PT Dephaze версия 1.0

Руководство пользователя

Дата редакции документа: 26.02.2025

Содержание

1. Об этом документе

Руководство пользователя содержит пошаговые инструкции и справочную информацию об использовании PT Dephaze. В руководстве описаны ключевые и дополнительные функции PT Dephaze, а также настройка функций для выполнения конкретных задач. Руководство не содержит инструкции по установке, первоначальной настройке и администрированию PT Dephaze.

Руководство адресовано специалистам, использующим PT Dephaze в своей работе.

Комплект документации PT Dephaze включает в себя следующие документы:

— Этот документ.

— Руководство по установке — содержит инструкции по установке и первоначальной настройке продукта.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о PT Dephaze (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 **ОК**	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

Пример	Описание
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT Dephaze

Вы можете найти дополнительную информацию о PT Dephaze 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 10).

2. О PT Dephaze

PT Dephaze — система автоматизированного тестирования на проникновение, предназначенная для оценки защищенности ИТ-инфраструктуры.

С помощью PT Dephaze вы можете запускать пентесты, которые включают различные техники и инструменты злоумышленников (атаки), для оценки защищенности анализируемого сегмента сети.

Ключевые возможности PT Dephaze:

— Создание автоматизированных пентестов.

— Визуализация схемы атаки.

— Согласование или отклонение атак.

— Журналирование действий, выполняемых в процессе тестирования на проникновение.

— Предоставление рекомендаций по устранению уязвимостей, обнаруженных в результате атаки.

— Формирование подробного отчета с результатами тестирования.

3. Вход в PT Dephaze

Перед входом в PT Dephaze получите у администратора системы логин и пароль.

- Чтобы войти в PT Dephaze:

  1. В адресной строке браузера введите ссылку для входа в интерфейс PT Dephaze.
  2. Введите логин и пароль.
  3. Нажмите **Войти**.

4. Интерфейс PT Dephaze

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

Все действия в PT Dephaze вы можете выполнять с помощью веб-интерфейса. Все передаваемые данные при работе с веб-интерфейсом защищаются при помощи HTTPS с использованием SSL-сертификата. Сертификат может быть самоподписанный или выданный официальным центром сертификации.

В этом разделе

4.1. Главное меню

Основным элементом управления в интерфейсе PT Dephaze является главное меню. Главное меню отображается на всех страницах и состоит из следующих кнопок:

 — переход на страницу **Пентесты**;

 — просмотр и управление наборами параметров атакующих действий;

 — просмотр информации о продукте;

Ru или **En** — смена языка интерфейса;

 — смена темы оформления интерфейса;

 — выход из системы.

4.2. Страница «Пентесты»

При входе в PT Dephaze по умолчанию открывается страница **Пентесты**. Вы также можете перейти к ней, нажав в главном меню  .

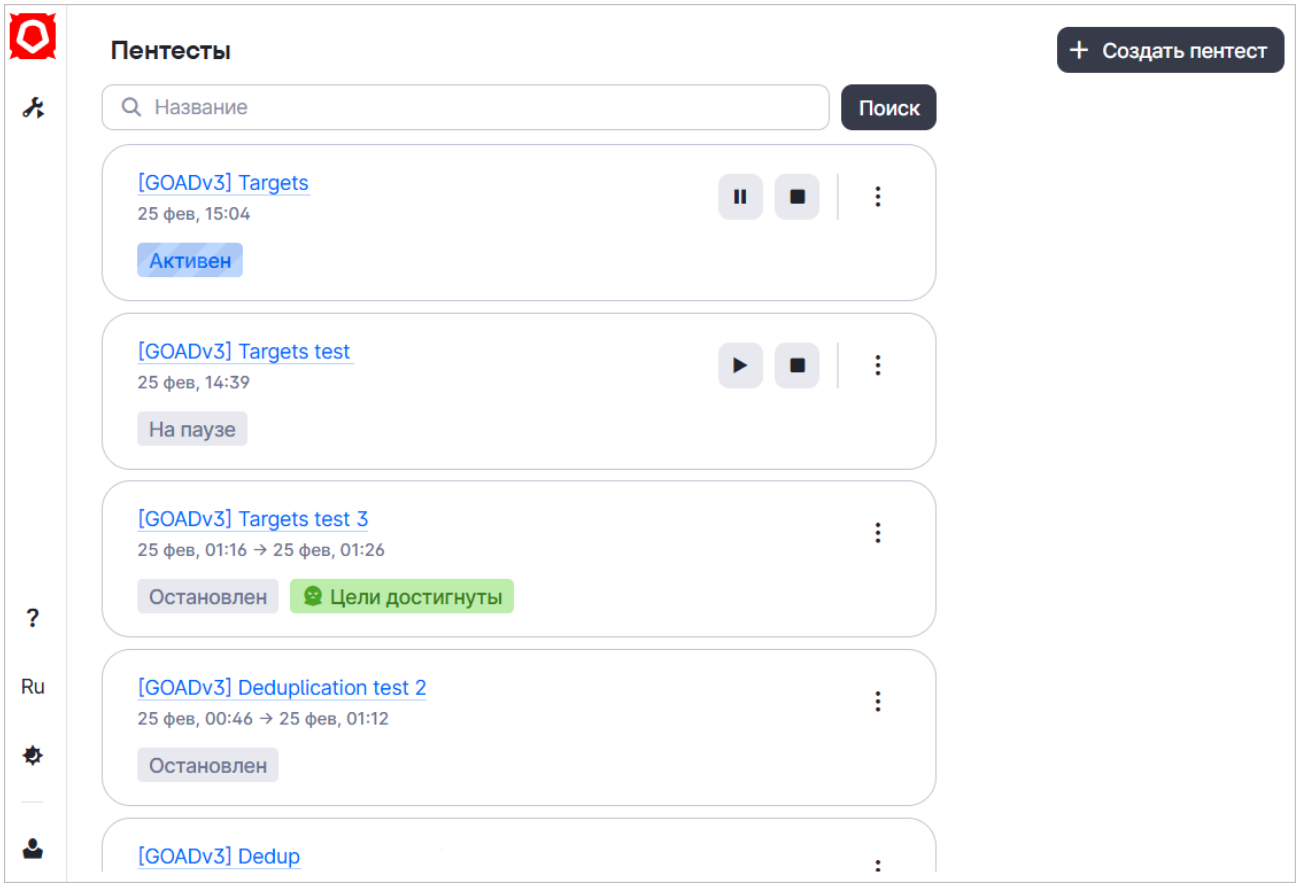

Рисунок 1. Страница **Пентесты**

В рабочей области страницы расположены:

— фильтр для поиска пентеста по названию или его части;

— кнопка **Создать пентест**;

— список карточек пентестов.

Каждая карточка пентеста отображает:

— название;

— дату и время запуска и завершения пентеста;

— статус;

Примечание. Пентест в статусе **Остановлен** недоступен для повторного запуска.

— кнопку ⋮ для просмотра параметров пентеста, создания копии или сохранения отчета с результатами тестирования;

— кнопки для управления состоянием активного пентеста:

⏸ — приостановить тестирование;

— запустить тестирование;

— остановить тестирование.

Примечание. Кнопки управления недоступны для пентестов в статусе **Остановлен**.

4.3. Параметры пентеста

Вы можете просмотреть параметры пентеста с помощью кнопки ⋮ → **Параметры** в карточке пентеста или на странице с информацией о нем (см. раздел 7).

В зависимости от параметров, которые были указаны при создании пентеста, в панели может отображаться следующая информация:

- Название пентеста.
- Дата и время запуска и завершения тестирования.
- Количество выполненных атакующих действий.
- Количество захваченных узлов.
- **Режим согласования** — определяет, какие атакующие действия в процессе тестирования необходимо согласовывать вручную:
  - **Все действия** — все атаки запускаются только после согласования;
  - **Только опасные** — согласования требуют только наиболее опасные атаки;
  - **Без согласования** — все атаки запускаются без согласования.
- **Агент** — название атакующего узла.
- **Сетевой интерфейс** — сетевой интерфейс, через который выполняется атака.
- **Область тестирования** — IP-адрес или диапазон IP-адресов инфраструктуры, в которых выполняется тестирование на проникновение.
- **Исключения** — IP-адрес или диапазон IP-адресов инфраструктуры, которые исключаются из области тестирования.
- **Атакующие действия** — экземпляры запуска определенных атак.
- **Набор параметров атакующих действий** — набор параметров, определяющий стратегию работы атакующих действий.
- **Учетные данные** — учетные данные, которые могут быть использованы для проведения атаки.
- **Цели** — IP-адрес или диапазон IP-адресов инфраструктуры, которые являются целью реализации атаки, а также критерий достижения цели.

4.4. Смена языка интерфейса

Интерфейс PT Dephaze доступен на русском и английском языках.

- Чтобы сменить язык интерфейса,

  в главном меню нажмите **Ru** или **En**.

4.5. Смена темы интерфейса

Интерфейс PT Dephaze доступен в светлой и темной темах, а также вы можете выбрать тему, как в вашей системе.

- Чтобы сменить тему интерфейса,

  в главном меню выберите → **<Название темы>**.

5. Настройка атакующих действий

Наборы параметров атакующих действий определяют стратегию их работы и используются в процессе тестирования на проникновение (например, при подборе учетных данных). Вы можете использовать в пентесте стандартный набор параметров, создать новый набор или создать копию на основе существующего набора.

Стандартный набор недоступен для изменения и удаления.

> **Внимание!** Некорректно заданные значения параметров могут привести к высокой загрузке сетевого канала, отказу в обслуживании тестируемых сервисов и другим непредсказуемым последствиям.

Создание набора

При создании набора в поля автоматически подставляются значения из стандартного набора параметров.

- Чтобы создать набор параметров:

  1. В главном меню нажмите .
  2. Нажмите **Добавить набор параметров**.
  3. Укажите название набора.
  4. Укажите количество параллельных потоков для перечисления учетных записей в Active Directory.
  5. Укажите максимальное количество учетных записей для перечисления в Active Directory.
  6. Укажите количество минут между попытками распыления пароля в Active Directory.
  7. Укажите максимальное количество попыток аутентификации в указанном интервале для распыления пароля.
  8. Укажите порты, которые будут использоваться для сканирования инфраструктуры.
  9. Укажите частоту сканирования.
  10. Укажите количество секунд задержки между созданием дампов памяти процесса LSASS.
  11. Нажмите **Сохранить**.

Создание копии набора

- Чтобы создать копию набора:

  1. В главном меню нажмите  .
  2. В карточке набора нажмите → **Создать копию**.
  3. Если требуется, измените параметры.
  4. Нажмите **Сохранить**.

Изменение параметров набора

Вы можете изменять параметры пользовательских наборов, стандартный набор недоступен для изменения.

- Чтобы изменить параметры набора:

  1. В главном меню нажмите  .
  2. Выберите набор параметров.
  3. Внесите изменения.
  4. Нажмите **Сохранить**.

6. Создание пентеста

Вы можете создать новый пентест или создать копию на основе существующего.

Создание пентеста

- Чтобы создать пентест:

  1. Откройте страницу **Пентесты**.
  2. Нажмите **Создать пентест**.
  3. Введите название пентеста.
  4. Выберите режим согласования.
  5. Выберите агент и сетевой интерфейс.
  6. Укажите область тестирования (IP-адрес в формате IPv4 или в нотации CIDR или диапазон IP-адресов).
  7. Если требуется, укажите исключения из области тестирования (IP-адрес в формате IPv4 или подсеть в нотации CIDR).
  8. Если требуется тонкая настройка пентеста, включите отображение дополнительных параметров.
  9. Выберите атакующие действия.

     Примечание. Если поле **Атакующие действия** оставить пустым, в процессе тестирования по умолчанию будут использованы все доступные действия.

  10. Выберите набор параметров атакующих действий.

      Примечание. Вы можете использовать стандартный набор параметров атакующих действий или создать новый (см. раздел 5).

  11. Добавьте учетные данные.

      Примечание. Вы можете добавлять учетные данные после запуска пентеста на странице с информацией о нем (см. раздел 7.1).

  12. Добавьте цели.
  13. Нажмите **Запустить**.

Создание копии пентеста

- Чтобы создать копию пентеста:

  1. Откройте страницу **Пентесты**.
  2. В карточке пентеста нажмите ⋮ → **Создать копию**.

3. Выберите агент и сетевой интерфейс.
4. Если требуется, измените параметры пентеста.
5. Нажмите **Запустить**.

Вы также можете создать копию пентеста на странице с информацией о нем (см. раздел 7).

7. Просмотр информации о пентесте

► Чтобы просмотреть подробную информацию о пентесте:

1. Откройте страницу **Пентесты**.
2. По ссылке с названием пентеста откройте страницу с информацией о нем.

На странице **Пентесты** → **<Название пентеста>** отображаются следующие элементы:

— Кнопки для управления активным пентестом.

— Кнопка ⋮ для просмотра параметров пентеста (см. раздел 4.3), создания копии (см. раздел 6) и скачивания отчета (см. раздел 9).

— Раздел **Согласование действий** для перехода к странице ручного согласования действий (см. раздел 8).

— Раздел **Журнал активности** для перехода к странице с журналом событий тестирования.

— Раздел **Артефакты** для перехода к странице с информацией о полученных артефактах в результате атаки.

— Схема атаки.

— Панель **Достигнутые цели** отображает количество достигнутых целей.

— Панель **Добавленные учетные данные** содержит количество записей и кнопку › для просмотра и добавления учетных данных.

Схема атаки

На схеме атаки визуально представлены данные атакующего узла и узлов из атакуемых подсетей, а также направление атаки. Атакующий узел отмечен значком красной маски. Значок зеленой маски означает, что узел является целью атаки и эта цель достигнута. Если для узла удалось получить привилегии, он считается захваченным и отмечается красным цветом.

Рядом с IP-адресом узла синим цветом отображается количество действий, требующих согласования (см. раздел 8). Вы можете выбрать узел и просмотреть список успешно завершенных действий, а также список действий, которые требуют согласования.

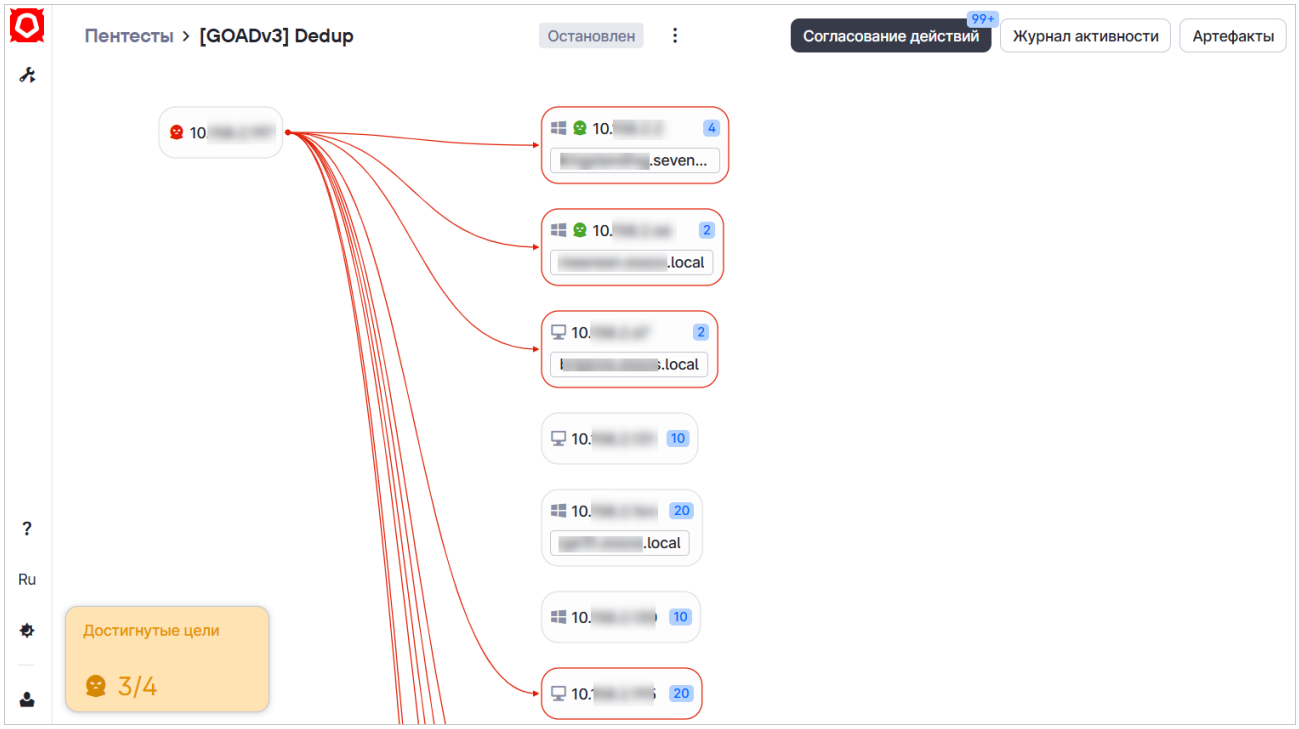

Рисунок 2. Схема атаки

В этом разделе

Добавление учетных данных (см. раздел 7.1)

Просмотр журнала активности (см. раздел 7.2)

Просмотр артефактов (см. раздел 7.3)

7.1. Добавление учетных данных

Вы можете добавить учетные данные в пентест, который находится в статусе **Активный** или **На паузе**.

- Чтобы добавить учетные данные в активный пентест:

  1. Откройте страницу **Пентесты**.
  2. По ссылке с названием пентеста откройте страницу с информацией о нем.
  3. В панели **Добавленные учетные данные** нажмите > .
  4. Нажмите **Добавить запись**.
  5. Укажите учетные данные.
  6. Нажмите ✓.

7.2. Просмотр журнала активности

Вы можете просмотреть в журнале активности все действия, которые были выполнены на атакуемых узлах в процессе тестирования. Для каждого действия отображаются дата и время запуска и завершения, название, IP-адрес атакуемого узла, агент атаки и статус.

- Чтобы просмотреть журнал активности:

  1. Откройте страницу **Пентесты**.
  2. По ссылке с названием пентеста откройте страницу с информацией о нем.
  3. Нажмите **Журнал активности**.

7.3. Просмотр артефактов

- Чтобы просмотреть полученные в процессе тестирования артефакты:

  1. Откройте страницу **Пентесты**.
  2. По ссылке с названием пентеста откройте страницу с информацией о нем.
  3. Нажмите **Артефакты**.

8. Согласование и отклонение действий

Если в пентесте выбран режим согласования **Все действия**, каждое атакующее действие необходимо согласовывать вручную.

В режиме согласования **Только опасные** атакующие действия, которые эксперты Positive Technologies оценивают как наиболее опасные, будут приостановлены до момента их согласования. Остальные действия продолжат выполняться.

В режиме **Без согласования** все действия выполняются без ручного согласования.

Вы можете просмотреть атакующие действия, которые требуют согласования, на странице с информацией о пентесте (см. раздел 7) с помощью кнопки **Согласование действий** или на схеме атаки выбрать узел и вкладку **Согласование действий**.

> **Внимание!** Атакующие действия, которые были отклонены на определенном узле, не будут отправляться повторно на согласование и по умолчанию не будут выполняться в текущем пентесте.

- Чтобы согласовать или отклонить действия на странице с информацией о пентесте:

  1. Откройте страницу **Пентесты**.
  2. По ссылке с названием пентеста откройте страницу с информацией о нем.
  3. Нажмите **Согласование действий**.
  4. Выберите действия, которые вы хотите согласовать.

     Примечание. Вы можете воспользоваться поиском по названию атакующего действия, потенциальной угрозе или атакуемому IP-адресу.
  5. Если требуется, укажите комментарий и нажмите **Подтвердить**.
  6. Нажмите **Согласовать** или **Отклонить**.

9. Скачивание отчета с результатами тестирования

Отчет с результатами тестирования содержит общую информацию о пентесте, оценку защищенности инфраструктуры, список реализованных атак, подробное описание этапов атаки, а также рекомендации по устранению обнаруженных уязвимостей.

- Чтобы просмотреть и скачать отчет с результатами тестирования:

  1. Откройте страницу **Пентесты**.
  2. В карточке пентеста нажмите ⋮ → **Скачать отчет**.

     PDF-файл с отчетом откроется в новой вкладке браузера. Вы можете сохранить его с помощью инструментов браузера.

Вы также можете скачать отчет с помощью кнопки ⋮ → **Скачать отчет** на странице с информацией о нем (см. раздел 7).

10. Техническая поддержка

Базовая техническая поддержка доступна для всех владельцев действующих лицензий на продукты Positive Technologies в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продуктов

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продуктов 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 продуктов.

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 продуктов в рамках выпуска обновленных версий продукта

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 2. 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.