



Data Security

версия 1.6.0

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: 17.09.2026

Содержание

1.	Об этом документе.....	4
1.1.	Условные обозначения.....	4
1.2.	Другие источники информации о PT DS	5
2.	Обзор PT Data Security.....	6
3.	Аппаратные и программные требования	8
4.	Лицензирование	10
5.	Развертывание PT DS.....	13
5.1.	Установка коннекторов отдельно от PT DS.....	14
5.2.	Установка и настройка шлюза обработки трафика.....	16
6.	Обновление PT DS.....	18
7.	Настройка доступов пользователей и аутентификация в PT DS.....	19
8.	Удаление PT DS.....	21

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по развертыванию, настройке и администрированию PT Data Security (далее также — PT DS). Руководство не содержит инструкций по использованию основных функций продукта.

Руководство адресовано специалистам, выполняющим установку, первоначальную настройку и администрирование PT DS.

Комплект документации PT DS 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.

В этом разделе

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

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

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. 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 OK	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду <i>Stop-Service</i>	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 DS

Вы можете найти дополнительную информацию о PT DS на справочном портале help.ptsecurity.com и на [Позитивном портале](#). Через Позитивный портал вы также можете обратиться в техническую поддержку.

2. Обзор PT Data Security

PT Data Security (далее также PT DS) — это система, предназначенная для защиты важных данных, которые хранит и обрабатывает организация. PT DS позволяет следить за тем, где и как хранятся данные (например, в таблицах или документах), сортирует их по степени важности для бизнеса и проверяет правомерность доступа к ним. Кроме того, PT DS оценивает риски утечки информации и других инцидентов, связанных с данными, помогает обнаружить подозрительные и зловердные обращения к данным.

Возможности

- Инвентаризация инфраструктуры хранения структурированных и неструктурированных данных.
- Классификация данных по уровню важности для бизнеса организации.
- Отслеживание обращений пользователей к данным, выявление подозрительных действий и несанкционированного доступа к критически важным данным организации.

Поддерживаемые типы активов

- СУБД PostgreSQL — версии 9.0—9.6, 10—18;
- СУБД Microsoft SQL Server — SQL Server 2012, 2014, 2016, 2017, 2019, 2022, 2025;
- Хранилище файлов SMB — файловые хранилища, поддерживающие протоколы SMB v2 и SMB v3, включая DFS;
- СУБД MySQL — версии 5.7, 8.0, 8.4 LTS, 9.x Innovation;
- СУБД Oracle Database — версии 11g, 12c, 18c, 19c, 21c, 23ai, 26ai;
- S3-хранилища — S3-совместимое API, включая Amazon Simple Storage Service (Amazon S3) и S3-совместимые объектные хранилища.

Принцип работы

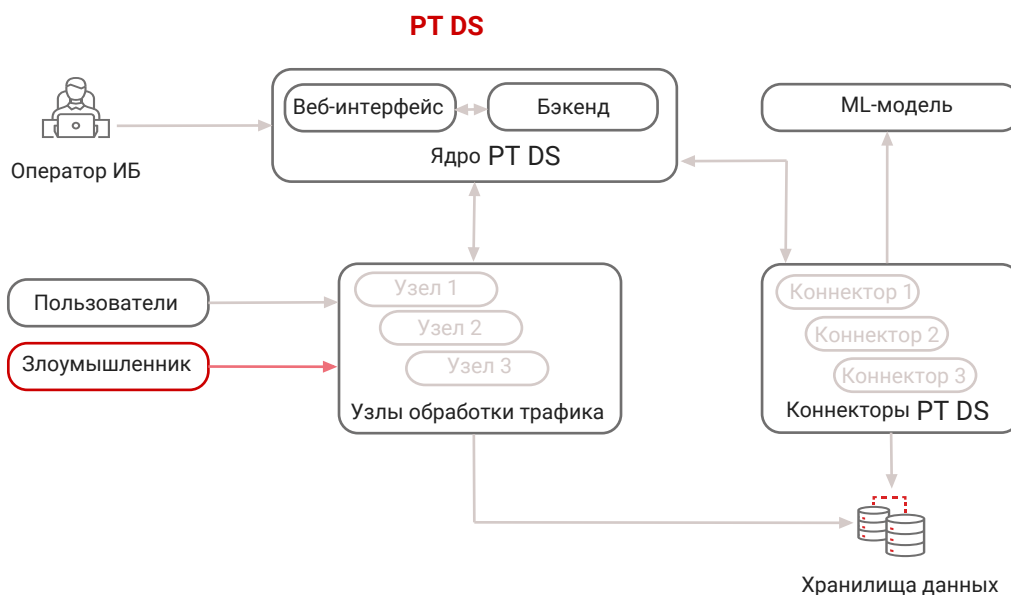


Рисунок 1. Схема взаимодействия компонентов

PT DS работает по следующему принципу:

1. PT DS получает данные о хранилищах данных в инфраструктуре организации.
2. Бэкенд PT DS, используя коннекторы, анализирует структуру хранилищ, выделяет отдельные объекты — структурные единицы хранения данных.
3. Бэкенд PT DS, используя коннекторы, проводит классификацию хранимых данных и определяет критически важные классы, которые необходимо защищать. При этом защищаемые данные на бэкенд не попадают, весь анализ происходит на коннекторах. На этом этапе может использоваться ML-модель в качестве дополнительного механизма классификации данных (не входит в комплект поставки).
4. Администратор с помощью экспертов Positive Technologies загружает политики безопасности в PT DS.
5. Политики безопасности передаются с бэкенда на узлы обработки трафика.
6. Узлы обработки трафика обрабатывают исходящие и входящие запросы к хранилищам данных в соответствии с политикой безопасности, регистрируют доступы к классифицированным данным.
7. Узлы обработки трафика передают информацию об инцидентах и рисках на бэкенд PT DS.
8. Информация об инцидентах и рисках отображается в интерфейсе и доступна пользователю PT DS для анализа.

3. Аппаратные и программные требования

В этом разделе приведены аппаратные и программные требования для установки и работы PT DS.

Требования к виртуальной машине

Для установки PT DS потребуется одна виртуальная машина. Если необходимо, вы можете использовать ML-модель в качестве дополнительного механизма классификации. В этом случае понадобится вторая виртуальная машина. Установка PT DS с ML-моделью возможна на сервере с нагрузкой на центральный процессор или на сервере с видеокартой. Если организация планирует защищать неструктурированные данные больших объемов, рекомендуется выбирать второй вариант (на сервере с видеокартой).

Таблица 2. Минимальные требования к виртуальной машине

Компонент	Минимальные требования
Центральный процессор	8 ядер
Память (ОЗУ)	16 ГБ
Жесткий диск (HDD)	200 ГБ
Сетевой адаптер	1 порт со скоростью 1 Гбит/с

Рекомендуется увеличить объем оперативной памяти до 32 ГБ, если на защищаемых активах размещено большое количество объектов (таблиц, файлов), так как это может увеличивать нагрузку на систему.

Таблица 3. Минимальные требования к виртуальной машине для ML-модели

Компонент	Минимальные требования для сервера с нагрузкой на процессор
Центральный процессор	18 ядер
Память (ОЗУ)	8 ГБ
Жесткий диск (HDD)	100 ГБ
Сетевой адаптер	1 порт со скоростью 1 Гбит/с

Для серверов, использующих видеокарту, требуется видеокарта NVIDIA.

Программные требования

PT DS поддерживает установку на ОС семейства Linux — Debian 12, Astra Linux 1.7.x, 1.8.x и Ubuntu 22.04.

Для работы с интерфейсом PT DS рекомендуется использовать монитор с разрешением 1280 × 800 пикселей и один из следующих браузеров:

- Google Chrome версии 149 и выше;
- Opera версии 130 и выше;
- Safari версии 25 и выше;
- Firefox версии 150 и выше
- Microsoft Edge версии 149 и выше.

4. Лицензирование

Для работы PT DS необходима лицензия. Лицензия фиксирует каждую установку продукта за клиентом и ограничивает возможности продукта параметрами и сроком действия. В этом разделе описано, что такое лицензия, как она работает, как установить лицензию, проверить ее статус.

Лицензия — это разрешение на использование продукта, которое Positive Technologies выдает клиенту. Лицензия привязана к инсталляции продукта и содержит:

- срок действия;
- ограничения по параметрам: максимальное количество контентных объектов и максимальное количество событий на шлюзах обработки трафика в сутки.

Принцип работы

Лицензия привязана к кластеру, на котором развернут продукт. Привязка выполняется по отпечатку инсталляции (фингерпринту) — уникальному идентификатору, который вычисляется по параметрам кластера Kubernetes. Установить лицензию, выпущенную для другой инсталляции, невозможно. В инсталляции может быть установлена только одна лицензия. Установка новой лицензии замещает предыдущую.

Сервис лицензирования периодически сверяет статус лицензии с сервером лицензирования и проверяет, что фактические значения параметров продукта не превышают лимиты, указанные в лицензии. Если сервер лицензирования недоступен, продукт продолжает работать на последнем известном статусе лицензии.

Возможные статусы лицензии

- **Активна** — лицензия активна.
- **Истекает через <N> дней** — срок действия лицензии закончится через указанное количество дней.
- **Превышены лимиты** — превышены лимиты на количество объектов или событий в сутки.
- **Истекла** — срок действия лицензии закончился. Доступны только чтение данных и раздел **Лицензия**.
- **Отозвана** — лицензия отозвана Positive Technologies. Доступны только чтение данных и раздел **Лицензия**. Необходимо обратиться в техническую поддержку.
- **Не установлена** — лицензия не установлена, доступны только чтение данных и раздел **Лицензия**.

При статусах **Не установлена**, **Отозвана** и **Истекла** сервис лицензирования отключает все активные расписания и отменяет запланированные работы. После восстановления лицензии расписания нужно включать вручную.

Предварительные условия

Для установки и удаления лицензии необходимо назначить пользователю роль ds-license. Также необходимо выполнить следующие условия:

- Установить (см. раздел 5) PT DS.
- Назначить IP-адрес или FQDN балансировщику входящего трафика. По этому адресу система вычислит отпечаток инсталляции.

Внимание! Лицензия привязана к кластеру, адресу (домену) точки входа и узлам, указанным в лицензии. Если вы замените кластер, перенесете точку входа на другой адрес или домен либо выведете из кластера узел из лицензии, потребуется перевыпустить лицензию.

- Передать отпечаток инсталляции в техническую поддержку — на его основе будет выпущен ключ или файл лицензии.
- Добавить ключ или файл лицензии в PT DS.

Установка лицензии онлайн

Установка лицензии онлайн происходит с помощью лицензионного ключа.

- ▶ Чтобы установить лицензию по лицензионному ключу:

1. Войдите в PT DS под учетной записью с ролью ds-license.
2. Скопируйте отпечаток инсталляции.
3. Передайте отпечаток в техническую поддержку.
Специалисты технической поддержки выпустят для вас лицензионный ключ.
4. Введите лицензионный ключ, который вы получили в технической поддержке.
5. Нажмите **Активировать**.

После активации на странице **Лицензия** отображаются статус лицензии, ее параметры и срок действия.

Если лицензия уже установлена, повторная установка по ключу замещает текущую лицензию лицензией из нового ключа.

Установка лицензии офлайн

Установка лицензии офлайн происходит с помощью файла, полученного в технической поддержке. Позволяет активировать продукт в закрытом контуре без доступа в интернет.

- ▶ Чтобы установить лицензию из файла:

1. Войдите в PT DS под учетной записью с ролью ds-license.
2. Скопируйте отпечаток инсталляции.

3. Передайте отпечаток пальца в техническую поддержку.

Специалисты технической поддержки выдают вам файл лицензии.

4. Получите от технической поддержки файл лицензии, выпущенный для этой установки.
5. Загрузите файл лицензии в формате ZIP или KEY.
6. Нажмите **Активировать**.

После активации на странице **Лицензия** отображаются статус лицензии, ее параметры и срок действия.

Просмотр статуса лицензии

Просмотр статуса лицензии доступен всем ролям.

- ▶ Чтобы проверить статус лицензии:

1. Войдите в PT DS.
2. Перейдите в раздел **Лицензия**.

В разделе отображаются: статус лицензии, дата окончания, отпечаток пальца (отпечаток установки), лимиты.

5. Развертывание PT DS

PT DS устанавливается на виртуальную машину с помощью установщика из комплекта поставки. [Установить коннекторы \(см. раздел 5.1\)](#) и [узлы обработки трафика \(см. раздел 5.2\)](#) вы можете как вместе с PT DS, так и отдельно — после установки продукта.

Подготовка к развертыванию

Перед установкой необходимо:

1. Установить на виртуальную машину ОС из списка рекомендуемых.
2. Создать учетную запись пользователя, который будет устанавливать PT DS, с правами суперпользователя (root).
3. Настроить следующие доменные имена: для доступа к веб-интерфейсу и сервису авторизации (Open Policy Agent). Если нужен доступ к бета-функциональности, то нужно настроить еще одно доменное имя. Например: fqdn.ds.local, auth-fqdn.ds.local, beta-fqdn.ds.local.
4. Получить у менеджера или партнера Positive Technologies архив `pt_ds_<Номер версии PT DS>.tgz` и распаковать его на локальной машине, откуда будет выполняться установка.

Установка PT DS

► Чтобы установить PT DS:

1. Откройте каталог с установочным комплектом.
2. Откройте на редактирование файл `my_vars.env`.
3. Укажите в файле следующие параметры:
 - `export USER` — логин пользователя для подключения к узлу, на который устанавливается PT DS.
 - `export FQDN` — FQDN узла, на который устанавливается PT DS. Используется для доступа к веб-интерфейсу.
 - `export AUTH_FQDN` — FQDN узла, на который устанавливается PT DS. Используется сервисом авторизации.
 - `export IP` — IP-адрес узла, на который устанавливается PT DS.
 - `EXTERNAL_CONNECTORS` — `true` (если необходимо установить коннекторы отдельно); `false` (если нужно установить коннекторы вместе с PT DS).
 - `export EXTERNAL_PGGW` — `true` (если необходимо установить узел обработки трафика отдельно); `false` (если нужно установить узел обработки трафика вместе с PT DS).
 - `export TLS_CERT`, `export TLS_KEY` — TLS-сертификат и ключ для Ingress-ресурсов, в формате BASE64. При значении `null` создается самоподписанный сертификат.

Пример указания параметров в файле `my_vars.env` (коннекторы и узел обработки трафика устанавливаются вместе с PT DS):

```
export USER=root
export FQDN=fqdn.ds.local
export AUTH_FQDN=auth-fqdn.ds.local
export IP=192.0.2.11
EXTERNAL_CONNECTORS=false
EXTERNAL_PGGW=false
export TLS_CERT=null
export TLS_KEY=null
```

4. Запустите скрипт установки `run.sh` от имени суперпользователя (root).
5. Выберите язык установки и нажмите Enter.
6. Введите пароль для подключения к узлу, на который устанавливается PT DS.
7. Примите условия лицензионного соглашения, нажав клавишу Y.

Начнется установка продукта. Информация о процессе установки записывается в файлы журналов в каталоге `_logs`.

Остановить процесс установки вы можете с помощью комбинации клавиш `Ctrl+C`. Запустить процесс повторно можно командой `/run.sh`.

После завершения установки вы можете войти в PT DS.

В этом разделе

[Установка коннекторов отдельно от PT DS \(см. раздел 5.1\)](#)

[Установка и настройка шлюза обработки трафика \(см. раздел 5.2\)](#)

5.1. Установка коннекторов отдельно от PT DS

Коннекторы — сервисы, предназначенные для работы с конкретным типом хранилища данных, например коннектор `pg` предназначен для работы с СУБД PostgreSQL. Коннекторы используются для анализа данных, при этом защищаемые данные на бэкенд не попадают, весь анализ происходит на коннекторах.

Стандартная установка PT DS вместе с коннекторами подходит для локальных тестовых стендов или небольших контуров. В больших распределенных системах источники данных могут находиться в разных сетевых сегментах, контурах, филиалах. Для использования продукта в таких системах удобнее размещать коннекторы рядом с защищаемыми активами для снижения нагрузки на ядро PT DS. Описание коннекторов приведено в таблице ниже.

► Чтобы установить коннекторы:

1. Установите PT DS, указав параметру `EXTERNAL_CONNECTORS` значение `true` (в файле `my_vars.env`).
2. Перейдите в каталог `external_svc`:
`cd external_svc`
3. Запустите скрипт `external-svc.sh`.

Скрипт соберет в текущий каталог необходимые файлы `docker-compose.yaml`, конфигурации и сертификаты для связи с ядром PT DS.

4. Перенесите каталог `external-svc` на устройство, куда будут устанавливаться коннекторы.
5. Откройте на редактирование файл `/etc/hosts`.

6. Добавьте в него следующие записи:

```
<IP-адрес PT DS> sp-<Доменное имя PT DS>
<IP-адрес PT DS> vault-<Доменное имя PT DS>
<IP-адрес PT DS> valkey-<Доменное имя PT DS>
```

В качестве IP-адреса необходимо указать значение переменной `export IP`, в качестве FQDN — значение переменной `export FQDN` из файла `my_vars.env`.

Например:

```
192.0.2.11 sp-fqdn.ds.local
192.0.2.11 vault-fqdn.ds.local
192.0.2.11 valkey-fqdn.ds.local
```

7. Откройте файл `docker-compose.yaml` и проверьте, что в секции `image` указаны **Название** (Name) и **Тег** (Tag) нужного коннектора.
8. Выполните одно из следующих действий:

- Если вы хотите установить один коннектор, выполните команду:
`docker compose --profile <Название коннектора> up -d`
- Если вы хотите установить несколько коннекторов, выполните команду:
`docker compose --profile <Название коннектора> --profile <Название коннектора> up -d`
- Если вы хотите установить все коннекторы, выполните команду:
`docker compose --profile "*" up -d`

Пример команды для установки коннектора `pg`:

```
docker compose --profile pg up -d
```

Коннекторы установлены. Просмотреть журналы установленного коннектора можно с помощью команды `docker logs <Название коннектора>-connector`.

Соответствие коннекторов типам активов

Таблица 4. Коннекторы PT DS и типы активов

Название в системе	Тип актива
pg	СУБД PostgreSQL
s3	Хранилище объектов MinIO
mssql	СУБД Microsoft SQL Server
mysql	СУБД MySQL
smb	Хранилище файлов SMB
oracle	СУБД Oracle Database

5.2. Установка и настройка шлюза обработки трафика

Шлюз обработки трафика проксирует обращения пользователей к СУБД, применяет правила защиты баз данных и передает информацию об инцидентах в PT DS. Шлюз обработки трафика можно разворачивать отдельно от PT DS. Это позволяет вынести обработку трафика за пределы ядра PT DS и гибко масштабировать инфраструктуру предприятия.

► Чтобы развернуть шлюз обработки трафика отдельно от инсталлятора:

1. В файле `my_vars.env` установите значение переменной `EXTERNAL_PGGW — true`.
2. Запустите установку PT DS.
3. После завершения установки перейдите в каталог `external_svc`.
4. Запустите скрипт `external-svc.sh`.

Скрипт соберет в тот же каталог файл `docker-compose.yaml` и необходимые сертификаты.

5. Перенесите каталог `external_svc` на устройство, на котором будет работать шлюз обработки трафика.
6. Откройте на редактирование файл `/etc/hosts`.
7. Добавьте в файл следующие записи:

```
<IP-адрес PT DS> sec-event-plugin-<FQDN PT DS>
<IP-адрес PT DS> sec-incident-plugin-<FQDN PT DS>
```

В качестве IP-адреса необходимо указать значение переменной `export IP`, в качестве FQDN — значение переменной `export FQDN` из файла `my_vars.env`.

Пример записи:

```
192.0.2.11 sec-incident-plugin-ds.example.com
```

8. Откройте файл `docker-compose.yaml` и проверьте, что в секции `image` указаны **Название** (Name) и **Тег** (Tag) нужного сервиса.

По умолчанию шлюз обработки трафика слушает порт (параметр `LISTEN_PORTS`) 15432 на всех интерфейсах (0.0.0.0). При необходимости это значение можно изменить также в файле `docker-compose.yaml`.

9. В каталоге `external_svc` выполните команду:

```
docker compose --profile pggw up -d
```

Шлюз обработки трафика запущен и готов к работе.

6. Обновление PT DS

► Чтобы обновить PT DS:

1. Получите у менеджера или партнера Positive Technologies архив с новой версией PT DS и распакуйте его.
2. Откройте каталог с установочным комплектом.
3. Откройте на редактирование файл `my_vars.env`.
4. Укажите в файле все параметры, приведенные в инструкции по установке в разделе Установка PT DS в пункте 3.
5. Запустите сценарий обновления `run.sh` от имени суперпользователя (`root`).
6. Выберите язык установки и нажмите Enter.

Начнется обновление продукта. Информация о процессе обновления записывается в файлы журналов в каталоге `_logs`.

7. Настройка доступов пользователей и аутентификация в PT DS

Аутентификация пользователей в PT DS выполняется через SSO-систему Keycloak по протоколу OpenID Connect. Такой способ аутентификации и авторизации позволяет не хранить учетные данные пользователей в PT DS, а получать их из Keycloak.

Первый вход без предварительно установленной Keycloak

Если на вашем предприятии не используется система Keycloak, то в процессе установки PT DS она будет автоматически развернута, а также созданы:

- стандартная учетная запись Keycloak с правами администратора (`admin`);
- изолированное пространство (`realm`) — `datasec` и все необходимые роли для работы с PT DS;
- приложение (`client`) — `datasec-client`;
- пользователь `ds_admin` с паролем `superadmin`.

При первом входе в PT DS вы будете перенаправлены в Keycloak для ввода учетных данных. Вам нужно ввести логин — `ds_admin`, пароль — `superadmin`. Сразу после первого входа необходимо сменить этот пароль в консоли администратора Keycloak. Пароль должен содержать не менее 12 символов, включая буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы. Вы также можете добавить нужные учетные записи и их роли (вкладка **Users** в Keycloak).

Вход с установленной системой Keycloak

Если вы уже используете Keycloak для управления учетными записями на предприятии, то необходимо:

- создать изолированное пространство (`realm`) и приложение (`client`);
- создать учетные записи пользователей (`users`);
- назначить пользователям следующие роли (`realm roles`):
 - `ds-read` — для доступа к запросам чтения данных PT DS;
 - `ds-write` — для создания и удаления сущностей PT DS с помощью веб-интерфейса;
 - `ds-expertise` — для работы с экспертизой PT DS (загрузка классов данных);
 - `ds-resolve-security` — требуется для работы с рисками инцидентами;
 - `ds-start-work` — для запуска задач в PT DS;
 - `ds-stop-work` — для остановки задач PT DS;
 - `ds-work-with-classes` — для работы с классами объектов;

- `ds-work-with-config` — для тонкой настройки сервисов PT DS.
- `ds-license` — для выпуска лицензии.

Подробная информация о Keycloak, инструкции по развертыванию, созданию изолированных пространств, приложений и настройке учетных записей приведены на сайте keycloak.org/documentation.

8. Удаление PT DS

► Чтобы удалить PT DS:

1. Перейдите в каталог с установочным комплектом:
2. Выполните команду:

```
./run.sh --uninstall
```

Начнется удаление PT DS.



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.