



BlackBox

версия 3.3

Руководство администратора

© Positive Technologies, 2026.

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: 07.09.2026

Содержание

1.	Об этом документе.....	4
2.	О сканере Positive Technologies BlackBox.....	5
3.	Состав компонентов ПО и его среды функционирования	6
4.	Аппаратные и программные требования	8
5.	Лицензирование	9
6.	Подготовка к установке PT BlackBox.....	10
7.	Установка PT BlackBox.....	14
8.	Обновление PT BlackBox	21
9.	Настройка аутентификации через SSO	22
10.	О технической поддержке	24

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по администрированию Positive Technologies BlackBox (далее также — PT BlackBox). Руководство также содержит инструкции по установке PT BlackBox и использованию основных функций продукта.

Руководство адресовано специалистам, администрирующим PT BlackBox.

Комплект документации PT BlackBox включает в себя следующие документы:

- Этот документ.
- Руководство пользователя — содержит подробную информацию о сценариях работы с продуктом, о настройке функций продукта для решения конкретных задач.
- Руководство по интеграции — содержит информацию по внедрению PT BlackBox в сборочный процесс CI-систем.
- Справочное руководство по REST API — содержит информацию о доступных функциях сервиса REST API в PT BlackBox.

2. О сканере Positive Technologies BlackBox

PT 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 PT 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 нескольких приложений (в зависимости от вида лицензии).
- Сканирование целей, для доступа к которым необходима авторизация.
- Возможность встроить PT BlackBox в процесс непрерывной интеграции и развертывания (CI/CD) с авторизацией по токenu. Используя специальные скрипты, пользователь сканера может встроить проверку своего приложения в процесс его сборки.

3. Состав компонентов ПО и его среды функционирования

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

- реляционная система управления базами данных PostgreSQL для хранения пользовательских данных и результатов сканирования;
- система управления базами данных Redis версии 7.2 для хранения данных активных сессий;
- брокер сообщений RabbitMQ;
- сервер сообщений Centrifugo;
- высокопроизводительное объектное хранилище данных MinIO;
- платформа аутентификации и авторизации пользователей CasGate;
- интерпретатор языка программирования Python 3.11 для выполнения кода компонентов ядра и приложения;
- интерпретатор языка программирования Golang (Go) для выполнения кода компонентов приложения.

Среда функционирования ПО включает:

- операционную систему Debian версии 10 или 11, Ubuntu версии 20.04, 22.04 или Astra Linux Special Edition версии 1.7 («Воронеж»);
- платформу управления контейнерами Kubernetes (K8s);
- веб-сервер nginx для работы Ingress-контроллера, который используется для проксирования доступа к сервисам Kubernetes.

В таблице ниже дана информация о лицензиях компонентов ПО.

Таблица 1. Лицензии компонентов ПО

Название компонента	Лицензия	Правообладатель	Ссылка на текст лицензии
PostgreSQL	PostgreSQL	1996—2024, The PostgreSQL Global Development Group. 1994, The Regents of the University of California	postgresql.org/about/licence/
Redis	RSALv2, SSPLv1	2023, Redis Ltd., 2018, MongoDB, Inc.	github.com/redis/redis/
RabbitMQ	MPL 2.0	VMware, Inc. или ее дочерние компании	rabbitmq.com/
Centrifugo	Apache 2.0	2023, Centrifugal Labs LTD	github.com/centrifugal/

Название компонента	Лицензия	Правообладатель	Ссылка на текст лицензии
Python 3.11	PSF-2.0	Python Software Foundation	docs.python.org/3.11/
CasGate	Apache 2.0	2024, Apache Software Foundation	github.com/casgate/
Golang (Go)	BSD 3-Clause	2009, The Go Authors	go.dev/
MinIO	GNU Affero General Public License v3.0	2007, MinIO, Inc.	github.com/minio/
Nginx	BSD 2-Clause	2011–2024, Nginx, Inc.	github.com/nginx/
Kubernetes (K8s)	Apache 2.0	2004, Cloud Native Computing Foundation	github.com/kubernetes/

4. Аппаратные и программные требования

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

Внимание! Не рекомендуется устанавливать антивирусы в операционной системе. Это может помешать установке PT BlackBox, вызвать сбои в его работе или привести к другим непредсказуемым последствиям.

PT BlackBox рекомендуется устанавливать на чистую 64-разрядную ОС. Поддерживаются:

- при установке на платформе Kubernetes ОС семейства Linux: Debian версий 11 и 12, Astra Linux Special Edition версии 1.7 («Воронеж») и выше;
- при установке на платформе Docker: Ubuntu 24.04 и 22.04, Debian 11, 12, Astra Linux Special Edition 1.8, «Альт Сервер» 10.4 и «РЕД ОС» 8.

Для корректного запуска сканирования целей в операционной системе должен быть установлен компонент sgroups версии 2 и выше.

Внимание! Для корректной установки PT BlackBox в операционной системе должна быть установлена утилита netcat.

Если планируется установка PT BlackBox на платформе Docker, необходимо установить на сервере Docker Engine версии не ниже 20.10, плагин Docker Compose версии не ниже 2.21.0 и утилита OpenSSL.

Таблица 2. Аппаратные требования

Параметр	Минимальные требования	Рекомендуемые требования
Центральный процессор	8 виртуальных или физических ядер	4 ядра на одно сканирование и 1 ядро для системы (для 5 параллельных сканирований необходимо 21 ядро)
Память (ОЗУ)	16 ГБ	4 ГБ на одно сканирование и 2 ГБ для системы (для 5 параллельных сканирований необходимо 22 ГБ)
Жесткий диск (HDD)	180 ГБ	От 180 ГБ (для хранения истории сканирований)

5. Лицензирование

Для работы PT BlackBox, его защиты от нелегального использования и получения обновлений из базы знаний экспертного центра Positive Technologies нужна лицензия.

При покупке лицензии устанавливается срок ее действия. В течение срока действия лицензии вы можете пользоваться всей функциональностью PT BlackBox.

По истечении срока действия лицензии вы можете работать с результатами сканирований, полученными ранее, но при этом следующие функции продукта будут недоступны:

- обновление продукта, сервиса обновлений и базы знаний;
- восстановление предыдущей версии базы знаний;
- создание цели сканирования;
- запуск сканирования.

Одна лицензия может быть активирована только в одном экземпляре PT BlackBox.

Лицензии различаются по количеству приложений, которые можно сканировать одновременно.

6. Подготовка к установке PT BlackBox

Перед началом установки PT BlackBox необходимо выполнить следующие действия:

1. Убедиться, что сервер соответствует [аппаратным и программным требованиям](#) (см. раздел 4).
2. Разрешить входящее и исходящее подключение к портам TCP 80 и 443.
3. На DNS-сервере предприятия добавить записи типа «А» для доменных имен PT BlackBox (например, `blackbox.example.com`) и сервиса аутентификации (например, `auth-blackbox.example.com`).
4. Если планируется установка PT BlackBox на платформе Docker, установить на сервере Docker Engine версии не ниже 19.03.0 и плагин Docker Compose версии не ниже 1.28.
5. Распаковать архив с дистрибутивом PT BlackBox.
6. Настроить конфигурационные параметры PT BlackBox.
7. Если планируется миграция данных, перенести ключ шифрования из версии 2.8 в версию 3.2.

Распаковка архива с дистрибутивом PT BlackBox

Примечание. Архив с дистрибутивом для развертывания PT BlackBox на платформе Kubernetes поставляется с названием `bbs_deployer_<Версия продукта>.tar.gz`, для развертывания в Docker — с названием `bbs_docker_deployer_<Версия продукта>.tar.gz`.

► Чтобы распаковать архив с дистрибутивом PT BlackBox:

1. Сохраните архив с дистрибутивом PT BlackBox в любой каталог.
2. Перейдите в каталог с архивом:
`cd <Имя каталога>`
3. Создайте каталог, в который будет распакован установочный комплект, например `bbs-installer`:
`mkdir bbs-installer`
4. Распакуйте архив в созданный каталог:
`tar -xvf bbs_deployer_<Версия продукта>.tar.gz -C bbs-installer/`

При развертывании в Docker каталог с распакованным архивом является установочным каталогом продукта (из него можно перезапускать, обновлять продукт, изменять конфигурационные файлы). При развертывании в Kubernetes в распакованном архиве находится установщик, который при установке развернет продукт PT BlackBox и далее использоваться не будет.

Архив с установщиком PT BlackBox распакован.

Теперь вы можете перейти к настройке конфигурационных параметров.

Настройка конфигурационных параметров PT BlackBox

► Чтобы настроить конфигурационные параметры PT BlackBox:

1. Откройте каталог с установочным комплектом.
2. Откройте на редактирование конфигурационный файл `my_vars.env`.

Внимание! Набор параметров в конфигурационном файле будет различаться в зависимости от платформы, на которую устанавливается PT BlackBox.

3. Укажите параметры, описанные в таблице ниже (см. таблицу 3).
4. Сохраните изменения и закройте файл.

Таблица 3. Параметры конфигурационного файла

Параметр	Обязательный		Описание
	K8s	Docker	
YOUR_USER YOUR_PASSWORD	+	-	Логин и пароль учетной записи для подключения к узлу, на котором устанавливается PT BlackBox. Учетная запись должна иметь права на установку ПО
YOUR_DNS	+	+	Доменное имя PT BlackBox (например, <code>blackbox.example.com</code>)
YOUR_AUTH_DNS	+	+	Доменное имя сервиса аутентификации (например, <code>auth-blackbox.example.com</code>)
YOUR_IP	+	-	IP-адрес узла, на котором устанавливается PT BlackBox
YOUR_LICENSE_TOKEN	+	+	K8s Токен лицензии, который хранится в файле <code>license-access-token.key</code> Docker Путь к файлу, где хранится токен лицензии (абсолютный или относительно каталога с распакованным установщиком)
YOUR_REGISTRY	+	-	Адрес хранилища Docker Registry
YOUR_KUBECONFIG	+	-	Путь к конфигурационному файлу для управления кластерами Kubernetes (kubeconfig)
YOUR_NAMESPACE	+	-	Название пространства имен (namespace) Kubernetes

Параметр	Обязательный		Описание
	K8s	Docker	
BACKEND_ENCRYPTION_KEY	+	+	Ключ шифрования данных авторизации, которые используются при сканировании целей. Параметр обязателен для заполнения, если планируется миграция данных из версии 2.8 в версию 3.2. Подробности см. в разделе Перенос ключа шифрования
BACKEND_PROXY_USER_ALLOWED	+	+	Разрешить использование прокси-сервера, указанного в профиле сканирования. По умолчанию — true
DEFAULT_PROXY_HOST DEFAULT_PROXY_PORT DEFAULT_PROXY_TYPE	+	+	Адрес, порт и тип прокси-сервера, который будет использоваться по умолчанию при сканировании. Все параметры обязательны, если задано значение хотя бы одного из них. Возможные значения DEFAULT_PROXY_TYPE: http, http_no_connect, https, socks5h, socks5, socks4, transparent Примечание. При сканировании цели указанные параметры игнорируются, если включен параметр BACKEND_PROXY_USER_ALLOWED и в профиле сканирования задан другой прокси-сервер
DEFAULT_PROXY_USERNAME DEFAULT_PROXY_PASSWORD	+	+	Логин и пароль учетной записи для подключения к прокси-серверу. Параметры обязательны, если задано значение хотя бы одного из них
BACKEND_SCAN_PRIVATE_IPS	+	+	Разрешить сканирование IP-адресов частной сети. По умолчанию — true
TLS_CERT	+	+	K8s TLS-сертификат (в формате Base64, в двойных кавычках). При пустом значении автоматически создается самоподписанный сертификат Docker Путь к файлу, где хранится сертификат (абсолютный или относительно каталога с распакованным установщиком)
TLS_KEY	+	+	K8s Ключ TLS-сертификата. Значение указывается в двойных кавычках

Параметр	Обязательный		Описание
	K8s	Docker	
			Docker Путь к файлу, где хранится ключ от TLS-сертификата (абсолютный или относительно каталога с распакованным установщиком)
BLACKBOX_POSTGRES_HOST	+	+	IP-адрес или FQDN сервера с БД PostgreSQL для PT BlackBox Позволяют настроить подключение к сторонней базе PostgreSQL для хранения данных, если используется внешняя БД (должно быть установлено расширение uuid-osspl)
BLACKBOX_POSTGRES_PORT	+	+	Порт для подключения к БД
BLACKBOX_POSTGRES_DB	+	+	Имя БД
BLACKBOX_POSTGRES_USER	+	+	Имя пользователя БД
BLACKBOX_POSTGRES_PASSWORD	+	+	Пароль пользователя БД
IAM_POSTGRES_HOST	+	+	IP-адрес или FQDN сервера с БД PostgreSQL для CasGate. Позволяют настроить подключение к сторонней базе PostgreSQL для хранения данных о пользователях
IAM_POSTGRES_PORT	+	+	Порт для подключения к БД
IAM_POSTGRES_DB	+	+	Имя БД
IAM_POSTGRES_USER	+	+	Имя пользователя БД
IAM_POSTGRES_PASSWORD	+	+	Пароль пользователя БД

Теперь вы можете перейти к установке PT BlackBox.

7. Установка PT BlackBox

PT BlackBox устанавливается в односерверной конфигурации. Перед установкой убедитесь, что выполнены подготовительные действия.

Внимание! Не рекомендуется устанавливать антивирусы в операционной системе. Это может помешать установке PT BlackBox, вызвать сбои в его работе или привести к другим непредсказуемым последствиям.

Возможны следующие варианты развертывания:

- Установка на платформе Docker — PT BlackBox устанавливается на целевом сервере. Этот способ рекомендуется для новых развертываний, он проще в настройке и управлении.
- Установка на платформе Kubernetes — PT BlackBox устанавливается с внешнего сервера. Для этого необходим SSH-доступ (по логину и паролю) к целевому серверу.

В процессе установки и проверки лицензии PT BlackBox обращается к серверам обслуживания Positive Technologies на поддоменах сайта ptsecurity.com.

Внимание! Если в вашей информационной системе используется межсетевой экран или другие средства контроля сетевого трафика, необходимо настроить в них правила, разрешающие доступ по протоколу HTTPS к серверам Positive Technologies со всех узлов PT BlackBox.

► Чтобы установить PT BlackBox на платформе Docker:

1. Перейдите в каталог с установочным комплектом:

```
cd bbs-installer/
```

2. Выдайте разрешение на исполнение файла `install.sh`:

```
chmod +x install.sh
```

3. Запустите сценарий установки PT BlackBox (распаковывать, устанавливать и запускать установку нужно под одним пользователем):

```
./install.sh
```

PT BlackBox установлен.

► Чтобы установить PT BlackBox на платформе Kubernetes:

1. Перейдите в каталог с установочным комплектом:

```
cd bbs-installer/
```

2. Выдайте разрешение на исполнение файла `run.sh`:

```
chmod +x run.sh
```

3. Запустите сценарий установки PT BlackBox от имени суперпользователя:

```
./run.sh
```

PT BlackBox установлен.

Утилита `bbctl`

Для управления работой PT BlackBox, установленного на платформе Docker, используется утилита `bbctl`. Вы можете запустить утилиту в консоли из любого каталога с помощью команды `bbctl`. Перечень доступных команд утилиты и их описание приведены в таблице ниже. Использовать описанные команды можно только после установки продукта, кроме команды `restore`. Если после установки PT BlackBox команда `bbctl` не выполняется без указания полного пути через `/`, то вам нужно завершить текущую пользовательскую сессию и войти в систему повторно.

Таблица 4. Список команд для работы с `bbctl`

Команда	Описание	Аргументы и примеры	Переменные окружения	Нужно подтверждение в консоли
<code>bbctl start</code>	Запускает все сервисы PT BlackBox	—	—	Нет
<code>bbctl stop</code>	Останавливает и удаляет все контейнеры PT BlackBox (в том числе встроенные контейнеры БД или хранилища)	—	—	Нет
<code>bbctl reconf</code>	Применяет конфигурацию из файла <code>my_vars.env</code>: переключает БД с внутренней на внешнюю (с удалением тома хранилища данных внутренней БД) или хранилище (артефакты сканирования при смене хранилища удаляются), применяет TLS-сертификат и ключ, лицензионный токен. В дистрибутив входит шаблон <code>my_vars.env.dist</code>. Вам необходимо самостоятельно переименовать этот шаблон в <code>my_vars.env</code> и заполнить вручную, либо запустить скрипт <code>install.sh</code> для автоматического создания файла из шаблона.	—	—	При смене БД или хранилища

Команда	Описание	Аргументы и примеры	Переменные окружения	Нужно подтверждение в консоли
	Внимание! Для сохранения данных и переноса их в другой источник создайте резервную копию до применения команды <code>reconf</code>			
<code>bbctl renew_cert</code>	Генерирует и применяет новый самоподписанный TLS-сертификат (только при работе с самоподписанным сертификатом)	—	—	Нет
<code>bbctl reset_password</code>	Сбрасывает пароль пользователя с указанной эл. почтой. Пароль задается интерактивно или через переменную <code>NEW_PASSWORD</code> , 8–256 символов. Нельзя использовать для пользователей, зарегистрированных через стороннюю систему SSO	Email. Например, для сброса пароля: <code>bbctl reset_password ivanov@example.org</code> Например, для установки нового пароля: <code>NEW_PASSWORD='Str0ng!Pass'</code> <code>bbctl reset_password ivanov@example.org</code>	<code>EMAIL, NEW_PASSWORD</code>	Нет
<code>bbctl register_users</code>	Регистрирует пользователей, указанных в JSON-файле (или с помощью стандартного ввода, если файл не указан). Требуется утилита <code>jq</code> .	Файл. В дистрибутив включены JSON-схемы <code>users.schema.ru.json</code> и <code>users.schema.en.json</code> , описывающие тре-	—	Нет

Команда	Описание	Аргументы и примеры	Переменные окружения	Нужно подтверждение в консоли
	В файле необходимо указать список учетных записей пользователей, можно указать группу учетных записей пользователей. Поля для создания учетной записи пользователя: — <code>email</code> — обязательно; — <code>password</code> — обязательно, 8–256 символов; — <code>firstname</code> — необязательно; — <code>lastname</code> — необязательно; — <code>role</code> — необязательно, системная роль пользователя: <code>guest</code> или <code>admin</code> (по умолчанию — <code>guest</code>). Поля для создания группы: — <code>name</code> — обязательно при наличии <code>group</code>; — <code>role</code> — необязательно, групповая роль: <code>moderator</code>, <code>operator</code> или <code>auditor</code> (по умолчанию — <code>auditor</code>).	буемый формат файла. Обе JSON-схемы расположены в каталоге <code>./user-schemas</code> относительно каталога с распакованным дистрибутивом PT BlackBox		
<code>bbctl backup</code>	Создает резервную копию продукта в виде архива <code>ptblackbox-backup-<code><Номер версии></code>-<code><Дата-Время></code>.tar</code> . Сохраняет в указанный каталог (по умолчанию <code>./backups</code>).	<code>--only <Названия компонентов></code> <code>--no-restart</code> Название каталога.	—	Да

Команда	Описание	Аргументы и примеры	Переменные окружения	Нужно подтверждение в консоли
	Копия состоит из компонентов; по умолчанию сохраняются все: — <code>db</code> — логические дампы баз данных PT BlackBox и IAM (как встроенного PostgreSQL, так и внешнего); — <code>s3</code> — пообъектная копия объектного хранилища (встроенного MinIO или внешнего S3). Артефакты сканирования не включаются в копию и не переносятся между разными S3-хранилищами; — <code>volumes</code> — тома с локальным состоянием сервисов; — <code>images</code> — образы контейнеров установленного продукта и служебные образы. Конфигурация на хосте (<code>.env</code>, <code>my_vars.env</code>, <code>versions.env</code>, compose-файлы, сертификаты, каталог <code>data/</code>, а также <code>VERSION</code>, <code>bbctl</code>, <code>bbctl.d</code>, <code>env.dist</code>) включается в архив всегда. Флаг <code>--only</code> сужает копию до перечисленных через запятую компонентов.	Например, для указания компонентов: <pre>bbctl backup --only db,s3</pre> Например, для того, чтобы продукт остался остановленным после создания копии: <pre>bbctl backup --no-restart /mnt/backups</pre>		

Команда	Описание	Аргументы и примеры	Переменные окружения	Нужно подтверждение в консоли
	Флаг <code>--no-restart</code> оставляет продукт остановленным после создания копии. Когда резервная копия создана, архив проверяется на целостность			
<code>bbctl restore</code>	Восстанавливает резервную копию из архива, созданного командой <code>backup</code>, и запускает ее. Перед началом из архива считывается метаданная (дата создания, версия продукта) и запрашивается подтверждение; затем проверяется целостность архива. Если данные восстанавливаются во внешнюю БД или внешнее S3, их доступность проверяется до внесения каких-либо изменений. Команду возможно запустить в одном из режимов: — Полное восстановление (запускается по умолчанию, без флага <code>--only</code>) — выполняется полная замена текущей установки. Удаляются все имеющиеся контейнеры и тома, а из архива восстанавливаются конфигурация, образы и данные (дампы загружаются в те БД и	Архив в формате TAR. <code>--only <Названия компонентов></code> Например, для запуска в режиме полного восстановления: <pre>bbctl restore ./backups/ptblackbox-backup-3.2-20260618-181500.tar</pre> Например, для запуска в режиме частичного восстановления: <pre>bbctl restore --only db ./backups/ptblackbox-backup-3.2-20260618-181500.tar</pre>	—	Да

Команда	Описание	Аргументы и примеры	Переменные окружения	Нужно подтверждение в консоли
	хранилище, которые прописаны в конфигурации архива). Предназначена для восстановления после серьезного сбоя или переноса продукта на другой сервер. — Частичное восстановление (запускается с флагом <code>--only</code> или для частичных архивов) — выполняется выборочное замещение компонентов (<code>db</code>, <code>s3</code>, <code>volumes</code>, <code>images</code> — только тех, что есть в архиве). Текущая конфигурация и остальные компоненты остаются без изменений, а данные загружаются в БД и хранилище согласно текущей конфигурации хоста. Предназначена для точечного восстановления отдельных элементов. Требуется, чтобы продукт уже был установлен			
<code>bbctl uninstall</code>	Полностью удаляет PT BlackBox: контейнеры, образы, тома, файлы конфигурации и сертификаты. Удаляются также все данные во встроенных базах	—	—	Да

8. Обновление PT BlackBox

Процесс обновления PT BlackBox зависит от варианта его установки. Обновление PT BlackBox, установленного на платформе Docker, происходит локально на целевом сервере. Обновление PT BlackBox, установленного на платформе Kubernetes, происходит с внешнего сервера и требует SSH-доступ (по логину и паролю).

Внимание! Перед обновлением рекомендуется создать резервную копию данных и конфигурационного файла `my_vars.env`.

► Чтобы обновить PT BlackBox, установленный на платформе Docker:

1. Распакуйте архив `bbs_docker_deployer <Версия продукта>.tar.gz` в каталог с установщиком предыдущей версии PT BlackBox.
2. Скопируйте параметры конфигурационного файла `my_vars.env` версии 3.2 и перенесите их в конфигурационный файл версии 3.3.
3. Перейдите в каталог с установщиком и выдайте разрешение на исполнение файла `update.sh`:
`chmod +x update.sh`
4. Запустите скрипт (с флагом `--no-backup`, если не нужно создавать резервную копию):
`./update.sh`

Пример команды с флагом:

```
./update.sh --no-backup
```

При обновлении с версий ниже 3.3 (например, с версии 3.2 на версию 3.3) резервная копия не создается автоматически. При обновлении с версии 3.3 и выше резервная копия создается автоматически, если не отключить создание флагом `--no-backup`.

► Чтобы обновить PT BlackBox на платформе Kubernetes:

1. Распакуйте архив с дистрибутивом продукта.
2. Скопируйте параметры конфигурационного файла `my_vars.env` версии 3.2 и перенесите их в конфигурационный файл версии 3.3.
3. Перейдите в каталог с установщиком:
`cd bbs-installer/`
4. Выдайте разрешение на исполнение файла `run.sh`:
`chmod +x run.sh`
5. Запустите сценарий установки PT BlackBox от имени суперпользователя (root):
`./run.sh`

9. Настройка аутентификации через SSO

В PT BlackBox возможна аутентификация и авторизация пользователей через стороннюю систему SSO по протоколу OpenID. Такая система не входит в комплект поставки, перед настройкой подключения в PT BlackBox необходимо установить и настроить ее самостоятельно.

Примечание. После настройки аутентификации через SSO, если у пользователя SSO-системы также есть локальная учетная запись PT BlackBox, ему будет доступна любая форма входа в продукт — напрямую или через форму SSO-системы.

► Чтобы настроить аутентификацию через SSO:

1. Перейдите на страницу **Панель управления**.
2. Выберите вкладку **Единый вход (SSO)**.
3. Нажмите **Добавить подключение**.
4. В поле **Код клиента** укажите имя клиента, указанное при регистрации в системе SSO.
5. Укажите секрет клиента, сгенерированный в системе SSO.
6. В поле **Адрес конфигурации OpenID** укажите конечную точку конфигурации в области realm.
7. Если требуется, укажите ключ сертификата SSO-системы для соединения по HTTPS.
8. Выберите вкладку **Соответствие пользователей**.
9. Укажите атрибут идентификатора пользователя SSO-системы.
10. Укажите атрибут электронной почты, адрес которой будет использован для дополнительной идентификации пользователя в PT BlackBox.
11. Укажите атрибут логина учетной записи, который будет использоваться при входе в PT BlackBox.
12. Укажите атрибуты имени и фамилии пользователя.
13. Нажмите **Добавить**.
14. Активируйте подключение.

Настройка соответствия ролей

С помощью атрибутов вы можете назначить пользователю SSO-системы системную роль в PT BlackBox.

► Чтобы настроить соответствие ролей:

1. Перейдите на страницу **Панель управления**.
2. Выберите вкладку **Единый вход (SSO)**.

3. Выберите вкладку **Соответствие ролей**.
4. Нажмите **Добавить соответствие**.
5. В блоке параметров **Сторонняя система** укажите атрибут SSO-системы, который будет использован при назначении роли в PT BlackBox.
6. Укажите значения атрибута через клавишу Enter.
7. В блоке параметров **PT BlackBox** выберите системную роль (**Администратор** или **Менеджер**), которая будет назначена пользователю в соответствии с указанным атрибутом.
8. Нажмите **Сохранить**.

10. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на PT BlackBox в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках гарантийной поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

Примечание. Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы и сроки ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются [на портале технической поддержки](#).

Портал технической поддержки

[На портале технической поддержки](#) вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к portalу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку [на портале технической поддержки](#) и предоставить следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг гарантийной поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решению проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по гарантийной поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 5. Время реакции на заявку

Уровень значимости заявки	Критерии значимости заявки	Время реакции на заявку
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

- о ходе диагностики по заявленной проблеме и ее результатах;
- планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.



Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.