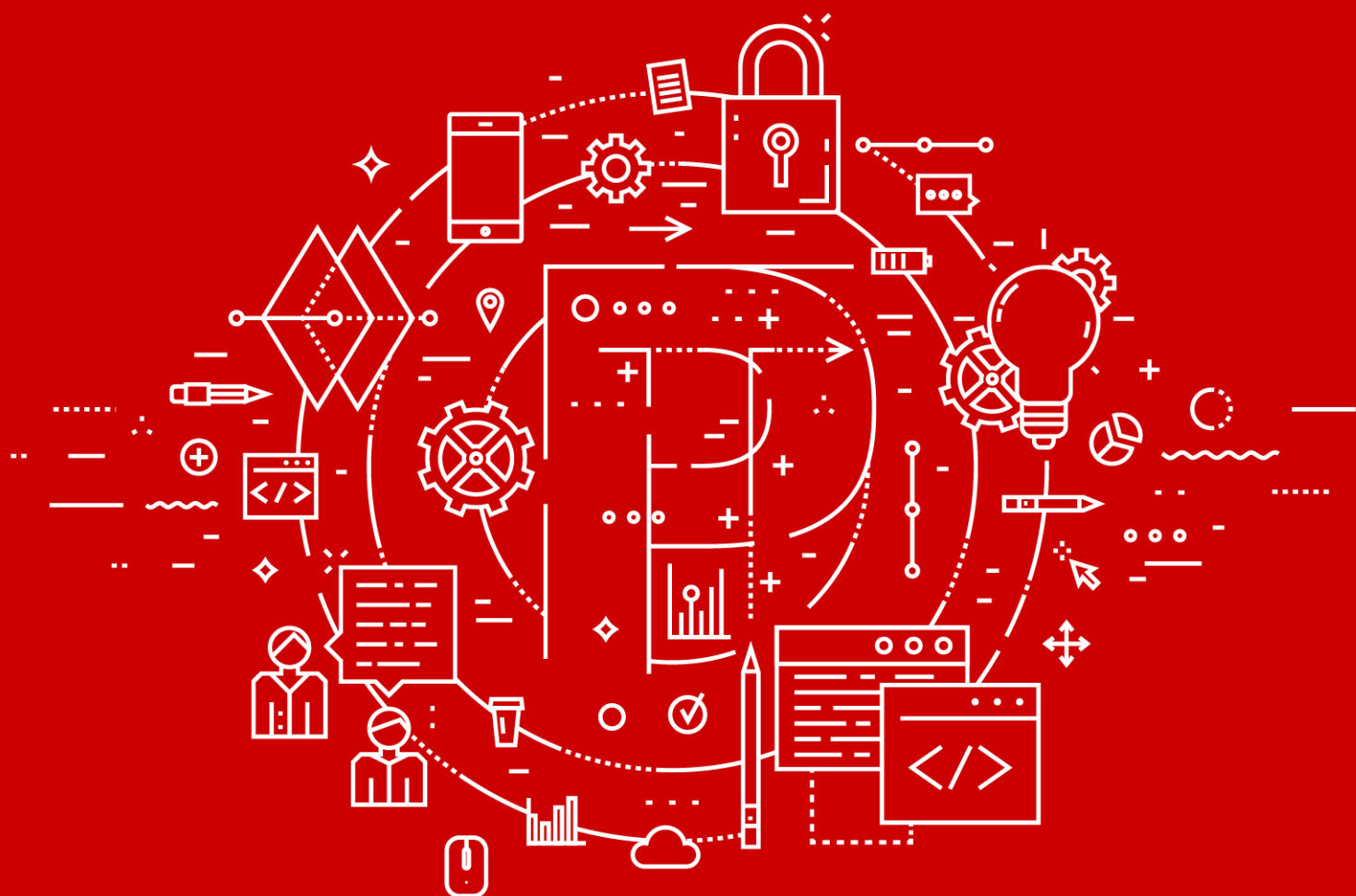


# Positive Technologies

## BlackBox

Версия 2.1



Руководство пользователя

POSITIVE TECHNOLOGIES

© Positive Technologies, 2017.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 31.08.2022

# Содержание

1.	Об этом документе .....	4
1.1.	Условные обозначения .....	4
1.2.	Другие источники информации о PT BlackBox .....	4
2.	О сканере Positive Technologies BlackBox .....	6
3.	Аппаратные и программные требования .....	7
4.	Состав компонентов ПО и его среды функционирования .....	8
5.	Установка сканера PT BlackBox .....	10
5.1.	Установка Docker .....	10
5.2.	Установка Docker Compose .....	11
5.3.	Добавление учетной записи пользователя в группу docker .....	11
5.4.	Установка PT BlackBox .....	12
6.	Работа с PT BlackBox .....	13
6.1.	Регистрация и вход в систему .....	13
6.2.	Интерфейс PT BlackBox .....	14
6.2.1.	Страница «Сайты» .....	14
6.2.2.	Страница с параметрами сканируемой цели .....	15
6.2.3.	Страница «Профиль» .....	15
6.2.4.	Страница с результатами сканирования .....	16
6.3.	Запуск сканирования .....	18
6.4.	Изменение параметров аутентификации .....	20
6.5.	Просмотр результатов и истории сканирования .....	20
6.6.	Работа с уведомлениями .....	21
7.	Интеграция в CI/CD .....	23
8.	Удаление PT BlackBox .....	24
9.	Обращение в службу технической поддержки .....	25
9.1.	Техническая поддержка на портале .....	25
9.2.	Время работы службы технической поддержки .....	25
9.3.	Как служба технической поддержки работает с запросами .....	26
9.3.1.	Предоставление информации для технической поддержки .....	26
9.3.2.	Типы запросов .....	26
9.3.3.	Время реакции и приоритизация запросов .....	27
9.3.4.	Выполнение работ по запросу .....	29

# 1. Об этом документе

Руководство пользователя содержит пошаговые инструкции и справочную информацию об использовании Positive Technologies BlackBox (далее также – PT BlackBox). В руководстве описаны ключевые и дополнительные функции PT BlackBox, а также даны инструкции по установке.

Руководство адресовано специалистам, использующим PT BlackBox в своей работе.

## В этом разделе

[Условные обозначения \(см. раздел 1.1\)](#)

[Другие источники информации о PT BlackBox \(см. раздел 1.2\)](#)

## 1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
<b>Внимание!</b> При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
<b>Примечание.</b> Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
▶ Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку <b>OK</b>	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду Stop-Service	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

## 1.2. Другие источники информации о PT BlackBox

Вы можете найти дополнительную информацию о PT BlackBox на [портале технической поддержки](#).

[Портал](#) содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь [в службу технической поддержки \(см. раздел 9\)](#).

## 2. О сканере Positive Technologies BlackBox

Positive Technologies BlackBox – сканер приложений, который ищет уязвимости и риски, связанные с безопасностью, и помогает защитить приложения от действий злоумышленников. PT BlackBox сканирует приложения, используя метод черного ящика. В основе этого метода – имитация поведения злоумышленника, у которого нет знания о внутреннем устройстве приложения. Сканер отправляет приложению различные запросы, анализирует динамические скрипты, формы, параметры, заголовки и прочие входные точки, через которые можно попасть внутрь системы и оказать на нее негативное воздействие. После окончания сканирования PT BlackBox выдает список обнаруженных проблем и рекомендации по их исправлению.

Ключевыми возможностями Positive Technologies BlackBox являются:

- Хранение истории сканирования.
- Возможность поделиться результатами сканирования на определенное время. Пользователь может отправить ссылку на результаты сканирования как в процессе сканирования, так и после его завершения.
- Одновременное сканирование до пяти целей.
- Возможность встроить PT BlackBox в процесс непрерывной интеграции и развертывания (CI/CD) с авторизацией по токену. Используя специальные скрипты, пользователь сканера может встроить проверку своего приложения в процесс его сборки.
- Сканирование целей, для доступа к которым необходима авторизация.

### 3. Аппаратные и программные требования

В данном разделе представлены требования к аппаратному и программному обеспечению для установки и использования PT BlackBox.

На сервере или локальном компьютере должны быть установлены:

- операционная система Ubuntu или Debian;
- Docker;
- Docker Compose версии 1.28 и выше.

Таблица 2. Аппаратные требования

Параметр	Минимальное значение	Рекомендуемое значение
Процессор	8 виртуальных или физических ядер	4 ядра на одно сканирование и 1 ядро для системы (для 5 параллельных сканирований необходимо 21 ядро)
ОЗУ	16 ГБ	4 ГБ на одно сканирование и 2 ГБ для системы (для 5 параллельных сканирований необходимо 22 ГБ)
Дисковое пространство	100 ГБ	От 100 ГБ (для хранения истории сканирований)

## 4. Состав компонентов ПО и его среды функционирования

В состав ПО входят следующие компоненты (все компоненты со свободной лицензией):

- реляционная система управления базами данных MariaDB для управления состоянием процессов сканирования;
- реляционная система управления базами данных PostgreSQL для хранения пользовательских данных и результатов сканирования;
- система управления базами данных Redis для хранения данных активных сессий;
- брокер сообщений RabbitMQ;
- сервер сообщений Centrifugo;
- интерпретатор языка программирования Python 2.7 для выполнения кода компонентов ядра;
- интерпретатор языка программирования Python 3.10 для выполнения кода компонентов приложения.

Среда функционирования ПО включает:

- операционную систему Debian версии 10 или 11 или Ubuntu версии 18.04, 20.04, 21.10 или 22.04;
- программное обеспечение для контейнеризации приложений Docker Engine версии 20.10 или выше;
- инструмент для запуска мультиконтейнерных приложений Docker Compose версии 1.28 или выше.

В таблице ниже дана информация о лицензиях компонентов ПО.

Таблица 3. Лицензии компонентов ПО

Название компонента	Лицензия	Правообладатель	Ссылка на текст лицензии
MariaDB	GPL-2.0	MariaDB Foundation	<a href="https://github.com/MariaDB/">github.com/MariaDB/</a>
PostgreSQL	PostgreSQL	1996–2022, PostgreSQL Global Development Group 1994, The Regents of the University of California	<a href="https://postgresql.org">postgresql.org</a>
Redis	BSD 3-Clause	2006–2020, Salvatore Sanfilippo	<a href="https://github.com/redis/redis/">github.com/redis/redis/</a>
RabbitMQ	MPL-2.0	VMware, Inc. or its affiliates	<a href="https://rabbitmq.com/mpl.html">rabbitmq.com/mpl.html</a>
Centrifugo	Apache-2.0	Centrifugal	<a href="https://github.com/centrifugal/">github.com/centrifugal/</a>
Python 2.7	Python-2.0	Python Software Foundation	<a href="https://python.org">python.org</a>



Название компонента	Лицензия	Правообладатель	Ссылка на текст лицензии
Python 3.10	Python-2.0	Python Software Foundation	<a href="https://docs.python.org/3.10/">docs.python.org/3.10/</a>

## 5. Установка сканера PT BlackBox

Устанавливать сканер можно как на сервере, так и на локальном компьютере, соответствующем аппаратным и программным требованиям. Учетную запись пользователя, который будет устанавливать PT BlackBox, необходимо добавить к группе sudo.

**Примечание.** Далее все команды должны выполняться пользователем, который устанавливает PT BlackBox.

Для установки PT BlackBox необходимо выполнить следующие шаги:

1. Установить Docker.
2. Установить Docker Compose.
3. Добавить учетную запись пользователя, который устанавливает PT BlackBox, в группу docker.
4. Установить PT BlackBox.

### В этом разделе

[Установка Docker \(см. раздел 5.1\)](#)

[Установка Docker Compose \(см. раздел 5.2\)](#)

[Добавление учетной записи пользователя в группу docker \(см. раздел 5.3\)](#)

[Установка PT BlackBox \(см. раздел 5.4\)](#)

### 5.1. Установка Docker

В разделе приводятся инструкции для установки Docker на системы Debian и Ubuntu. После установки Docker необходимо установить Docker Compose. Команды необходимо выполнять в интерфейсе терминала Debian или Ubuntu.

► Чтобы установить Docker на операционную систему Debian:

1. Обновите индекс пакетов и установите пакеты, последовательно выполнив команды:

```
sudo apt-get update
sudo apt-get install ca-certificates curl gnupg lsb-release
```

2. Добавьте GPG-ключ для Docker, последовательно выполнив команды:

```
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg --dearmor -o /etc/apt/
keyrings/docker.gpg
```

## 3. Выполните команду:

```
echo \  
"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] https://  
download.docker.com/linux/debian \$(lsb_release -cs) stable" | sudo tee /etc/apt/  
sources.list.d/docker.list > /dev/null
```

## 4. Обновите индекс пакетов и установите Docker, последовательно выполнив следующие команды:

```
sudo apt-get update  
sudo apt-get install docker-ce docker-ce-cli containerd.io
```

Docker установлен на операционную систему Debian.

## ► Чтобы установить Docker на операционную систему Ubuntu:

## 1. Обновите индекс пакетов и установите пакеты, последовательно выполнив команды:

```
sudo apt-get update  
sudo apt-get install ca-certificates curl gnupg lsb-release
```

## 2. Добавьте GPG-ключ для Docker, последовательно выполнив команды:

```
sudo mkdir -p /etc/apt/keyrings  
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /etc/apt/  
keyrings/docker.gpg
```

## 3. Выполните команду:

```
echo \  
"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] https://  
download.docker.com/linux/ubuntu \$(lsb_release -cs) stable" | sudo tee /etc/apt/  
sources.list.d/docker.list > /dev/null
```

## 4. Обновите индекс пакетов и установите Docker, последовательно выполнив следующие команды:

```
sudo apt-get update  
sudo apt-get install docker-ce docker-ce-cli containerd.io
```

Docker установлен на операционную систему Ubuntu.

## 5.2. Установка Docker Compose

Устанавливать Docker Compose необходимо автономно (вариант standalone).

## ► Чтобы установить Docker Compose,

последовательно выполните команды:

```
sudo curl -SL https://github.com/docker/compose/releases/download/v2.6.1/docker-compose-  
linux-x86_64 -o /usr/local/bin/docker-compose  
sudo chmod +x /usr/local/bin/docker-compose
```

## 5.3. Добавление учетной записи пользователя в группу docker

После установки Docker и Docker Compose необходимо добавить учетную запись пользователя, который будет устанавливать PT BlackBox, в группу docker.

- ▶ Чтобы добавить учетную запись пользователя в группу docker,

выполните команду:

```
sudo usermod -aG docker $USER
```

**Внимание!** После установки Docker, Docker Compose и добавления учетной записи пользователя в группу docker необходимо перезагрузить систему.

## 5.4. Установка PT BlackBox

Для успешной установки PT BlackBox необходимы свободные 80-й и 443-й порты.

- ▶ Чтобы установить PT BlackBox:

1. Предоставьте пользователю права на исполнение установочного файла `ptblackbox.run`, выполнив команду:

```
chmod +x ptblackbox.run
```

2. Запустите установочный файл `ptblackbox.run` из комплекта поставки, выполнив команду:

```
./ptblackbox.run --target ./on_premise
```

Начнется процесс установки.

По окончании установки появится информация об успешном завершении процесса.

После установки необходимо зарегистрироваться в системе и войти в нее, используя логин и пароль.

Вы можете войти в PT BlackBox по адресу <IP-адрес сервера, на котором установлен PT BlackBox>:443. Вы также можете войти в систему, используя вместо IP-адреса доменное имя сервера, на котором установлен PT BlackBox.

## 6. Работа с PT BlackBox

В разделе описана работа с основными функциями Positive Technologies BlackBox.

### В этом разделе

[Регистрация и вход в систему \(см. раздел 6.1\)](#)

[Интерфейс PT BlackBox \(см. раздел 6.2\)](#)

[Запуск сканирования \(см. раздел 6.3\)](#)

[Изменение параметров аутентификации \(см. раздел 6.4\)](#)

[Просмотр результатов и истории сканирования \(см. раздел 6.5\)](#)

[Работа с уведомлениями \(см. раздел 6.6\)](#)

### 6.1. Регистрация и вход в систему

Войти в PT BlackBox может только зарегистрированный пользователь.

► Чтобы зарегистрироваться в PT BlackBox:

1. В адресной строке браузера введите адрес `https://<DNS-имя или IP-адрес сервера с установленным PT BlackBox>`.
2. В правом верхнем углу нажмите кнопку **Регистрация**.  
Откроется страница регистрации.
3. В поле **Эл. почта** введите адрес электронной почты.
4. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.  
**Примечание.** Минимальная длина пароля 8 символов.
5. Нажмите кнопку **Зарегистрироваться**.

Вы зарегистрированы в PT BlackBox.

► Чтобы войти в PT BlackBox:

1. В адресной строке браузера введите адрес `https://<DNS-имя или IP-адрес сервера с установленным PT BlackBox>`.
2. Введите адрес эл. почты и пароль, указанные при регистрации.
3. Нажмите кнопку **Войти**.

Откроется главная страница PT BlackBox.

## 6.2. Интерфейс PT BlackBox

В этом разделе приводится описание страниц и основных элементов интерфейса PT BlackBox, доступных после входа.

### В этом разделе

[Страница «Сайты»](#) (см. раздел 6.2.1)

[Страница с параметрами сканируемой цели](#) (см. раздел 6.2.2)


[Страница «Профиль»](#) (см. раздел 6.2.3)

[Страница с результатами сканирования](#) (см. раздел 6.2.4)



### 6.2.1. Страница «Сайты»

После входа в PT BlackBox и проведения первого сканирования по умолчанию открывается страница **Сайты**.

На странице отображаются адресная строка для указания цели сканирования и карточки целей сканирования. На карточках отображается краткая информация о последнем или продолжающемся в данный момент сканировании: об адресе цели сканирования, времени начала, окончания и продолжительности сканирования, количестве найденных уязвимостей и прогрессе сканирования в процентах.

Завершенное сканирование обозначено значком . По нажатию на этот значок вы можете повторно запустить сканирование цели. На этой же странице вы можете остановить запущенное сканирование.

Из карточки цели сканирования вы можете перейти на страницы с параметрами сканируемого приложения (ссылка **Настройка**) и просмотреть историю сканирований (ссылка **История сканирований**).

Страница **Сайты** содержит следующие кнопки:  — для просмотра уведомлений и  — для перехода на страницу **Профиль** или выхода из системы.

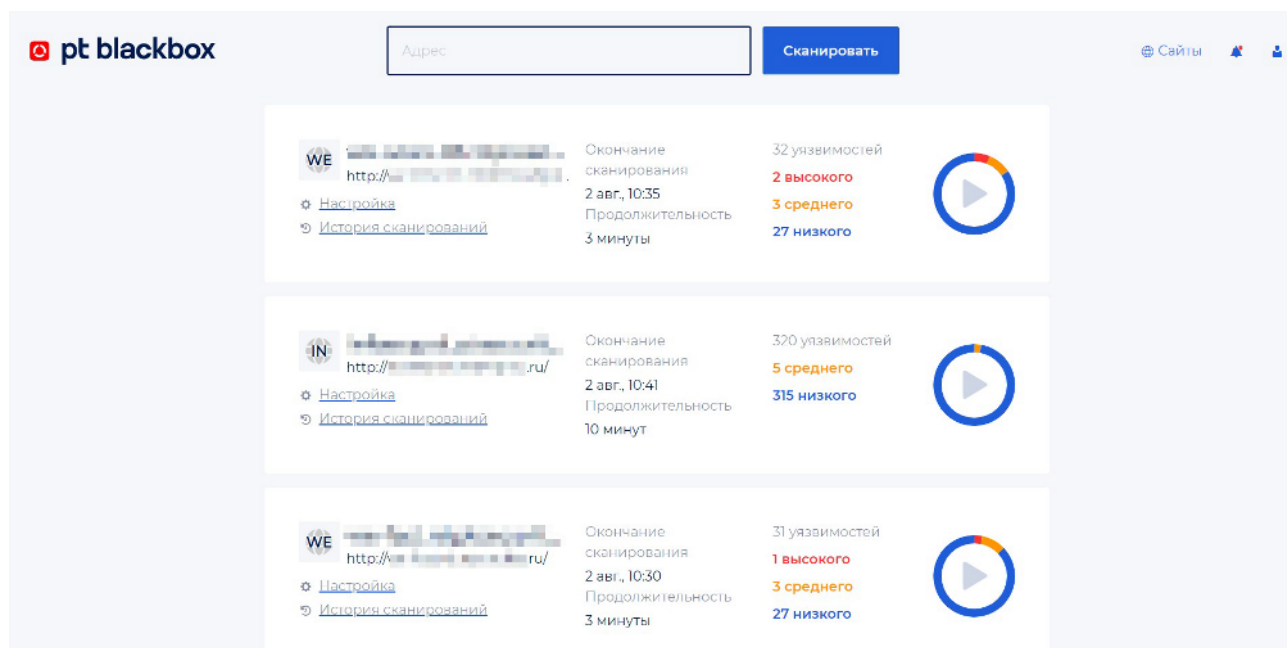


Рисунок 1. Страница Сайты

## 6.2.2. Страница с параметрами сканируемой цели

Страница с параметрами сканируемой цели содержит следующие кнопки — **Сайт**, **Аутентификация** и **Сканирование**.

По кнопке **Сайт** вы можете изменить название сканируемой цели или удалить информацию о цели.

По кнопке **Аутентификация** вы можете [изменить параметры аутентификации](#) (см. [раздел 6.4](#)) PT BlackBox при сканировании цели.

По кнопке **Сканирование** вы можете просмотреть профиль сканирования в формате XML, созданный PT BlackBox. Профиль предназначен для тонкой настройки сканирования. Вносить изменения в профиль сканирования не рекомендуется. Данная возможность доступна только для партнеров Positive Technologies в пилотной версии продукта.



## 6.2.3. Страница «Профиль»


Страница **Профиль** содержит кнопки: **Профиль** и **Токен аутентификации**.

По кнопке **Профиль** вы можете изменить параметры учетной записи пользователя (адрес почты, пароль и имя) и изменить язык веб-интерфейса PT BlackBox.

По кнопке **Токен аутентификации** вы можете получить токен аутентификации и использовать его для аутентификации вашего скрипта на сканируемом ресурсе. Это необходимо, если вы хотите [интегрировать](#) (см. [раздел 7](#)) PT BlackBox в процесс сборки.

## 6.2.4. Страница с результатами сканирования

В верхней части страницы отображается адрес сканируемого приложения и статус сканирования. По значку  вы можете просмотреть историю сканирования приложения. Для изменения параметров сканируемого приложения предусмотрена ссылка со значком . Кроме этого, страница с результатами сканирования содержит:

- Кнопку для управления сканированием — на кнопке отображается прогресс сканирования в процентах. С помощью кнопки вы можете останавливать и запускать сканирование.
- Кнопки с информацией о найденных уязвимостях — для удобства уязвимости распределены в группы, на кнопках отображается количество найденных уязвимостей в каждой группе. В группах могут быть уязвимости разного уровня опасности: низкого, среднего и высокого. Количество уязвимостей на кнопке выделено синим цветом, если в группе есть уязвимости только низкого уровня опасности; желтым, если в группе есть хотя бы одна уязвимость среднего уровня опасности; красным, если в группе есть хотя бы одна уязвимость высокого уровня опасности. Если во время сканирования не найдены уязвимости из какой-либо группы, такая группа отмечается значком .
- Кнопки для переключения между панелями с общей информацией о сканируемой цели (кнопка **Обзор**) и подробной информацией о найденных уязвимостях (кнопка **Уязвимости**).
- Две панели с информацией о сканировании.

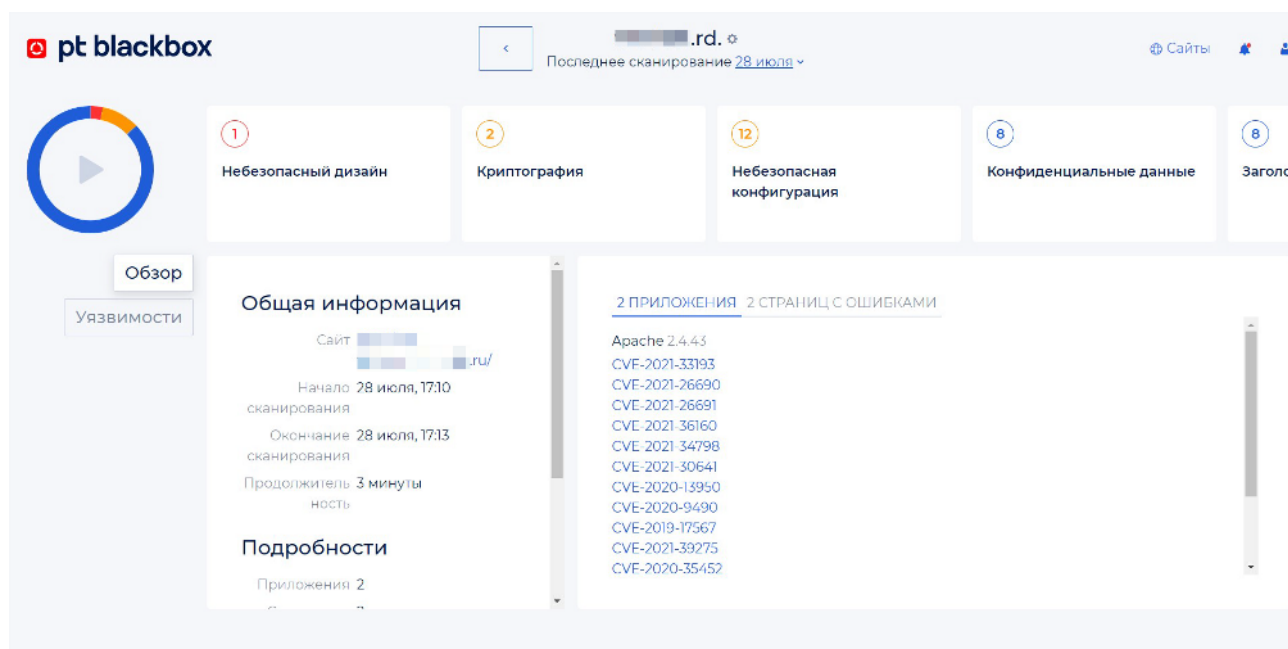


Рисунок 2. Страница с результатами сканирования



## Общая информация о цели сканирования

Общую информацию о цели сканирования вы можете просмотреть на странице с результатами сканирования по кнопке **Обзор**.

В левой панели содержится общая информация о сканируемой цели — адрес, дата и время начала и окончания сканирования, продолжительность сканирования, количество найденных приложений, страниц с ошибками, уязвимостей разных уровней опасности. Кроме того, в этой панели вы можете получить ссылку на страницу с результатами сканирования.

Правая панель содержит подробную информацию о найденных приложениях: название, версию и возможные уязвимости приложений. Кроме того, в панели отображаются названия и адреса страниц с ошибками сканируемого приложения.

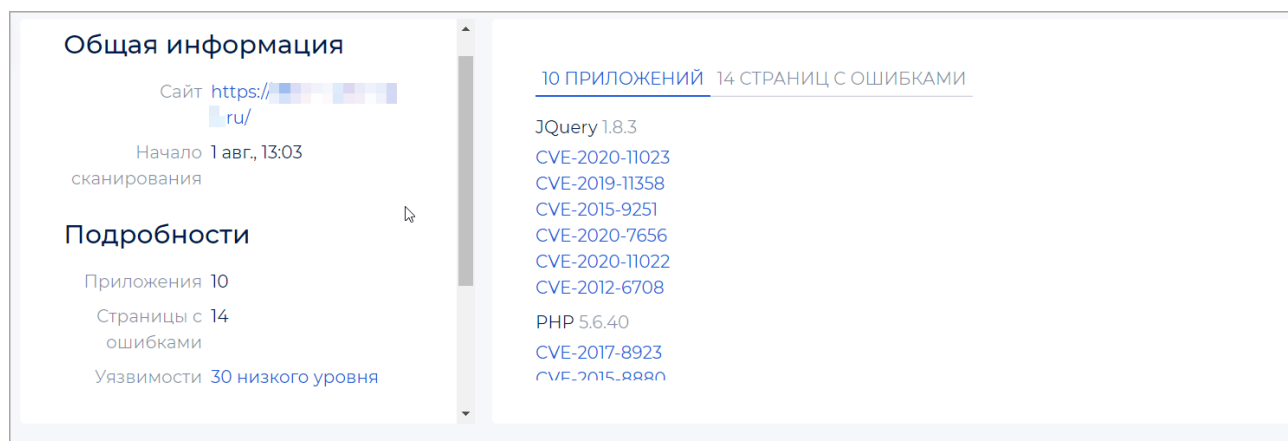


Рисунок 3. Панели с общей информацией о цели сканирования

## Информация о найденных уязвимостях

Подробную информацию о найденных при сканировании уязвимостях вы можете просмотреть на странице с результатами сканирования по кнопке **Уязвимости**.

В левой панели отображаются названия уязвимостей, в правой панели отображается подробная информация о выбранной уязвимости — описание, уровень опасности, адрес, по которому обнаружена уязвимость.

Вы можете переключаться между группами уязвимостей по кнопкам, расположенным над панелями. По нажатию на кнопку с нужной группой отображаются уязвимости только из этой группы.

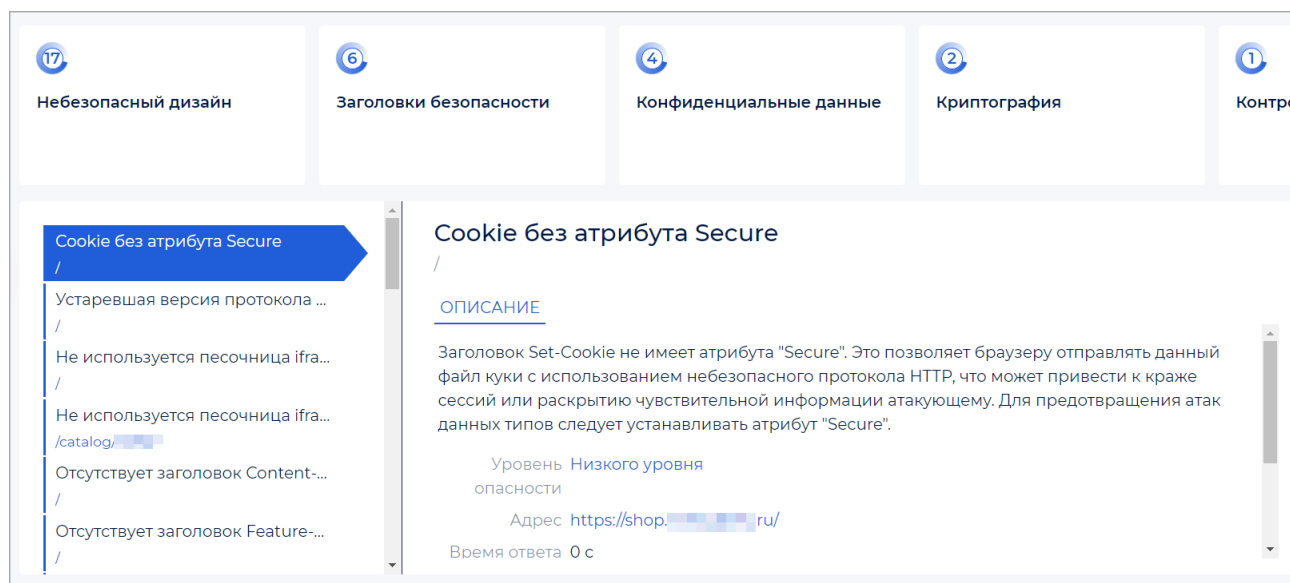


Рисунок 4. Панели с информацией о найденных уязвимостях

### 6.3. Запуск сканирования

При первом входе в систему откроется страница **Сайты**, на которой вы можете запустить сканирование вашего приложения. Также на этой странице отображается информация о текущих или уже завершенных сканированиях. Одновременно вы можете запускать не более пяти сканирований.

Если сканирование было по каким-то причинам остановлено, вы можете начать его сначала. История всех сканирований независимо от результата сохраняется и отображается на странице **Сайты** на карточках целей сканирования по ссылке **История сканирований**.

► Чтобы запустить сканирование:

1. В адресной строке браузера введите адрес `https://<DNS-имя или IP-адрес сервера с установленным PT BlackBox>`.

Откроется страница входа в PT BlackBox.

2. [Войдите в систему \(см. раздел 6.1\)](#).

Откроется страница [Сайты \(см. раздел 6.2.1\)](#).

3. В поле **Адрес** введите адрес приложения, которое необходимо проверить.
4. Нажмите кнопку **Сканировать**.

Откроется страница для указания параметров аутентификации.

## Подготовьтесь к сканированию своего сайта

### Укажите адрес сайта

PT BlackBox сканирует все подразделы по указанному адресу. Чтобы проверить сайт целиком, просто укажите его доменное имя (например, мойсайт.рф).

https://

### Настройте аутентификацию для сайта

Тип

Нет

Через форму на сайте

Базовая

Сканировать

Рисунок 5. Указание параметров аутентификации

5. Выберите тип аутентификации, используемый вашим приложением, и заполните нужные поля:
  - Если аутентификации нет, выберите вариант **Нет**.
  - Если аутентификация происходит через форму на сайте, выберите вариант **Через форму на сайте** и укажите параметры аутентификации.

- Если на сайте используется базовая аутентификация (basic access authentication, аутентификация, при которой имя пользователя и пароль передаются в виде открытого текста), выберите вариант **Базовая** и укажите параметры аутентификации.
6. Нажмите кнопку **Сканировать**.  
PT BlackBox начнет сканирование, откроется страница с результатами сканирования. Прогресс сканирования отобразится в левой части экрана.

По окончании сканирования появятся [итоговые результаты](#) (см. раздел 6.5) сканирования и рекомендации по устранению уязвимостей.

### См. также

[Страница «Сайты»](#) (см. раздел 6.2.1)

[Просмотр результатов и истории сканирования](#) (см. раздел 6.5)

## 6.4. Изменение параметров аутентификации

Вы можете изменить тип и параметры аутентификации PT BlackBox на выбранной цели сканирования. Изменять параметры вы можете после окончания сканирования.

► Чтобы изменить тип и параметры аутентификации:

1. Перейдите на страницу **Сайты**.
2. На карточке нужной цели сканирования нажмите ссылку **Настройка**.  
Откроется [страница с параметрами сканируемой цели](#) (см. раздел 6.2.2).
3. Нажмите кнопку **Аутентификация**.
4. Выберите нужный тип аутентификации.
5. Введите данные для аутентификации, если это необходимо.
6. Если вы хотите сохранить новые параметры аутентификации, нажмите кнопку **Сохранить**.
7. Если вы хотите, чтобы PT BlackBox проверил возможность аутентификации с новыми параметрами, а затем сохранил их, нажмите **Сохранить и проверить**.

Параметры аутентификации изменены.

### См. также

[Страница с параметрами сканируемой цели](#) (см. раздел 6.2.2)

## 6.5. Просмотр результатов и истории сканирования

Просмотреть результаты и историю сканирования вы можете на странице **Сайты**. Эта страница открывается по умолчанию после первого сканирования при последующих входах в систему.

Просмотр результатов сканирования доступен сразу после его начала. Дождаться окончания сканирования при этом не обязательно. В процессе сканирования вы также, не дожидаясь его окончания, можете поделиться ссылкой с результатами сканирования.

► Чтобы просмотреть результаты сканирования:

1. В адресной строке браузера введите адрес `https://<DNS-имя или IP-адрес сервера с установленным PT BlackBox>`.

Откроется страница [Сайты](#) (см. раздел 6.2.1).

2. На карточке нужного ресурса нажмите ссылку **История сканирования**.

3. Во всплывающем окне по ссылке с нужным сканированием перейдите на [страницу с результатами сканирования](#) (см. раздел 6.2.4).

4. Если вы хотите просмотреть общую информацию о сканируемом ресурсе или приложении, в левой части экрана нажмите кнопку **Обзор**.

Откроется панель с информацией о приложениях, используемых ресурсом, и страницах с ошибками.

5. Если вы хотите просмотреть подробную информацию о найденных уязвимостях и получить рекомендации по их устранению, в левой части экрана нажмите кнопку **Уязвимости**.

Откроется страница с уязвимостями и рисками, найденными в процессе сканирования. Для удобства они распределены по группам, которые отображаются в верхней части экрана.

Вы можете получить ссылку на страницу с результатами сканирования, чтобы поделиться ими.

► Чтобы получить ссылку на страницу с результатами сканирования:

1. Нажмите кнопку **Обзор**.

2. В левой панели нажмите значок **Сохранить и поделиться** .


Появится ссылка на страницу с результатами сканирования.

3. В раскрывающемся списке **Срок действия** выберите срок действия сгенерированной ссылки.

4. Нажмите значок .

Ссылка получена.

## 6.6. Работа с уведомлениями

Вы можете просматривать уведомления о завершенных сканированиях и о статусе аутентификации на сканируемых ресурсах. Уведомления отображаются на главной странице PT BlackBox в правом верхнем углу по нажатию на значок . В уведомлениях

отображаются адреса проверенных ресурсов, информация о результатах сканирования и результаты аутентификации. Из панели с уведомлениями вы можете перейти к просмотру результатов сканирования.

► Чтобы перейти к просмотру результатов сканирования:

1. Перейдите на главную страницу PT BlackBox.

2. В правом верхнем углу нажмите .

Откроется панель с уведомлениями.

3. Нажмите на уведомление о сканировании, результаты которого вы хотите просмотреть.

Откроется страница с результатами сканирования.

## 7. Интеграция в CI/CD

PT BlackBox может быть встроен в процесс непрерывной интеграции (CI/CD) на агентах сборки, что позволяет автоматизировать процесс тестирования безопасности разрабатываемых приложений.

Ссылка для скачивания скриптов для интеграции и генератор токенов аутентификации для них находятся на странице **Профиль** → **Токен аутентификации**. По этой ссылке вы можете скачать нужные скрипты и прочитать подробную информацию о работе с ними в файле README.md.

### **См. также**

[Страница «Профиль» \(см. раздел 6.2.3\)](#)

## 8. Удаление PT BlackBox

- ▶ Чтобы удалить PT BlackBox,

последовательно выполните следующие команды:

```
docker stop $(docker ps -a -q)
docker rm -vf $(docker ps -a -q)
docker rmi -f $(docker images -a -q)
docker volume rm $(docker volume ls -q)
docker network prune -f
```

PT BlackBox удален.



## 9. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на [портале](#).

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

### В этом разделе

[Техническая поддержка на портале \(см. раздел 9.1\)](#)

[Время работы службы технической поддержки \(см. раздел 9.2\)](#)

[Как служба технической поддержки работает с запросами \(см. раздел 9.3\)](#)

### 9.1. Техническая поддержка на портале

[Портал](#) предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

[Портал](#) содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

### 9.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

## 9.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

### В этом разделе

[Предоставление информации для технической поддержки \(см. раздел 9.3.1\)](#)

[Типы запросов \(см. раздел 9.3.2\)](#)

[Время реакции и приоритизация запросов \(см. раздел 9.3.3\)](#)

[Выполнение работ по запросу \(см. раздел 9.3.4\)](#)

### 9.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

### 9.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

#### Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

## Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

## Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

## Обновление продукта

Positive Technologies предоставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

## Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

### 9.3.3. Время реакции и приоритизация запросов

**Время реакции** на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

**Время обработки** запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 4).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 4. Время реакции на запрос и время его обработки

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

### 9.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

- о диагностике проблемы и ее результатах;
- о поиске решения или возможности обойти причины возникновения проблемы;
- о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

- предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;
- проблема классифицирована как неподдерживаемая.