Positive Technologies Cybersecurity Intelligence

Версия 2.0

Руководство администратора

POSITIVE TECHNOLOGIES

Дата редакции документа: 15.11.2019

Содержание

1. Об этом документе

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

Руководство адресовано специалистам, администрирующим Cybsi.

В этом разделе

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример текста с условным обозначением	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 Cybsi

Вы можете найти дополнительную информацию о Cybsi на ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать учетную запись на портале.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 8).

2. О Cybsi

Cybsi — это программная платформа для накопления знаний о существующих и потенциальных угрозах информационной безопасности, а также о способах их обнаружения. Cybsi собирает, анализирует и хранит информацию об угрозах информационной безопасности и индикаторах компрометации, которые могут быть выделены в рамках угрозы. Индикаторы компрометации — это артефакты, наблюдаемые в сети или в операционной системе и указывающие на вредоносную активность в инфраструктуре.

3. Архитектура Cybsi

Cybsi работает на нескольких узлах, которыми могут быть физические серверы или виртуальные машины. На узлах по отдельности устанавливаются следующие программные компоненты Cybsi:

- сервисы Cybsi;
- база данных под управлением СУБД PostgreSQL;
- хранилище объектов Minio.

Установка и настройка всех компонентов осуществляется удаленно на машине администратора при помощи ПО Ansible для удаленной настройки UNIX-систем.

> **Примечание.** В качестве машины администратора не рекомендуется использовать узлы, предназначенные для установки программных компонентов Cybsi.

4. Требования к программному обеспечению

Перед развертыванием Cybsi вам необходимо подготовить инфраструктуру в соответствии с программными требованиями.

Требования к машине администратора:

- операционная система Debian 8, Debian 9 или Ubuntu (последней версии или последней LTS-версии);
- Ansible версии 2.7 и выше;
- интерпретатор Python версии 2.7 и выше;
- менеджер пакетов pip;
- архиватор tar;
- библиотека OpenSSL;
- утилита sshpass для выполнения команд на удалённом сервере по протоколу SSH без ввода пароля вручную;
- утилита сжатия файлов Gzip;
- удаленный доступ по протоколу SSH на узлы с программными компонентами.

Требования к узлам с программными компонентами:

- операционная система Debian версии 9;
- настроенный sshd-сервер для удаленного управления узлами с машины администратора;
- доступ в интернет.

5. Подготовка к установке

Перед началом установки Cybsi вам необходимо подготовить машину администратора:

- скачать пакеты, указанные в требованиях к машине администратора (см. раздел 4);
- распаковать архив с программными компонентами Cybsi в любой каталог на машине администратора.

► Чтобы подготовить машину администратора:

1. Установите пакеты, необходимые для работы Cybsi:
   ```
   sudo apt-get install tar gzip sshpass openssl python python-pip
   ```
2. Установите Ansible:
   ```
   sudo -H pip install ansible
   ```
3. Распакуйте архив с установщиком Cybsi:
   ```
   tar xf cybsi-installer-<номер версии>.tar.gz
   ```
4. Перейдите в каталог с распакованным установщиком Cybsi:
   ```
   cd cybsi-installer-<номер версии>
   ```

Машина администратора подготовлена, вы можете приступить к настройке параметров конфигурационных файлов.

6. Предварительная настройка

Предварительная настройка Cybsi включает базовую настройку параметров конфигурационных файлов, без которой продукт не может работать корректно, и дополнительную настройку источников, позволяющую адаптировать Cybsi под конкретную инфраструктуру.

В этом разделе

6.1. Базовая настройка

Базовая настройка параметров конфигурационных файлов необходима для дальнейшей установки продукта. Каталог `cybsi-installer-<номер версии>` содержит следующие настраиваемые конфигурационные файлы:

- `hosts.ini`;
- `group_vars/cybsi/cybsi.yml`;
- `group_vars/all/secrets.yml`;
- `group_vars/cybsi/secrets.yml`.

Также каталог содержит файл `group_vars/cybsi/defaults.yml` с параметрами по умолчанию, которые не требуется настраивать (за исключением установки пользовательских сертификатов).

В этом разделе

6.1.1. Настройка параметров конфигурационного файла hosts.ini

В конфигурационном файле `hosts.ini` вы задаете Ansible-роли для узлов с программными компонентами Cybsi.

Внимание! Файл `hosts.ini` обязателен для заполнения.

► Чтобы настроить базовые параметры конфигурационного файла `hosts.ini`:

1. Откройте конфигурационный файл `hosts.ini` в каталоге `cybsi-installer-<номер версии>`.
2. Укажите доменное имя узла, на который будут установлены сервисы Cybsi.

   Например:
   ```
   [cybsi]
   server-01.domain.com
   ```

   Примечание. Доменное имя необходимо указывать на новой строке после тега.
3. Укажите доменное имя узла, на который будет установлена база данных под управлением СУБД PostgreSQL.

   Например:
   ```
   [postgresql]
   server-02.domain.com
   ```
4. Укажите доменное имя узла, на который будет установлено хранилище данных Minio.

   Например:
   ```
   [s3]
   server-03.domain.com
   ```

Базовые параметры конфигурационного файла `hosts.ini` настроены.

6.1.2. Настройка параметров конфигурационного файла group_vars/cybsi/cybsi.yml

В конфигурационном файле `group_vars/cybsi/cybsi.yml` вы задаете основные конфигурационные параметры Cybsi.

Внимание! Файл `group_vars/cybsi/cybsi.yml` обязателен для заполнения.

► Чтобы настроить базовые параметры конфигурационного файла `group_vars/cybsi/cybsi.yml`:

1. Откройте конфигурационный файл `cybsi.yml` в каталоге `cybsi-installer-<номер версии>/group_vars/cybsi`.
2. Заполните следующие поля:

- **cydsi_backend_version** — версия backend-компонента Cybsi (предоставляется вместе с архивом установщика);
- **cydsi_frontend_version** — версия frontend-компонента Cybsi (предоставляется вместе с архивом установщика);
- **cydsi_api_adapter_version** — версия API-адаптера для сервисов Pyshok и VirusLocal (предоставляется вместе с архивом установщика);
- **cydsi_sso_host** — доменное имя или IP-адрес сервиса управления пользователями и доступом Positive Technologies Identity and Access Management (PT IAM);

  Примечание. Если вы указываете доменное имя, оно должно совпадать с доменным именем, для которого выдан SSL-сертификат PT IAM для https.
- **cydsi_tms_host** — доменное имя или IP-адрес сервиса Tenant Management Service (TMS), может совпадать с **cydsi_sso_host**.

  Примечание. Если вы указываете доменное имя, оно должно совпадать с доменным именем, для которого выдан SSL-сертификат PT IAM для https.
- **dns_server** — доменное имя или IP-адрес DNS-сервера, к которому Cybsi обращается для получения DNS-информации.

Базовые параметры конфигурационного файла `group_vars/cybsi/cybsi.yml` настроены.

6.1.3. Настройка параметров конфигурационного файла group_vars/all/secrets.yml

Конфигурационный файл `group_vars/all/secrets.yml` содержит конфиденциальные данные хранилищ и SSH, поэтому рекомендуется хранить файл в зашифрованном виде на машине администратора.

Внимание! Файл `group_vars/all/secrets.yml` обязателен для заполнения.

► Чтобы настроить базовые параметры конфигурационного файла `group_vars/all/secrets.yml`:

1. Откройте файл `secrets.yml` в каталоге `cybsi-installer-<номер версии>/group_vars/all`.
2. Заполните следующие поля:
   - **ansible_ssh_user** — имя пользователя, под которым Ansible обращается к узлам по протоколу SSH;
   - **ansible_ssh_pass** — пароль для подключения Ansible по протоколу SSH (не используется, если указано значение для **ansible_ssh_private_key_file**);
   - **ansible_become_pass** — пароль для повышения привилегий с помощью sudo;
   - **ansible_ssh_private_key_file** — ключ для подключения Ansible по протоколу SSH (не используется, если указано значение для **ansible_ssh_pass**);

- **node_ssh_user** — пользователь, от имени которого Ansible настраивает систему (по умолчанию **cybsi**, обычно совпадает с именем пользователя в **ansible_ssh_user**);
- **db_user** — имя пользователя СУБД PostgreSQL (по умолчанию **cybsi**);
- **db_password** — пароль пользователя СУБД PostgreSQL;
- **s3_access_key** — ключ для подключения к Minio (по умолчанию **cybsi-accesskey**);
- **s3_secret_key** — пароль для подключения к Minio.

Базовые параметры конфигурационного файла `group_vars/all/secrets.yml` настроены.

См. также

Шифрование файлов secrets.yml (см. раздел 6.1.5)

6.1.4. Настройка параметров конфигурационного файла group_vars/cybsi/secrets.yml

Конфигурационный файл `group_vars/cybsi/secrets.yml` содержит конфиденциальные данные сервисов Cybsi, поэтому рекомендуется хранить его в зашифрованном виде на машине администратора.

Внимание! Файл `group_vars/cybsi/secrets.yml` обязателен для заполнения.

► Чтобы настроить базовые параметры конфигурационного файла `group_vars/cybsi/secrets.yml`:

1. Откройте файл `secrets.yml` в каталоге `cybsi-installer-<номер версии>/group_vars/cybsi`.
2. Заполните следующие поля:
   - **cybsi_auth_basic_credentials** — "имя:uuid:пароль" для авторизации в API (например,"cybsi-api-user:eb480250-45a3-4193-ba79-bbd625c9f5af:724cd9e1f596b58246a2c");
   - **cybsi_archive_default_password** — пароль от архива, в который Cybsi запаковывает скачиваемые пользователями файлы (по умолчанию **infected!**);
   - **cybsi_docker_registry_user** — имя пользователя для подключения к реестру docker registry (зависит от лицензии и предоставляется вместе с архивом установщика);
   - **cybsi_docker_registry_password** — пароль для подключения к реестру docker registry (зависит от лицензии и предоставляется вместе с архивом установщика).

   Базовые параметры конфигурационного файла `group_vars/cybsi/secrets.yml` настроены.

См. также

Шифрование файлов secrets.yml (см. раздел 6.1.5)

6.1.5. Шифрование файлов secrets.yml

► Чтобы зашифровать конфигурационные файлы `group_vars/all/secrets.yml` и `group_vars/cybsi/secrets.yml`:

1. Выполните команду:
```
ansible-vault encrypt group_vars/all/secrets.yml
ansible-vault encrypt group_vars/cybsi/secrets.yml
```
2. В отобразившейся строке введите пароль для шифрования.

Конфигурационные файлы зашифрованы.

► Чтобы расшифровать конфигурационные файлы `group_vars/all/secrets.yml` и `group_vars/cybsi/secrets.yml`:

1. Выполните команду:
```
ansible-vault decrypt <путь до файла>
```
2. В отобразившейся строке введите пароль для расшифровки.

Конфигурационные файлы расшифрованы.

Вы также можете изменить параметры каждого зашифрованного файла без расшифровки, используя команду:

```
ansible-vault edit <путь до файла>
```

6.1.6. Установка пользовательского SSL-сертификата

Для доступа к страницам веб-интерфейса Cybsi через HTTPS-соединение необходимо установить в Cybsi SSL-сертификат.

По умолчанию Cybsi самостоятельно генерирует самоподписанный сертификат и копирует его на узел, указанный в параметре `[cybsi]` файла `hosts.ini`. Если вы хотите использовать свой сертификат, необходимо установить его отдельно.

► Чтобы установить пользовательский SSL-сертификат:

1. Перейдите в каталог с распакованным установщиком Cybsi:
2. Откройте файл `group_vars/cybsi/defaults.yml`.
3. В поле **cybsi_generate_ssl_certificates** установите значение **false**.
4. Откройте файл `group_vars/cybsi/secrets.yml`.
5. В поле **cybsi_ssl_cert_content** укажите содержимое открытого ключа своего SSL-сертификата.
6. В поле **cybsi_ssl_key_content** укажите содержимое закрытого ключа своего SSL-сертификата.

```
cybsi_ssl_cert_content: |
        -----BEGIN CERTIFICATE-----
        MIIF5DCCBMygAwIBAgISBJTngpTqbIzMN3t47R6JMbhmMA0GCSqGSIb3DQEBCwUA
        OrJ6wkM4jT1x8kZteQP0mZOgPcGQi6zVvwcxp2864miigaN+YZvI4DjcvisCa2Ig
        ...
        q1/6tzl41mk91biVk//961WWjJK062U5AgHYN1rDpbWRUYNSOO+ycjFzb8G/0ewy
        XiVI7x9mSCS+WMmEE7KANdI6JRPISrTS
        -----END CERTIFICATE-----

cybsi_ssl_key_content: |
        -----BEGIN PRIVATE KEY-----
        MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQDJmKijPBXwufxi
        x8upsKMnl0wWYC4YmjB4BdGaCkKxBOJcoO/WjDNbRufDt0nLQrXqNw4nSxwehnej
        ...
        d9KOZfEZI95Qc0OtnEHDDcjAo/ao4pkedfFC9dqgBgp9xUPyFnGtsORInL7ClrsN
        YL7Qx2Dd4ohTWqq9WBsn5w==
        -----END PRIVATE KEY-----
```

Рисунок 1. Пример содержимого открытого и закрытого ключей

Пользовательский SSL-сертификат установлен.

6.2. Настройка источников

Источники для Cybsi содержат информацию об угрозах и индикаторах компрометации. Некоторые источники подключены по умолчанию и не требуют дополнительной настройки при установке Cybsi, подключение к другим источникам настраивается при установке Cybsi.

В этом разделе

6.2.1. Настройка Positive Technologies MultiScanner

Внимание! Лицензия Positive Technologies MultiScanner (далее также — PT MS) должна включать публичный API.

Для подключения Cybsi к PT MS необходимо в конфигурационном файле `group_vars/cybsi/cybsi.yml` в поле **cybsi_pt_ms_host** указать API-узел или IP-адрес PT MS, в конфигурационном файле `group_vars/cybsi/secrets.yml` в поле **cybsi_pt_ms_api_key** указать ключ авторизации для API PT MS.

6.2.2. Настройка AlienVault Open Threat Exchange

Для подключения Cybsi к AlienVault Open Threat Exchange необходимо в конфигурационном файле `group_vars/cybsi/secrets.yml` в поле **cybsi_alienvault_api_key** указать ключ авторизации для API AlienVault Open Threat Exchange. Вы можете получить ключ на сайте продукта после регистрации.

6.2.3. Настройка Malware Information Sharing Platforms

Источник Malware Information Sharing Platforms по умолчанию активирован и не требует дополнительной настройки при установке Cybsi. Фиды, получаемые от Malware Information Sharing Platforms, доступны на сайтах circl.lu и botvrij.eu.

6.2.4. Настройка Positive Technologies Network Attack Discovery

Для подключения Cybsi к Positive Technologies Network Attack Discovery (далее также — PT NAD) необходимо:

- в конфигурационном файле `group_vars/cybsi/cybsi.yml` в поле **cybsi_pt_nad_host** указать API-узел или IP-адрес PT NAD;
- в конфигурационном файле `group_vars/cybsi/secrets.yml` в поле **cybsi_pt_nad_user** указать имя пользователя API PT NAD;
- в конфигурационном файле `group_vars/cybsi/secrets.yml` в поле **cybsi_pt_nad_password** указать пароль пользователя API PT NAD.

6.2.5. Настройка Trend Micro Deep Discovery Analyzer

Для подключения Cybsi к Trend Micro Deep Discovery Analyzer необходимо в конфигурационном файле `group_vars/cybsi/cybsi.yml` в поле **cybsi_tm_ddam_host** указать API-узел или IP-адрес Trend Micro Deep Discovery Analyzer, в конфигурационном файле `group_vars/cybsi/secrets.yml` в поле **cybsi_tm_ddan_api_key** указать ключ авторизации для API Trend Micro Deep Discovery Analyzer.

6.2.6. Настройка VirusLocal

Для подключения Cybsi к VirusLocal необходимо в конфигурационном файле `group_vars/cybsi/cybsi.yml` в поле **cybsi_virus_local_host** указать API-узел или IP-адрес VirusLocal (по умолчанию указан vl.portal.cert.ru), в конфигурационном файле `group_vars/cybsi/secrets.yml` в поле **cybsi_virus_local_api_key** указать ключ авторизации для API VirusLocal.

6.2.7. Настройка Pyshok

Для подключения Cybsi к Pyshok необходимо:

- в конфигурационном файле `group_vars/cybsi/cybsi.yml` в поле **cybsi_pyshok_host** указать API-узел или IP-адрес Pyshok (по умолчанию pyshok.portal.cert.ru);
- в конфигурационном файле `group_vars/cybsi/secrets.yml` в поле **cybsi_pyshok_user** указать имя пользователя API Pyshok;
- в конфигурационном файле `group_vars/cybsi/secrets.yml` в поле **cybsi_pyshok_password** указать пароль пользователя API Pyshok.

6.2.8. Настройка источника "БД ЦНИИС"

Для подключения Cybsi к источнику "БД ЦНИИС" необходимо в конфигурационном файле `group_vars/cybsi/cybsi.yml` в поле **cybsi_zniis_mpo_host** указать API-узел или IP-адрес БД ЦНИИС (по умолчанию nums.zniis.ru), в конфигурационном файле `group_vars/cybsi/secrets.yml` в поле **cybsi_zniis_mpo_api_bearer_token** указать ключ авторизации для API БД ЦНИИС.

6.2.9. Настройка источника "Россвязь"

Источник "Россвязь" по умолчанию активирован и не требует дополнительной настройки при установке Cybsi. Для обогащения информации о стационарных телефонных номерах в Cybsi используются следующие реестры Россвязи:

- https://rossvyaz.ru/data/ABC-3xx.csv;
- https://rossvyaz.ru/data/ABC-4xx.csv;
- https://rossvyaz.ru/data/ABC-8xx.csv.

7. Установка продукта

По завершении настройки базовых параметров конфигурационных файлов и параметров источников вы можете запустить установку Cybsi.

► Чтобы установить Cybsi:

1. Выполните команду:

   `ansible-playbook -i hosts.ini cybsi.yml`, если файлы `group_vars/all/secrets.yml` и `group_vars/cybsi/secrets.yml` не зашифрованы;

   `ansible-playbook -i hosts.ini cybsi.yml --ask-vault-pass`, если файлы зашифрованы.

2. Если файлы зашифрованы, в отобразившейся строке введите пароль для расшифровки.

3. Дождитесь завершения установки.

Cybsi, а также сервисы Postgresql и Minio установлены на соответствующие узлы.

После установки продукт доступен по адресу https://<cybsi-host>/, где <cybsi-host> — узел, указанный в параметре `[cybsi]` файла `hosts.ini`.

8. 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 support.ptsecurity.com или по телефону. Запросы на портале — основной способ обращений за технической поддержкой.

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

В этом разделе

8.1. Техническая поддержка на портале

Портал support.ptsecurity.com 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 support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Технолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать учетную запись на портале.

Портал технической поддержки доступен на русском, английском, немецком и итальянском языках.

8.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по следующим телефонам:

- Великобритания +44 20 3769 3606
- Италия +39 06 9763 1532
- Казахстан +7 727 350 52 92
- Россия +7 495 744 01 44
- США +1 857 208 7273
- Чехия +420 530 510 700
- Южная Корея +82 2 6410 8582

Техническая поддержка по телефону предоставляется на русском и английском языке.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданному запросу.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте запрос на портале support.ptsecurity.com. Запрос на портале, созданный и обновляемый по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

8.3. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся запросам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

8.4. 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

8.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" 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).

"Позитив Текнолоджиз" 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.

8.4.2. 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 "Позитив Текнолоджиз" 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). "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

"Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

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

8.4.3. 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 2).

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 2. 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	До 24 часов	Не ограничено

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
	и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес		
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).

8.4.4. 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, "Позитив Текнолоджиз" 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.

О компании

"Позитив Текнолоджиз" — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения "Позитив Текнолоджиз" для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты "Позитив Текнолоджиз" заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com