

PT Application Inspector

Максимальная точность
Минимум ложных срабатываний
Встраивание в процессы разработки

ПОДДЕРЖИВАЕМЫЕ ЯЗЫКИ ДЛЯ АНАЛИЗА

PHP, Java, C#, JavaScript, Kotlin,
VB.NET, Python, Objective-C,
Swift, C/C++, Go, SQL (PL/SQL,
T-SQL, MySQL)

Текущая версия продукта: 3.6.3

УЗНАТЬ ПОДРОБНЕЕ

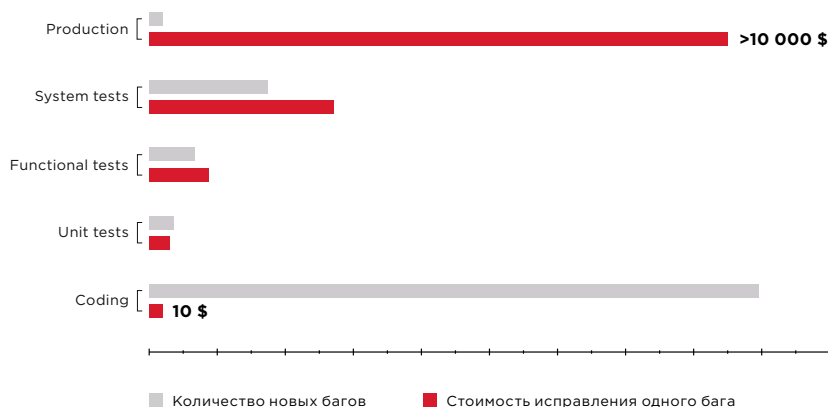
Больше информации
о PT Application Inspector
на продуктовой странице
решения: [ptsecurity.com/
ru-ru/products/ai](https://ptsecurity.com/ru-ru/products/ai)



Веб-приложения по-прежнему остаются популярной целью для злоумышленников. Как показали наши исследования¹, каждая пятая атака направлена на веб-ресурсы организаций, чаще всего — государственных и медицинских учреждений, онлайн-сервисов, организаций сферы науки и образования и IT-компаний.

В большинстве случаев атакующие эксплуатируют имеющиеся уязвимости. В среднем, согласно исследованиям, в одном приложении их больше двух десятков, пятая часть из которых — критические. Их эксплуатация может привести к серьезным финансовым и репутационным рискам для компании: краже важных данных, проникновению в инфраструктуру организации, временным простоям или полной остановке системы.

Большинство уязвимостей содержатся в исходном коде, их можно устранить на самых ранних этапах создания приложения. Такой подход, во-первых, позволяет обработать максимальное количество уязвимостей, во-вторых, предотвращает реализацию рисков, в-третьих, гораздо выгоднее, чем устранение уязвимостей на стадии production.



Стоимость устранения дефекта на разных стадиях жизненного цикла приложения
(Applied Software Measurement, Capers Jones)

¹ «Актуальные киберугрозы: итоги 2019 года», Positive Technologies: ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/

PT Application Inspector выявляет уязвимости не только в работающем приложении, но и в исходном коде. Это позволяет устранить их на ранней стадии, тем самым свести к нулю возможность их эксплуатации.

ДОПОЛНИТЕЛЬНО**РАБОТАЕТ ON-PREMISE**

PT Application Inspector не передает код и другие данные за пределы периметра компании и может работать без доступа в интернет.

ГИБКОЕ МАСШТАБИРОВАНИЕ

Если необходимо нарастить мощность и увеличить скорость анализа, PT Application Inspector можно горизонтально масштабировать. Архитектура решения позволяет сделать это максимально безболезненно и с минимумом трудозатрат.

БЫСТРОЕ ЗАКРЫТИЕ УЯЗВИМОСТЕЙ

По результатам анализа PT Application Inspector может формировать специальные виртуальные патчи для использования в PT Application Firewall². Они могут предотвратить эксплуатацию уязвимостей в приложениях.

СЕРТИФИЦИРОВАННОЕ РЕШЕНИЕ

PT Application Inspector состоит в российском реестре ПО (регистрационный номер 1253), имеет действующий сертификат ФСТЭК № 4000, помогает выполнять РС БР ИББС-2.6-2014, приказы ФСТЭК и требования PA DSS и PCI DSS.

2 Консалтинг и сервисы Positive Technologies ptsecurity.com/upload/corporate/ru-ru/services/security-services/pt-consulting-services-sb-rus.pdf

3 PT Application Firewall — межсетевой экран уровня веб-приложений: ptsecurity.com/ru-ru/products/af/

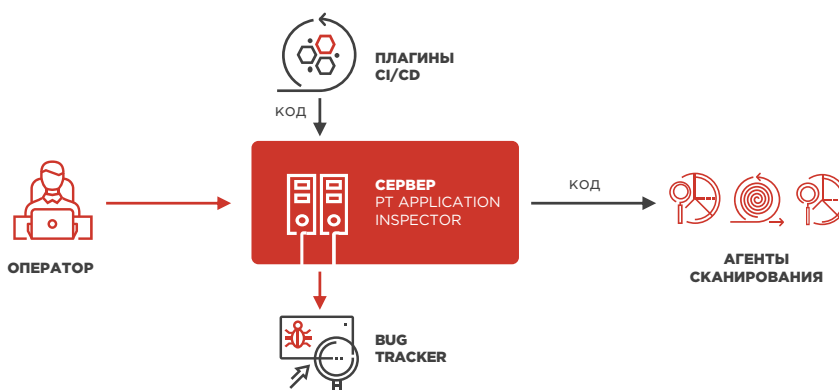


Схема встраивания PT Application Inspector в существующий процесс разработки

Преимущества

Максимальный охват и приоритизация уязвимостей. PT Application Inspector объединяет несколько типов анализа: статистический, динамический, интерактивный (SAST, DAST, IAST), а также анализ сторонних компонентов (SCA). Комбинация позволяет охватить максимальное количество уязвимостей, а гибкая система фильтрации дает возможность приоритизировать их в зависимости от степени критичности. Разработчик концентрируется на важных проблемах, а эксперты гораздо меньше занимаются ручной проверкой.

Подтверждение наличия уязвимости. PT Application Inspector не только находит уязвимости, но и вычисляет условия их эксплуатации, а также может генерировать безопасные эксплойты для их проверки.

Экспертиза: мировые стандарты, исследования и практика. База знаний PT Application Inspector регулярно пополняется уникальными методами обнаружения уязвимостей от экспертов отдела исследований и разработки (R&D). В ней содержатся данные о более чем 150 тыс. уязвимостей из международной базы NVD, а также информация об уникальных уязвимостях, обнаруженных специалистами отдела анализа защищенности приложений².

Интеграция в действующие процессы разработки. PT Application Inspector гибко встраивается в существующие процессы за счет ролевой модели разграничения доступа, а также готовых плагинов для подключения к системам сборки и доставки приложений, баг-трекерам и IDE-системам. Это позволяет использовать PT Application Inspector для безопасной разработки кода (DevSecOps).

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDAYS

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](https://facebook.com/PositiveTechnologies), [ВКонтакте](https://vk.com/ptsecurity), [Twitter](https://twitter.com/ptsecurity)), а также в разделе «Новости» на сайте ptsecurity.com.