоки данных
- конфигурацию
- HTTP-запросы и ответы
- библиотеки, фреймворки и другие компоненты
- информацию о внутреннем подключении

# Партнерство с вендорами и интеграторами



Юлия Котова

site</title>  
ta http-equiv="keywo  
eta name="keywo  
meta name="descrip  
meta name="langua  
<link rel="stylesha  
<link rel="shortc  
>  
color="#ffffff">  
nContent

# Спасибо за внимание!



**PHP Scan**  
online code scanner

[www.PHPScan.com](http://www.PHPScan.com)

## Есть вопросы? Пишите!



CEO PHP Scan  
Юлия Котова

