Positive Technologies Threat Intelligence Feeds

Версия 1.4

Руководство пользователя

POSITIVE TECHNOLOGIES

Дата редакции документа: 06.09.2022

Содержание

1. Об этом документе

Руководство пользователя содержит инструкции и справочную информацию об установке, первоначальной настройке, обновлении и удалении Positive Technologies Threat Intelligence Feeds (далее также — PT Feeds). Руководство также содержит инструкции по настройке источников для получения внешних данных.

Руководство адресовано специалистам, выполняющим установку и администрирование PT Feeds в организации.

В этом разделе

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 кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT Feeds

Вы можете найти дополнительную информацию о PT Feeds 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 15).

2. О PT Feeds

Positive Technologies Threat Intelligence Feeds (далее также — PT Feeds) обеспечивает доставку данных об угрозах информационной безопасности и индикаторах компрометации (фидов), специфичных для отдельной организации в данный момент времени. Индикаторы компрометации — это артефакты, наблюдаемые в сети или в операционной системе и указывающие на вредоносную активность в инфраструктуре.

3. Функциональные возможности PT Feeds

PT Feeds выполняет следующие функции:

- получение индикаторов компрометации из коммерческих и публичных источников;
- формирование на основе полученных данных выходных репутационных списков;
- удаление повторяющихся индикаторов компрометации в репутационных списках;
- отслеживание устаревших индикаторов компрометации;
- распространение индикаторов компрометации на средства защиты информации.

4. Аппаратные и программные требования

Данный раздел содержит требования к аппаратному и программному обеспечению, необходимые для установки и работы PT Feeds.

Таблица 2. Аппаратные и программные требования к PT Feeds

Компонент	Минимальные требования
Центральный процессор	4 ядра
Память (ОЗУ)	4 ГБ
Свободное дисковое пространство	200 ГБ
Операционная система	Debian версии 9 или 10 Ubuntu 16.04 LTS

Для работы PT Feeds в операционной системе должны быть установлены следующие компоненты:

- Docker CE версии 20 или выше.
- Docker Compose версии 1.28 или выше.

Также при установке PT Feeds автоматически устанавливается СУБД PostgreSQL.

5. Установка

Примечание. Для корректной работы с PT Feeds пользователь, от имени которого выполняется установка, должен состоять в группах docker и sudo.

- Чтобы установить PT Feeds:

  1. Убедитесь, что порты 2080/TCP и 2443/TCP не используются приложениями.
  2. Перейдите в каталог с deb-пакетом PT Feeds:
     `cd <Имя каталога>`
  3. Запустите установку deb-пакета PT Feeds:
     - Если deb-пакет с Docker CE уже установлен:
       `sudo apt install ./cybsi-lite-offline.1.4.deb`
     - Если вместе с deb-пакетом PT Feeds вы хотите установить deb-пакет с Docker CE:
       `dpkg -i *.deb`

       Примечание. Для установки PT Feeds в Debian 10 необходимо помимо основного deb-пакета с PT Feeds установить в тот же каталог два дополнительных пакета: docker-ce_18.06.0~ce~3-0~debian_amd64.deb и libltdl7_2.4.6-9_amd64.deb. Для установки этих deb-пакетов нужно выполнить команду `dpkg -EGi <path>/*.deb`, где `path` — путь к каталогу с тремя deb-пакетами.
  4. Выполните команду `docker ps` для проверки установленных Docker-контейнеров.

     Если установка прошла успешно, отобразятся два запущенных контейнера `cybsi/cybsi-lite` и `postgres`.

6. Запуск и остановка PT Feeds

Вы можете запускать и останавливать PT Feeds вручную.

- Чтобы запустить приложение:
  1. Перейдите в каталог `/opt/pt/cybsi-lite`.
  2. Выполните команду:
     - Если нужно запускать приложение из консоли:
       ```
       docker-compose up
       ```
     - Если нужно запускать приложение с помощью Docker Daemon:
       ```
       docker-compose up -d
       ```
- Чтобы остановить приложение:
  1. Перейдите в каталог `/opt/pt/cybsi-lite`.
  2. Выполните команду:
     ```
     docker-compose down --remove-orphans
     ```

7. Удаление

- Чтобы удалить все данные и Docker-образы PT Feeds,

  выполните команду:

  ```
  sudo apt remove cybsi-lite
  ```

8. Обновление

Вы можете обновлять PT Feeds как с предыдущей версии, так и в рамках текущей версии, сценарии обновления при этом не различаются.

- Чтобы обновить PT Feeds:

  1. Перейдите в каталог с deb-пакетом PT Feeds:
     ```
     cd <Имя каталога>
     ```
  2. Остановите приложение:
     ```
     docker-compose down
     ```
  3. Запустите установку deb-пакета:
     ```
     sudo apt install ./cybsi-lite-offline.1.4.deb
     ```

  PT Feeds обновлен.

9. Принцип работы

PT Feeds получает внешние данные (фиды) из разных источников (см. раздел 10). На основе фидов PT Feeds регистрирует индикаторы компрометации трех видов: mask (домены и URL), ip и hash. Для каждого индикатора создаются события: create (индикатор зарегистрирован), update (индикатор изменен), delete (индикатор удален).

В конфигурационном файле `config.yml`, который находится в каталоге `/opt/pt/cybsi-lite/app`, вы можете настроить срок актуальности индикаторов компрометации (параметры `masks_ttl` и `ips_ttl`). По истечении этого срока PT Feeds сгенерирует событие delete и удалит индикатор (кроме индикаторов hash, которые актуальны всегда).

10. Настройка получения фидов

PT Feeds поддерживает пять источников данных об угрозах информационной безопасности и индикаторах компрометации. После установки PT Feeds необходимо настроить получение фидов только от одного источника.

В этом разделе

10.1. Настройка получения фидов от репутационного сервиса компании «Лаборатория Касперского»

Для выполнения настройки необходима лицензия на репутационный сервис компании «Лаборатория Касперского» (подробнее на сайте kaspersky.ru). PT Feeds поддерживает интеграцию со следующими фидами:

- Malicious URL Data Feed;
- Ransomware URL Data Feed;
- Phishing URL Data Feed;
- Botnet C&C URL Data Feed;
- IP Reputation Data Feed;
- Malicious Hash Data Feed;
- Mobile Botnet C&C URL Data Feed.

► Чтобы настроить получение фидов от репутационного сервиса компании «Лаборатория Касперского»:

1. Разместите файл `kaspersky.pfx` в каталоге `/opt/pt/cybsi-lite/app/`.
2. В файле `/opt/pt/cybsi-lite/app/config.yml` измените значение параметра `kaspersky` → `enable`:
   ```
   enable: true
   ```
3. Если требуется, измените URL для доступа к фидам репутационного сервиса.

4. В качестве значения параметра `kaspersky` → `pfx_pass` укажите пароль от файла `kaspersky.pfx`.
5. Перезапустите PT Feeds:
   ```
   docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml down
   docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml up -d
   ```

Получение фидов от репутационного сервиса компании «Лаборатория Касперского» настроено.

10.2. Настройка получения фидов от репутационного сервиса компании Group-IB

Для выполнения настройки необходима лицензия на репутационный сервис компании Group-IB (подробнее на сайте group-ib.ru).

- Чтобы настроить получение фидов от репутационного сервиса компании Group-IB:

1. В файле `/opt/pt/cybsi-lite/app/config.yml` измените значение параметра `group-ib` → `enable`:
   ```
   enable: true
   ```
2. Если требуется, измените URL для доступа к фидам репутационного сервиса.
3. В качестве значений параметров `group-ib` → `login` и `group-ib` → `password` укажите логин и пароль для доступа к фидам репутационного сервиса.
4. Перезапустите PT Feeds:
   ```
   docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml down
   docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml up -d
   ```

Получение фидов от репутационного сервиса компании Group-IB настроено.

10.3. Настройка получения фидов от репутационного сервиса MISP Threat Sharing

- Чтобы настроить получение фидов от репутационного сервиса MISP Threat Sharing:

1. В файле `/opt/pt/cybsi-lite/app/config.yml` измените значение параметра `misp` → `enable`:
   ```
   enable: true
   ```
2. Измените значение параметра `misp` → `feeds_urls`:
   ```
   feeds_urls: http(s)://<misp-host>/<feed-url>
   ```
   где `feed-url` — относительный URL фида в MISP Threat Sharing.

Например, `https://www.circl.lu/doc/misp/feed-osint;http://www.botvrij.eu/data/feed-osint`.

3. Перезапустите PT Feeds:
   ```
   docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml down
   docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml up -d
   ```

Получение фидов от репутационного сервиса MISP Threat Sharing настроено.

10.4. Настройка получения фидов от репутационного сервиса PT CybSI

- Чтобы настроить получение фидов от репутационного сервиса PT CybSI:

1. В файле `/opt/pt/cybsi-lite/app/config.yml` измените значение параметра `cybsi → enable`:
   ```
   enable: true
   ```
2. Если вы выполняете обновление PT Feeds с предыдущей версии, укажите значение параметра `cybsi → feeds_urls`:
   ```
   feeds_urls: http(s)://<cybsi-host>/<feed-path>
   ```
   где `feed-path` — относительный URL фида в PT CybSI.

   Примечание. Для получения всех фидов от PT CybSI нужно указать следующие URL: https://cybsi.ptsecurity.com/api/feeds/long-lived-ips/1/json;https://cybsi.ptsecurity.com/api/feeds/long-lived-domains/1/json;https://cybsi.ptsecurity.com/api/feeds/long-lived-urls/1/json;https://cybsi.ptsecurity.com/api/feeds/long-lived-hashes/1/json;https://cybsi.ptsecurity.com/api/feeds/short-lived-ips/1/json;https://cybsi.ptsecurity.com/api/feeds/short-lived-domains/1/json;https://cybsi.ptsecurity.com/api/feeds/short-lived-urls/1/json;https://cybsi.ptsecurity.com/api/feeds/short-lived-hashes/1/json.
3. Измените значение параметра `cybsi → auth_url`:
   ```
   auth_url: https://<cybsi-host>/auth/token
   ```
4. Если для доступа к фидам вы используете локальный экземпляр PT CybSI, в качестве значения параметра `cybsi.api_key` укажите ключ API для подключения к PT CybSI.
5. Если вы подключаетесь к публичным фидам Positive Technologies, измените значение параметра `cybsi → flus`:
   ```
   enable: true
   ```
6. В качестве значения параметра `cybsi → cybsi.flus.licence_token` укажите содержимое лицензионного ключа PT CybSI.

Примечание. В этом случае в качестве `<cybsi-host>` используйте адрес `cybsi.ptsecurity.com`.

7. Перезапустите PT Feeds:
   ```
   docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml down
   docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml up -d
   ```

Получение фидов от репутационного сервиса PT CybSI настроено.

10.5. Настройка получения фидов в формате STIX 2.0

- Чтобы настроить получение фидов в формате STIX 2.0 по протоколу TAXII:

  1. В файле `/opt/pt/cybsi-lite/app/config.yml` измените значение параметра `taxii2 → enable`:
     ```
     enable: true
     ```
  2. В качестве значений параметров `taxii2→ login` и `taxii2 → password` укажите логин и пароль для доступа к коллекции фидов.
  3. Если требуется, измените URL для доступа к коллекции фидов (параметр `collection_urls`).
  4. Если требуется, измените URL TAXII-сервера (параметр `discovery_url`).
  5. Перезапустите PT Feeds:
     ```
     docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml down
     docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml up -d
     ```

  Получение фидов в формате STIX 2.0 настроено.

11. Получение фидов

Вы можете настроить получение фидов с помощью запроса к REST API PT Feeds.

Метод и URL запроса:

`GET <Корневой URL API>/api/reputationLists`

URL запроса может содержать параметры строки, описанные в таблице ниже.

Таблица 3. Параметры строки запроса на получение фидов

Параметр	Обязательный	Тип (формат)	Описание
`token`	Нет	Integer	Параметр для перехода на следующую страницу списка. Нужно указать значение из параметра `lastToken`, полученное в предыдущем запросе
`limit`	Нет	Integer	Количество событий фида, отображаемых на одной странице (0;10 000]

Ответ на запрос

В ответ на успешный запрос сервис возвращает фид. Тело ответного сообщения может содержать поля, описанные в таблице ниже. HTTP-статус `204 NoContent` вместо `200 OK` означает, что достигнут конец фида.

Таблица 4. Схема ответа на запрос на получение фидов

Поле	Тип (формат)	Описание
`items`	Array of objects	Список событий фида
`items` → `id`	String (UUID)	Идентификатор фида
`items` → `object`	Object	Упоминаемый индикатор компрометации
`items` → `object` → `type`	String	Тип индикатора. Возможные значения: `hash`, `ip`, `mask`
`items` → `object` → `hash`	Object	Ключевые атрибуты индикатора `hash`
`items` → `object` → `hash` → `sha256`	String	Хеш-сумма SHA-256
`items` → `object` → `hash` → `sha1`	String	Хеш-сумма SHA-1
`items` → `object` → `hash` → `md5`	String	Хеш-сумма MD5

Поле	Тип (формат)	Описание
items → object → ip	String (byte)	IP-адрес. Только для индикатора ip
items → object → mask	String	Домен или URL. Только для индикатора mask
items → object → threatType	String	Типы атак
items → object → firstSeen	String (date-time)	Дата и время первого упоминания об индикаторе
items → object → lastSeen	String (date-time)	Дата и время последнего упоминания об индикаторе
items → object → score	Integer	Репутация индикатора на момент выгрузки. От 0 до 100, где 100 — вредоносный, 0 — безопасный
items → object → labels	Array of strings	Список меток
items → object → sources	Array of strings	Список источников
items → object → noderoles	Array of strings	Список ролей узла в сети. Только для индикаторов mask и ip
items → object → malwareFamilies	Array of objects	Список семейств ВПО. Может принимать значение null
items → object → malwareFamilies → name	String	Название семейства ВПО
object → malwareFamilies → aliases	Array of strings	Список синонимов семейства ВПО
items → object → malwareFamilies → description	String	Описание семейства ВПО
items → object → description	String	Описание индикатора

Поле	Тип (формат)	Описание
items → object → hostMatch	String	Предикат для сравнения с FQDN. Только для индикаторов mask фидов Group-IB и "Лаборатории Касперского". Возможные значения: h:dAS, h:dEX
items → object → URLMatch	String	Предикат для сравнения с URL. Только для индикаторов mask фидов Group-IB и "Лаборатории Касперского". Возможные значения: u:hAS, u:hEX, u:hEXdEX, u:hAS,pEX, u:hAS, dAS, u:hAS, pSW, u:hAS, pTM
items → status	String	Статус события (первичный импорт индикатора или его обновление). Возможные значения: create, update, delete
lastToken	Integer	Токен для перехода на следующую страницу списка событий. Нужно указать его значение в следующем запросе в параметре token

Пример

Запрос:

```
GET https://cybsi.ptsecurity.ru/api/reputationLists?limit=2&token=218280
```

Ответ:


```
{
  "items": [
    {
      "id": "213dbac9-0eec-4902-9e9f-0f7b0ee81f48",
      "object": {
        "ip": "76.91.1.19",
        "type": "ip",
        "score": 90,
        "labels": [],
        "sources": [
          "taxii2"
        ],
        "lastSeen": "2022-03-23T14:50:59.743Z",
        "firstSeen": "2022-03-23T14:50:59.743Z",
        "nodeRoles": null,
        "threatType": "indicator",
        "description": "Sources: taxii2",
        "malwareFamilies": []
      },
      "status": "create"
    },
    {
```

```
      "id": "13836865-a190-42ca-a690-11041afa0347",
      "object": {
        "ip": "188.166.92.54",
        "type": "ip",
        "score": 90,
        "labels": [],
        "sources": [
          "taxii2"
        ],
        "lastSeen": "2022-03-23T14:51:03.606Z",
        "firstSeen": "2022-03-23T14:51:03.606Z",
        "nodeRoles": null,
        "threatType": "indicator",
        "description": "Sources: taxii2",
        "malwareFamilies": []
      },
      "status": "create"
    }
  ],
  "lastToken": 218282
}
```

12. Журналирование данных

Для журналирования данных в PT Feeds используется служба systemd-journald, поэтому файлы журналов собираются и ротируются средствами ОС. Для просмотра файлов журнала Docker-контейнера вам нужно знать его имя.

- Чтобы просмотреть файлы журнала из Docker-контейнера:

  1. Получите имя Docker-контейнера:
     ```
     docker ps
     ```
  2. Выполните команду:
     - Если нужно отображать всю информацию в файле журнала:
       ```
       docker-compose logs CONTAINER_NAME=<Имя Docker-контейнера>
       ```
     - Если нужно отслеживать появление новых сообщений в журнале:
       ```
       docker-compose logs -f <Имя Docker-контейнера>
       ```

13. Резервное копирование базы данных PostgreSQL

Данные PT Feeds хранятся в базе данных PostgreSQL. Вы можете создавать резервные копии данных, чтобы обеспечить их сохранность.

- Чтобы выполнить резервное копирование базы данных PostgreSQL:

  1. Перейдите в каталог `/var/lib/docker/volumes/cybsi-lite_pgdata/_data`.
  2. Выполните команду:

     - Если нужно создать резервную копию в виде архива формата TAR:

       ```
       docker exec -it cybsi-lite_db_1 pg_dump -U cybsilite -d cybsilite -Ft -f /data/postgres/backup/cybsilite.tar
       ```

     - Если нужно создать резервную копию в виде архива формата BAK:

       ```
       docker exec -it cybsi-lite_db_1 pg_dump -U cybsilite -d cybsilite -Fc -f /data/postgres/backup/cybsilite.bak
       ```

  Резервная копия базы данных PostgreSQL создана. Архив с резервной копией доступен по пути `/var/lib/docker/volumes/cybsi-lite_pgbackup/_data`.

14. Восстановление базы данных PostgreSQL

- Чтобы восстановить базу данных PostgreSQL из дампа:

  1. На узле с PT Feeds переместите дамп в каталог `/var/lib/docker/volumes/cybsi-lite_pgbackup/_data`.
  2. Выполните команду:

     - Если нужно восстановить базу данных из архива формата TAR:

       ```
       docker exec -it cybsi-lite_db_1 pg_restore -U cybsilite -d cybsilite -Ft /data/postgres/backup/cybsilite.tar
       ```

     - Если нужно восстановить базу данных из архива формата BAK:

       ```
       docker exec -it cybsi-lite_db_1 pg_restore -U cybsilite -d cybsilite -Fc /data/postgres/backup/cybsilite.bak
       ```

  База данных PostgreSQL восстановлена.

15. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

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

Вы можете получать техническую поддержку на портале.

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

В этом разделе

15.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

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

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

Техническая поддержка на портале предоставляется на русском и английском языках.

15.2. Время работы службы технической поддержки

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

15.3. Как служба технической поддержки работает с запросами

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

В этом разделе

Предоставление информации для технической поддержки (см. раздел 15.3.1)

Типы запросов (см. раздел 15.3.2)

Время реакции и приоритизация запросов (см. раздел 15.3.3)

Выполнение работ по запросу (см. раздел 15.3.4)

15.3.1. Предоставление информации для технической поддержки

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

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

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

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

15.3.2. Типы запросов

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

Вопросы по установке, повторной установке и предстартовой настройке продукта

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

Вопросы по администрированию и настройке продукта

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

Восстановление работоспособности продукта

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

Обновление продукта

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

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

Устранение дефектов продукта

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

15.3.3. Время реакции и приоритизация запросов

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

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

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 5).

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

Таблица 5. Время реакции на запрос и время его обработки

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

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

15.3.4. Выполнение работ по запросу

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

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

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

Работы по запросу считаются выполненными, если:

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

POSITIVE TECHNOLOGIES

О нас

Positive Technologies — ведущий разработчик решений для кибербезопасности. Наши технологии и сервисы используют более 2300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Уже 20 лет наша основная задача — предотвращать хакерские атаки 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).