Data Security версия 0.10

Руководство пользователя

Дата редакции документа: 05.09.2025

Содержание

1. Обзор PT Data Security

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 зловредные 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.

Принцип работы

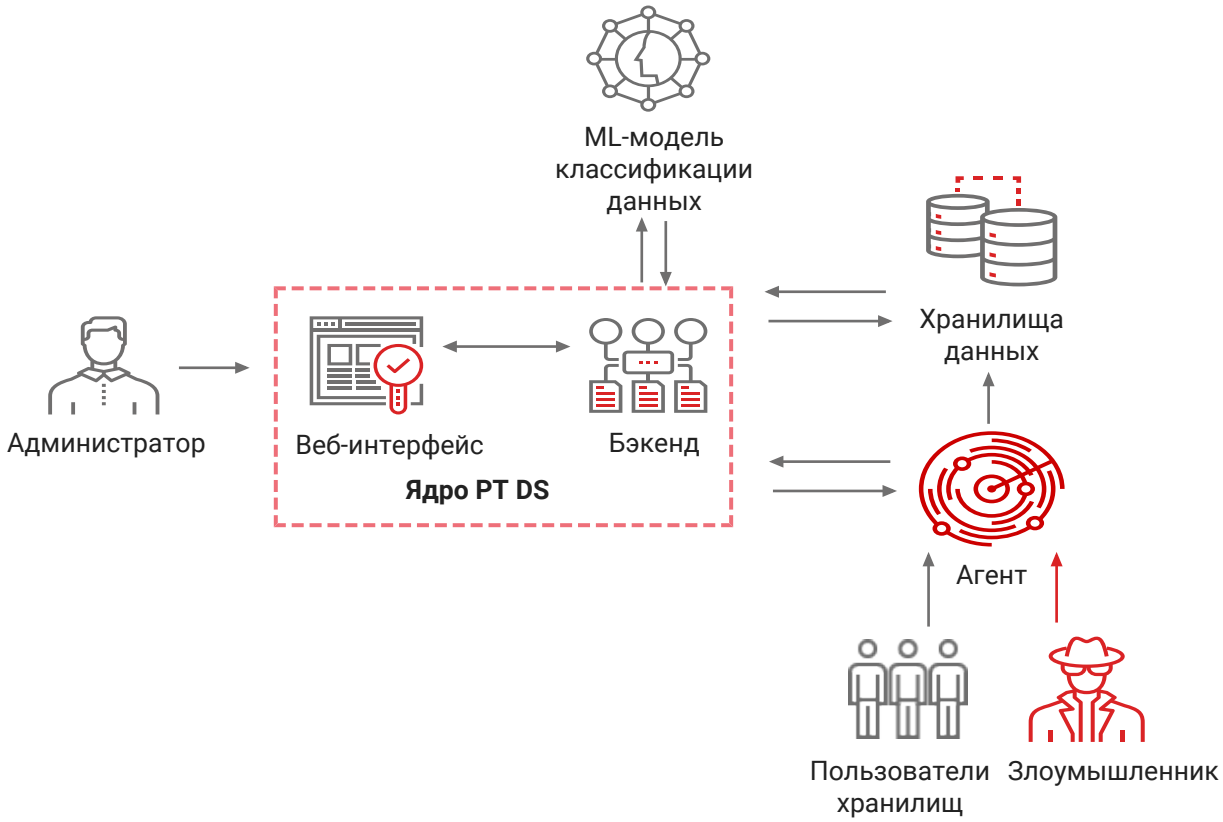

Рисунок 1. Схема взаимодействия компонентов

PT DS работает по следующему принципу:

1. PT DS получает данные о хранилищах данных в инфраструктуре организации.
2. Бэкенд PT DS анализирует структуру хранилищ, выделяет отдельные объекты — структурные единицы хранения данных.
3. Бэкенд PT DS проводит классификацию хранимых данных и определяет критически важные классы, которые необходимо защищать. На этом этапе может использоваться ML-модель классификации данных.
4. Администратор системы настраивает политики безопасности в интерфейсе PT DS.
5. Политики безопасности передаются с бэкенда на агент.
6. Агент обрабатывает исходящие и входящие запросы к БД в соответствии с политикой безопасности, регистрирует доступы к классифицированным данным.
7. Агент передает 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.

2. 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 две виртуальные машины: для установки продукта и для ML-модели. 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 1. Минимальные требования к виртуальной машине

Компонент	**Минимальные требования**
Центральный процессор	4 ядра
Память (ОЗУ)	16 ГБ
Жесткий диск (HDD)	100 ГБ
Сетевой адаптер	1 порт со скоростью 1 Гбит/с

Таблица 2. Минимальные требования к виртуальной машине для ML-модели

Компонент	**Минимальные требования для сервера с нагрузкой на процессор**	**Минимальные требования для сервера с видеокартой**
Центральный процессор	17 ядер	2 ядра
Память (ОЗУ)	5 ГБ	3 ГБ
Оперативная память видеокарты	—	6 ГБ (рекомендуемый производитель — NVIDIA)
Жесткий диск (HDD)	100 ГБ	
Сетевой адаптер	1 порт со скоростью 1 Гбит/с	

Программные требования

PT DS поддерживает установку на ОС семейства Linux — Debian 12, Astra Linux 1.7.7 и Ubuntu 22.04.

3. Начало работы с PT DS

Выполните описанные ниже шаги, чтобы начать защищать данные вашей организации.

Шаг 1. Вход в PT DS

Вход в PT DS осуществляется с помощью браузера по ссылке вида <Доменное имя узла, на который установлен PT DS> ptsecurity.ru/system/assets. Для входа в PT DS вам понадобятся логин и пароль, которые вы можете получить у представителя компании-интегратора или менеджера Positive Technologies.

Шаг 2. Добавление активов в систему

Чтобы защитить данные, которые хранит и обрабатывает организация, следить за ними, проверять правомерность доступа к данным, необходимо добавить в систему активы организации. Для этого необходимо перейти на страницу **Система** и добавить активы (см. раздел 6).

Шаг 3. Классификация данных

Классификация данных происходит автоматически во время интроспекции. Если необходимо, вы можете классифицировать данные вручную (см. раздел 8) на странице **Классификация** или в карточке актива с помощью кнопки **Классифицировать данные**.

4. Вход в PT DS

- Чтобы войти в PT DS:

  1. В адресной строке браузера введите ссылку для входа в интерфейс PT DS.
  2. Введите логин и пароль.

5. Интерфейс PT DS

В этом разделе приводится описание основных элементов пользовательского интерфейса, доступных после входа в PT DS.

После входа в веб-интерфейс по умолчанию открывается страница **Инфраструктура и объект**ы. Веб-интерфейс PT DS состоит из главного меню и рабочей области. Главное меню содержит разделы для перехода к страницам продукта, а также кнопку выхода из системы .

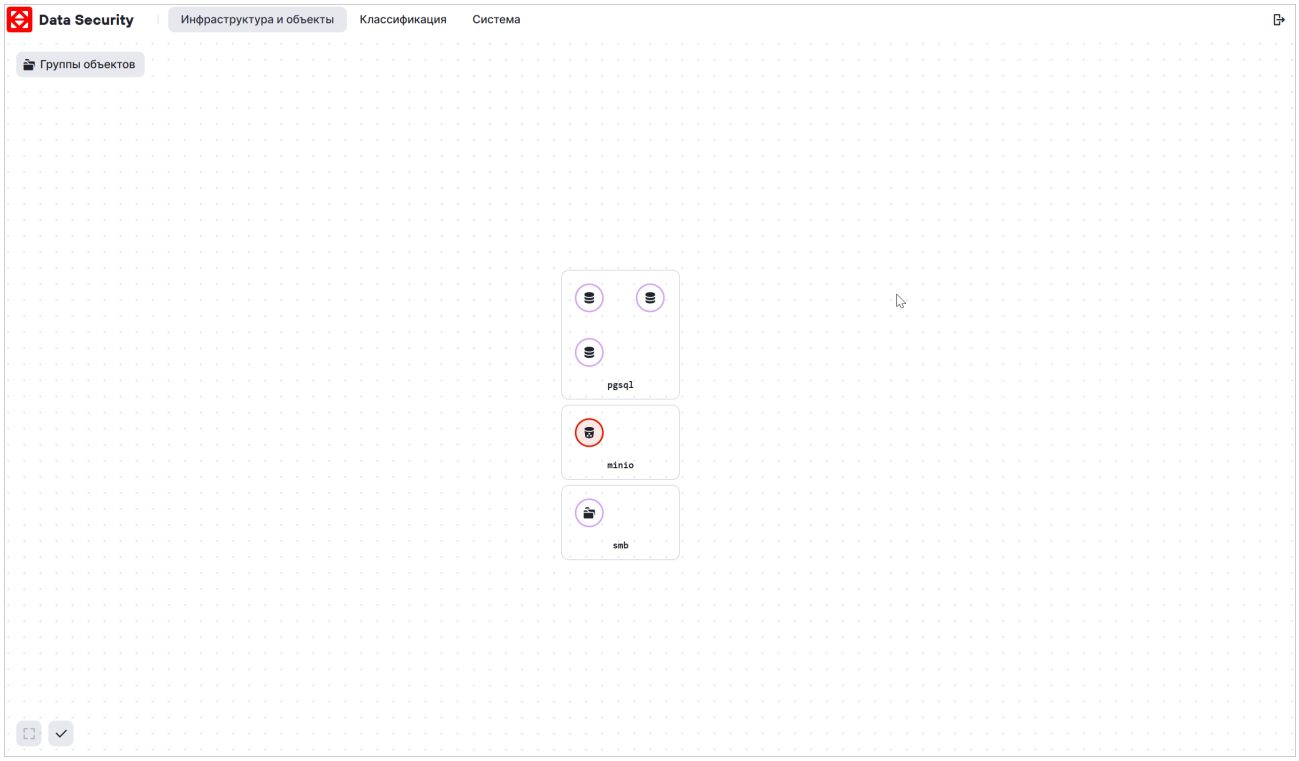

Рисунок 2. Страница **Инфраструктура и объекты**

6. Добавление активов в систему и запуск интроспекции

Вы можете добавлять активы в систему с помощью CSV-файла или вручную. Шаблон файла для импорта можно скачать на странице **Система** → **Добавить активы** → **Импортировать**.

Добавление активов с помощью CSV-файла

Добавлять активы в систему с помощью файла удобно, когда нужно добавить большое количество активов. В файле нельзя указать данные для аутентификации на активе, поэтому после добавления их нужно указать вручную в веб-интерфейсе.

- Чтобы добавить активы с помощью файла:

  1. Перейдите на страницу **Система**.
  2. Нажмите кнопку **Добавить активы** и выберите **Импортировать**.
  3. Перетащите заранее подготовленный CSV-файл с активами в область загрузки или нажмите на ссылку **выберите**.

     PT DS обработает файл и покажет количество распознанных и нераспознанных активов.
  4. Нажмите **Далее**.
  5. Выберите активы, за которыми вы хотите наблюдать, — они будут добавлены в PT DS.

     На этом этапе вы также можете добавить актив вручную, если его нет в файле.
  6. Нажмите **Добавить активы**.

     Добавленные активы отобразятся на вкладке **Система** → **Активы в инфраструктуре**.
  7. В каждом добавленном активе заполните блок параметров **Аутентификация на активе** и сохраните изменения.
  8. Выберите добавленные активы и нажмите **Запустить интроспекцию**.

     Во время интроспекции PT DS анализирует структуру активов, находит элементы, содержащие данные (например, таблицы в БД или файлы в S3-бакете) и классифицирует их.

     По окончании процесса статус актива сменится с **В процессе** на **Проведена**.

  После того как интроспекция окончена вы может просмотреть информацию об активах и объектах, хранящихся в них, на странице **Инфраструктура и объекты**.

Добавление актива вручную

- Чтобы добавить актив в PT DS вручную:

  1. Перейдите на страницу **Система**.
  2. Нажмите кнопку **Добавить активы** и выберите пункт + Добавить вручную.
  3. Укажите параметры для подключения актива в блоке **Сетевые параметры**.
  4. Укажите данные для аутентификации в блоке **Аутентификация на активе**.
  5. Если необходимо, укажите дополнительную информацию.

     Добавленный актив отобразится на вкладке **Система** → **Активы в инфраструктуре**.
  6. Выберите добавленный актив и нажмите **Запустить интроспекцию**.

     По окончании процесса статус актива сменится с **В процессе** на **Проведена**.

7. Инвентаризация и просмотр информации об активах

Инвентаризация в PT DS — это процесс, необходимый для актуализации защищаемых активов и объектов, входящих в их состав. Инвентаризация состоит из двух этапов: добавления активов в систему (см. раздел 6) и интроспекции.

Во время интроспекции анализируется содержимое актива, включая базы данных, и сканируются все объекты внутри этих баз. После завершения интроспекции вы сможете просматривать информацию об активах и объектах, которые размещены в них (например, базах данных или хранилищах данных).

Регулярная интроспекция рекомендуется даже при отсутствии новых активов в системе. Частота запуска зависит от особенностей инфраструктуры предприятия и активности пользователей.

Информацию об активах и объектах можно просматривать на странице **Инфраструктура и объекты**. На странице в графическом виде отображаются активы и хранящиеся в них объекты (значок). При наведении курсора на объект отображается его название и информация о его статусе в системе. При выборе объекта открывается карточка с информацией о нем. Из карточки объекта можно запустить классификацию, если необходимо.

- Чтобы просмотреть информацию об объекте в составе актива:

  1. Перейдите на страницу **Инфраструктура и объекты**.
  2. Выберите нужный объект на схеме.

     Откроется карточка объекта. В ней отображаются данные об активе, в котором расположен объект, общая информация об объекте и структура данных объекта.

Вы можете просматривать информацию о группах объектов в виде списка.

- Чтобы просмотреть информацию о группах объектов:

  1. Перейдите на страницу **Инфраструктура и объекты**.
  2. Нажмите **Группы объектов**.

Вы можете перетаскивать объекты из одной папки списка в другую и группировать объекты как вам удобно. При этом принадлежность объекта определенному активу сохранится.

8. Классификация данных

Посмотреть, как данные распределяются по категориям, и классифицировать данные вы можете на странице **Классификация**.

Для чего нужна классификация

Защита информации. Классификация помогает понять, где хранятся важные файлы, и убедиться, что они находятся в надежном месте.

Безопасность данных. Благодаря классификации можно убедиться, что конфиденциальная информация не хранится в незащищенных местах, где ее могут украсть злоумышленники.

Порядок в системе. Когда все данные распределены по категориям, ими проще управлять и находить нужную информацию.

Как это работает

Классификация — это отнесение объекта к определенному классу данных на основе заданных экспертами Positive Technologies критериев. Например:

- Файлы ИНН будут отнесены к классу «ИНН».
- Электронные письма — к классу «Почтовые сообщения».
- Номера банковских счетов — к классу «Финансовые данные».

► Чтобы запустить классификацию данных:

1. Перейдите на страницу **Классификация**.
2. Нажмите **Классифицировать данные**.

   Начнется процесс классификации данных. Вы можете отслеживать процесс на странице **Инфраструктура и объекты** (значок ✓ в левом нижнем углу).

9. О технической поддержке

Базовая техническая поддержка доступна для всех владельцев действующих лицензий на PT DS 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 технической 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 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 порталу 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.

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения технической 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 технической 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 технической поддержке продукта не включают в себя услуги по переустановке продукта, решение 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 технической 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 3. 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 технической 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

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.