



PT Dephaze

версия 2026.3.0

Руководство администратора

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 31.08.2026

Содержание

1.	Об этом документе.....	4
1.1.	Условные обозначения.....	4
1.2.	Другие источники информации о PT Dephaze	5
2.	О PT Dephaze.....	6
3.	Архитектура PT Dephaze.....	7
4.	Аппаратные и программные требования	8
5.	Развертывание PT Dephaze.....	12
5.1.	Импорт образа виртуальной машины с программным обеспечением PT Dephaze	12
5.2.	Установка и настройка сервера PT Dephaze	12
5.3.	Установка и настройка атакующего узла	13
5.4.	Настройка сетевого интерфейса	15
5.5.	Настройка синхронизации системного времени.....	16
5.6.	Установка пользовательских SSL-сертификатов	16
6.	Развертывание мобильного модуля PT Dephaze	19
6.1.	Установка Debian из подготовленного ISO-образа	19
6.2.	Установка мобильного модуля PT Dephaze	21
6.3.	Настройка операционной системы	21
6.4.	Инициализация PT Dephaze.....	21
6.5.	Импорт и настройка виртуальной машины с атакующим узлом	22
6.6.	Подключение атакующего узла к серверу PT Dephaze.....	24
6.7.	Проверка подключения к сети	25
7.	Лицензирование	26
8.	Обновление PT Dephaze	27
8.1.	Обновление сервера	27
8.2.	Обновление атакующего узла до версии 2026.3.0	27
8.3.	Обновление мобильного модуля	28
9.	Решение проблем.....	30
9.1.	Ошибки при установке мобильного модуля	30
9.2.	Не открывается веб-интерфейс PT Dephaze.....	31
9.3.	Агент не отображается в списке доступных	32
10.	О технической поддержке	33
	Глоссарий.....	37

1. Об этом документе

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

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

Комплект документации PT Dephaze включает в себя следующие документы:

- Этот документ.
- Руководство пользователя — содержит подробную информацию о сценариях работы с продуктом, о настройке функций продукта для решения конкретных задач.

В этом разделе

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

[Другие источники информации о PT 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 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 Dephaze

Вы можете найти дополнительную информацию о PT Dephaze на справочном портале help.ptsecurity.com и на [Позитивном портале](#). Через Позитивный портал вы также можете обратиться [в техническую поддержку](#) (см. раздел 10).

2. О PT Dephaze

PT Dephaze — система для автоматизированного тестирования на проникновение, предназначенная для выявления недостатков во внутренней ИТ-инфраструктуре и ошибок в конфигурации средств защиты.

PT Dephaze реализует действия злоумышленника в ИТ-инфраструктуре, используя распространенные тактики и техники кибератак, а также хакерские инструменты для их реализации. В результате атак вы получаете отчет о тестировании с оценкой защищенности инфраструктуры и рекомендациями по устранению недостатков.

Ключевые функции PT Dephaze:

- автоматизированное проведение тестирования на проникновение методами черного и серого ящика;
- обнаружение угроз;
- визуализация схемы атаки;
- контроль над процессом тестирования с возможностью ручного согласования или отклонения атак;
- журналирование действий, выполняемых в процессе тестирования;
- предоставление рекомендаций по устранению недостатков;
- сбор учетных записей, которые были обнаружены и использованы в процессе тестирования на проникновение;
- формирование подробного отчета с результатами тестирования.

3. Архитектура PT Dephaze

PT Dephaze состоит из серверной части и атакующего узла. Сервер — основной компонент, который позволяет конфигурировать PT Dephaze через веб-интерфейс. Атакующий узел — узел, на который устанавливается агент для выполнения атакующих действий в рамках пентеста.

Внимание! Для перехвата учетных данных PT Dephaze использует технику атаки «Прослушивание сетевого трафика». Для выполнения этой техники атакующий узел необходимо расположить в одном сегменте сети с атакуемыми узлами.

В минимальной конфигурации PT Dephaze может разворачиваться на двух узлах. Для тестирования нескольких сегментов сети вы можете установить дополнительные атакующие узлы. При этом все развернутые атакующие узлы будут управляться одним сервером PT Dephaze.

Взаимодействие между компонентами системы:

- При запуске пентеста сервер отправляет на атакующий узел данные, необходимые для выполнения команд и инструкций к атаке.
- На атакующем узле агент обрабатывает полученные данные и на их основе выполняет команды.
- Агент передает на сервер статус выполнения команд и инструкций.

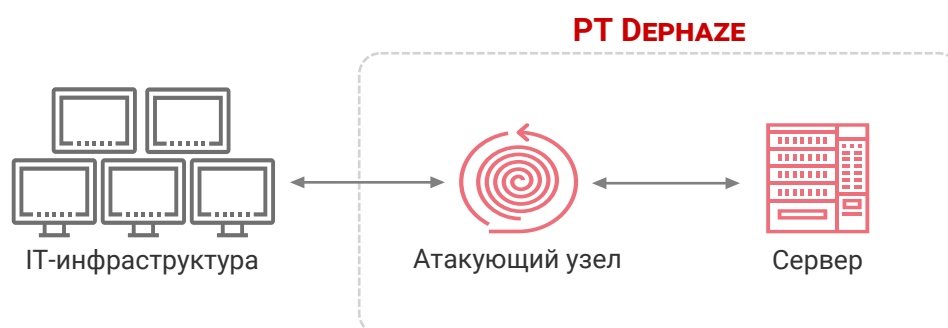


Рисунок 1. Архитектура PT Dephaze

4. Аппаратные и программные требования

В этом разделе приведены аппаратные и программные требования к серверу PT Dephaze и атакующему узлу.

Требования к программному обеспечению

PT Dephaze разворачивается в виртуальной среде. Рекомендуется использовать системы виртуализации VMware ESXi версии 6 или выше, Microsoft Hyper-V Server 2019 или KVM с модулем ядра Linux версии 6.1.0 или выше.

PT Dephaze поставляется в виде двух дистрибутивов. Каждый дистрибутив содержит образ виртуальной машины в формате OVF. Сервер, атакующий узел и мобильный модуль PT Dephaze устанавливаются на операционную систему Debian 13 Trixie, которая входит в состав дистрибутивов.

Для работы в интерфейсе PT Dephaze рекомендуется использовать следующие браузеры:

- Google Chrome версии 138 или выше;
- Microsoft Edge версии 137 или выше;
- Mozilla Firefox версии 140 или выше;
- Яндекс Браузер версии 25.6 или выше.

Требования к аппаратному обеспечению

Таблица 2. Аппаратные требования к серверу PT Dephaze

Параметр	Минимальные требования	Рекомендуемые требования
Виртуальный процессор	8 ядер	8 ядер (или больше)
Физический процессор	Intel Xeon серии E3 или аналогичные	Intel Xeon Gold или более поздние
Память (ОЗУ)	16 ГБ	32 ГБ
Твердотельный накопитель (SSD)	100 ГБ (или HDD со скоростью вращения 10 000 об./мин или выше)	200 ГБ
Графический процессор ¹	С поддержкой адаптеров NVIDIA, совместимых с CUDA Toolkit (серии GeForce RTX, Quadro или Tesla), например, GeForce RTX 4060 для ноутбуков с 8 ГБ видеопамяти	

¹ Графический процессор используется при реализации атак методом подбора учетных данных (brute force).

Таблица 3. Аппаратные требования к атакующему узлу

Параметр	Минимальные требования	Рекомендуемые требования
Виртуальный процессор	6 ядер	8 ядер
Память (ОЗУ)	8 ГБ	16 ГБ
Жесткий диск (HDD)	40 ГБ	—
Твердотельный накопитель (SSD)	—	100 ГБ

Таблица 4. Аппаратные требования к ноутбуку

Параметр	Минимальные требования	Рекомендуемые требования
Виртуальный процессор	14 ядер	20 ядер или более
Физический процессор	Intel Core i7-13700	Intel Core i9-13900
Память (ОЗУ)	32 ГБ	64 ГБ
Твердотельный накопитель (SSD)	200 ГБ	1 ТБ
Графический процессор	С поддержкой адаптеров NVIDIA, совместимых с CUDA Toolkit (серии GeForce RTX, Quadro или Tesla), например, GeForce RTX 4060 для ноутбуков с 8 ГБ видеопамяти	
Сетевой порт	Ethernet RJ-45	

Требования к сетевой инфраструктуре

Для обеспечения сетевого взаимодействия компонентов сервера PT Dephaze необходимо разрешить входящее и исходящее подключение к портам, указанным в таблице ниже.

Таблица 5. Компоненты сервера PT Dephaze и порты взаимодействия

Компонент	Протокол	Порт	Направление	Назначение
Рабочая станция	SSH (TCP)	22	Входящее и исходящее	Подключение по протоколу SSH для взаимодействия с ОС
Веб-интерфейс PT Dephaze	TCP	443	Входящее	Доступ к веб-интерфейсу PT Dephaze
Сервис взаимодействия сервера с агентом	TCP	16956	Входящее и исходящее	Обмен данными между сервером и агентом

Компонент	Протокол	Порт	Направление	Назначение
Система поисковых и аналитических инструментов OpenSearch	TCP	5601	Входящее	Обработка данных
Система хранения и анализа метрик VictoriaMetrics	TCP	8428	Входящее	База данных метрик сервера и атакующего узла
Система мониторинга и виртуализации данных Grafana	TCP	3000	Входящее	Виртуализация данных

Для сетевого взаимодействия компонентов агента с элементами IT-инфраструктуры и сервером PT Dephaze необходимо разрешить входящее и исходящее подключения к портам, указанным в таблице ниже.

Таблица 6. Компоненты атакующего узла и порты взаимодействия

Компонент	Протокол	Порт	Направление	Назначение
Рабочая станция администратора	SSH (TCP)	22	Входящее	Подключение по протоколу SSH для взаимодействия с ОС
Атакующие действия	UDP	53, 88, 137, 389, 1434, 5353, 5355	Входящее и исходящее	Получение и обработка данных для запуска атакующих действий
	TCP	21, 25, 53, 80, 88, 110, 135, 139, 143, 389, 443, 445, 587, 636, 1433, 3389, 5985, 5986, 47386	Входящее и исходящее	

Взаимодействие со средствами защиты информации

Средства обеспечения безопасности могут влиять на работу PT Dephaze. Поэтому при установке средств защиты информации (СЗИ) на виртуальные машины с компонентами PT Dephaze необходимо создать белые списки с исключениями для сканирования и проверок безопасности.

На сервере PT Dephaze необходимо добавить в исключения следующие каталоги:

- /home/dephaze/*
- /var/lib/docker/volumes/*
- /var/lib/docker/overlay2/*
- /var/lib/docker/containers/*
- /tmp/*

Внимание! Не рекомендуется выполнять пентест атакующих узлов, а также запускать одновременно несколько пентестов с одинаковым и пересекающимся набором узлов.

На атакующем узле PT Dephaze необходимо выполнить следующие действия:

- Отключить мониторинг всех процессов.
- Добавить в исключения следующие каталоги:
 - /home/dephaze/*
 - /tmp/*
 - /var/lib/docker/overlay2/*
 - /var/lib/docker/containers/*
 - /usr/bin/
 - /usr/sbin/
 - /usr/lib/python3/dist-packages/*
 - /usr/share/doc/python3-impacket/*
- Исключить из мониторинга входящее и исходящее подключение [к портам, которые использует \(см. раздел 4\)](#) PT Dephaze.

5. Развертывание PT Dephaze

Для развертывания и подготовки PT Dephaze к работе необходимо выполнить следующие действия:

1. Импортировать образы виртуальных машин сервера PT Dephaze и атакующего узла в систему виртуализации.
2. Если в вашей инфраструктуре не используется DHCP-сервер, настроить сетевой интерфейс на сервере PT Dephaze и атакующем узле.
3. Установить и настроить сервер PT Dephaze.
4. Установить и настроить атакующий узел.
5. Настроить синхронизацию системного времени на сервере PT Dephaze и атакующем узле с NTP-серверами.

В этом разделе

[Импорт образа виртуальной машины с программным обеспечением PT Dephaze \(см. раздел 5.1\)](#)

[Установка и настройка сервера PT Dephaze \(см. раздел 5.2\)](#)

[Установка и настройка атакующего узла \(см. раздел 5.3\)](#)

[Настройка сетевого интерфейса \(см. раздел 5.4\)](#)

[Настройка синхронизации системного времени \(см. раздел 5.5\)](#)

[Установка пользовательских SSL-сертификатов \(см. раздел 5.6\)](#)

5.1. Импорт образа виртуальной машины с программным обеспечением PT Dephaze

PT Dephaze поставляется в виде двух образов виртуальных машин (VM):

- `pt-dephaze-server-<Версия продукта>.ovf` — образ для сервера PT Dephaze;
- `pt-dephaze-attack-node-<Версия продукта>.ovf` — образ для атакующего узла.

Необходимо скачать архивы с образами VM, распаковать их и импортировать каждый файл в систему виртуализации.

5.2. Установка и настройка сервера PT Dephaze

Внимание! Если в вашей инфраструктуре не используется DHCP-сервер, перед установкой сервера PT Dephaze необходимо [указать параметры сетевого интерфейса \(см. раздел 5.4\)](#).

► Чтобы установить и настроить сервер PT Dephaze:

1. Запустите импортированную ВМ.
2. Войдите в ОС, используя логин dephaze и пароль dePh@ze2025!.
3. Снова введите dePh@ze2025! и дважды укажите новый пароль.

Примечание. Пароль должен содержать не менее 16 символов, включая буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы.

4. Откройте приложение Terminal.
5. Если доступен пакет обновлений, [установите его \(см. раздел 8.1\)](#).
6. Запустите установку сервера PT Dephaze:

```
./dephaze-init.bin
```

Примечание. При запросе пароля для sudo необходимо ввести пароль пользователя dephaze.

7. Выберите язык установки. По умолчанию выбран русский язык (RU). Для выбора английского введите 2 и нажмите Enter.
8. Введите логин, который будет использоваться для входа в веб-интерфейс PT Dephaze.
9. Сохраните логины и пароли для доступа к сервисам PT Dephaze.

Внимание! При копировании данных из консоли использование комбинации клавиш Ctrl+C недопустимо. Это действие прервет процесс установки продукта.

10. Подтвердите сохранение данных.

► Чтобы проверить корректность развертывания сервера:

1. Запустите браузер и введите в адресной строке `https://<FQDN или IP-адрес сервера PT Dephaze>`.

Примечание. Необходимо оставить без внимания предупреждение о небезопасном сертификате. Передаваемые данные защищаются при помощи HTTPS с использованием самоподписанного TLS-сертификата. При необходимости вы можете использовать сертификат, выданный официальным центром сертификации.

2. Введите логин и пароль, полученные при установке сервера PT Dephaze.

Теперь вы можете перейти к [активации лицензии \(см. раздел 7\)](#).

5.3. Установка и настройка атакующего узла

Внимание! Если в вашей инфраструктуре не используется DHCP-сервер, перед установкой атакующего узла необходимо [указать параметры сетевого интерфейса \(см. раздел 5.4\)](#).

► Чтобы установить и настроить атакующий узел PT Dephaze:

1. Запустите импортированную ВМ.
2. Войдите в ОС, используя логин `dephaze` и пароль `dePh@ze2025!`.
3. Снова введите `dePh@ze2025!` и дважды укажите новый пароль.

Примечание. Пароль должен содержать не менее 16 символов, включая буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы.

4. Откройте приложение Terminal Emulator.
5. Если доступен пакет обновлений, [установите его \(см. раздел 8.2\)](#).
6. Запустите установку атакующего узла:

```
./dephaze-init.bin
```

Примечание. При запросе пароля для `sudo` необходимо ввести пароль пользователя `dephaze`.

7. Выберите язык установки. По умолчанию выбран русский язык (RU). Для выбора английского введите 2 и нажмите Enter.
8. Укажите имя агента.

Примечание. Имя агента должно содержать не более 20 символов и состоять из букв латинского алфавита в нижнем регистре, цифр и минуса (-).

9. Укажите FQDN или IP-адрес сервера PT Dephaze.
10. Откройте конфигурационный файл `resolv.conf`:

```
sudo nano /etc/resolv.conf
```

11. Укажите IP-адреса DNS-серверов:

```
search <Доменное имя>
nameserver <IP-адрес 1>
nameserver <IP-адрес 2>
```

Атакующий узел установлен и настроен.

► Чтобы проверить корректность развертывания атакующего узла:

1. Запустите браузер и введите в адресной строке `https://<FQDN или IP-адрес сервера PT Dephaze>`.
2. Введите логин и пароль, указанные при установке PT Dephaze.

3. В главном меню нажмите .

4. Нажмите **Создать пентест**.

В списке **Агенты** отображается имя агента, которое вы указали при установке.

5. Если агент не отображается в списке, обратитесь к разделу [«Решение проблем» \(см. раздел 9.3\)](#).

5.4. Настройка сетевого интерфейса

По умолчанию PT Dephaze настроен на получение сетевых параметров от DHCP-сервера. Если в вашей инфраструктуре не используется DHCP-сервер, перед установкой сервера PT Dephaze и атакующего узла необходимо вручную указать параметры сетевого интерфейса.

► Чтобы настроить сетевой интерфейс на сервере PT Dephaze:

1. Запустите импортированную VM.
2. Войдите в ОС, используя логин `dephaze` и пароль `dePh@ze2025!`.
3. Откройте приложение Terminal.
4. Откройте на редактирование файл конфигурации сетевых интерфейсов:

```
sudo nano /etc/network/interfaces
```
5. Настройте сетевой интерфейс:

```
auto <Имя сетевого интерфейса>
iface <Имя сетевого интерфейса> inet static
    address <IP-адрес сети>
    netmask <Маска сети>
    gateway <Сетевой шлюз>
    dns-nameservers <IP-адреса DNS-серверов>
```
6. Перезапустите службу управления сетевыми интерфейсами:

```
sudo systemctl restart networking
```

► Чтобы настроить сетевой интерфейс на атакующем узле:

1. Запустите импортированную VM.
2. Войдите в ОС, используя логин `dephaze` и пароль `dePh@ze2025!`.
3. Откройте приложение Terminal Emulator.
4. Откройте на редактирование файл конфигурации сетевых интерфейсов:

```
sudo nano /etc/network/interfaces
```
5. Настройте параметры сетевого интерфейса `eth0`:

```
auto eth0
iface eth0 inet static
    address <IP-адрес сети>
    netmask <Маска сети>
    gateway <Сетевой шлюз>
```
6. Перезапустите службу управления сетевыми интерфейсами:

```
sudo systemctl restart networking
```

5.5. Настройка синхронизации системного времени

Для корректной работы PT Dephaze необходимо настроить синхронизацию системного времени на сервере PT Dephaze и атакующем узле с NTP-серверами.

► Чтобы настроить синхронизацию системного времени:

1. Откройте конфигурационный файл `timesyncd.conf`:
`sudo nano /etc/systemd/timesyncd.conf`
2. В секции `Time` в параметре `NTP` укажите адреса NTP-серверов через пробел.
 Например:
`[Time]`
`NTP=ntp0.ntp-servers.net ntp1.ntp-servers.net`
3. Включите автоматическую синхронизацию времени с NTP-серверами:
`sudo timedatectl set-ntp true`
4. Перезапустите сервис, чтобы изменения вступили в силу:
`sudo systemctl restart systemd-timesyncd`

Вы можете проверить корректность настройки с помощью команды `timedatectl show-timesync --all | grep -i SystemNTPServers`.

5.6. Установка пользовательских SSL-сертификатов

При первом запуске PT Dephaze автоматически устанавливает самоподписанные сертификаты для доступа к его веб-интерфейсу через HTTPS. Вы можете установить собственные SSL-сертификаты, выполнив инструкцию ниже.

Примечание. По умолчанию самоподписанные сертификаты хранятся в каталоге `/home/dephaze/certs` и действуют один год.

Допустимый формат файлов сертификатов и ключей — PEM.

► Чтобы установить пользовательские сертификаты:

1. Разместите файлы сертификатов в каталоге `/home/dephaze/certs`.
2. Откройте интерфейс командной строки и подключитесь к серверу PT Dephaze:
`ssh dephaze@<IP-адрес сервера PT Dephaze>`
3. Остановите сервисы OpenSearch и Grafana, последовательно выполнив команды:
`docker compose down`
`docker compose -f docker-compose-opensearch.yml down`
`docker compose -f grafana/docker-compose-monitoring.yml down`
4. Откройте на редактирование файл `docker-compose.yml` и укажите файлы сертификатов:
`services:`
`dephaze-frontend:`

```

environment:
  Hosting_Certificate_Key: /certs/<Файл ключа сертификата>
  Hosting_Certificate_FileName: /certs/<Файл сертификата>
volumes:
  - ./certs:/certs:ro
pg-admin:
  volumes:
    - pgadmin_data:/var/lib/pgadmin
    - ./certs/<Файл ключа сертификата>:/certs/server.key:ro
    - ./certs/<Файл сертификата>:/certs/server.cert:ro

```

5. Сохраните изменения и закройте файл.

6. Откройте на редактирование файл `docker-compose-opensearch.yml` и укажите файлы сертификатов:

```

services:
  opensearch:
    environment:
      plugins.security.ssl.http.pemcert_filepath: certs/<Файл сертификата>
      plugins.security.ssl.http.pemkey_filepath: certs/<Файл ключа сертификата>
      plugins.security.ssl.http.pemtrustedcas_filepath: certs/<Файл корневого сертификата>
      plugins.security.ssl.transport.pemcert_filepath: certs/<Файл сертификата>
      plugins.security.ssl.transport.pemkey_filepath: certs/<Файл ключа сертификата>
      plugins.security.ssl.transport.pemtrustedcas_filepath: certs/<Файл корневого
сертификата>
      plugins.security.authcz.admin_dn: CN=<Название корневого центра сертификации
(например, DephazeRootCA)>
    volumes:
      - ./certs:/usr/share/opensearch/config/certs:ro
  opensearch-dashboards:
    environment:
      SERVER_SSL_CERTIFICATE: /usr/share/opensearch-dashboards/config/<Файл сертификата>
      SERVER_SSL_KEY: /usr/share/opensearch-dashboards/config/<Файл ключа сертификата>
    volumes:
      - ./certs/<Файл сертификата>:/usr/share/opensearch-dashboards/config/<Файл
сертификата>:ro
      - ./certs/<Файл ключа сертификата>:/usr/share/opensearch-dashboards/config/<Файл
ключа сертификата>:ro

```

7. Сохраните изменения и закройте файл.

8. Откройте на редактирование файл `grafana/docker-compose-monitoring.yml` и укажите файлы сертификатов:

```

services:
  grafana:
    environment:
      GF_SERVER_CERT_FILE: /etc/ssl/certs/<Файл сертификата>
      GF_SERVER_CERT_KEY: /etc/ssl/certs/<Файл ключа сертификата>
    volumes:
      - ./certs/<Файл сертификата>:/etc/ssl/certs/<Файл сертификата>:ro
      - ./certs/<Файл ключа сертификата>:/etc/ssl/certs/<Файл ключа сертификата>:ro

```

9. Сохраните изменения и закройте файл.

10. Запустите службы OpenSearch и Grafana, последовательно выполнив команды:

```
docker compose -f docker-compose-opensearch.yml up -d
docker compose -f grafana/docker-compose-monitoring.yml up -d
docker compose up -d
```

Вы можете просмотреть список запущенных контейнеров с помощью команды `docker ps`. Для проверки работоспособности сертификатов необходимо войти в веб-интерфейс PT Dephaze.

6. Развертывание мобильного модуля PT Dephaze

Мобильный модуль PT Dephaze — это облегченная версия PT Dephaze с оптимизированными системными требованиями, которая не требует выделения серверных ресурсов для развертывания. Мобильный модуль предназначен для проведения тестирования на проникновение в сегментах сети, к которым отсутствует прямой сетевой доступ из инфраструктуры PT Dephaze. Модуль используется в случаях, когда развертывание полноценного экземпляра PT Dephaze невозможно или нецелесообразно, например при проверке изолированных или территориально удаленных сегментов сети.

Мобильный модуль PT Dephaze устанавливается на ноутбук. Перед установкой необходимо проверить устройство на соответствие [аппаратным и программным требованиям](#) (см. раздел 4).

Для установки мобильного модуля PT Dephaze необходимо выполнить следующие действия:

1. Установить операционную систему Debian.
2. Установить мобильный модуль PT Dephaze.
3. Скачать и установить приложение «[Ассистент](#)».
4. Настроить операционную систему.
5. Импортировать и настроить виртуальную машину с атакующим узлом PT Dephaze.
6. Подключить атакующий узел к серверу PT Dephaze.
7. Проверить подключение к сети.

В этом разделе

[Установка Debian из подготовленного ISO-образа \(см. раздел 6.1\)](#)

[Установка мобильного модуля PT Dephaze \(см. раздел 6.2\)](#)

[Настройка операционной системы \(см. раздел 6.3\)](#)

[Инициализация PT Dephaze \(см. раздел 6.4\)](#)

[Импорт и настройка виртуальной машины с атакующим узлом \(см. раздел 6.5\)](#)

[Подключение атакующего узла к серверу PT Dephaze \(см. раздел 6.6\)](#)

[Проверка подключения к сети \(см. раздел 6.7\)](#)

6.1. Установка Debian из подготовленного ISO-образа

Для установки операционной системы Debian вам потребуется файл `mobile-dephaze-installer-
<Версия PT Dephaze>.iso`, который входит в комплект поставки, а также внешний носитель с объемом памяти не менее 32 ГБ.

Внимание! В процессе установки ОС все данные на диске ноутбука будут удалены.

Внимание! Перед началом установки необходимо запустить ноутбук в режиме UEFI (BIOS — не поддерживается). В UEFI, в разделе параметров хранилища (Storage), необходимо отключить контроллер Intel VMD.

► Чтобы установить Debian из подготовленного ISO-образа:

1. Создайте установочный носитель из ISO-файла, который входит в комплект поставки.
2. Запустите ноутбук с установочным носителем, созданным из ISO-файла.
Откроется экран установки Debian.
3. Выберите **Graphical install** и нажмите Enter.
4. На этапе выбора языка (**Select a language**) выберите **Русский** и нажмите **Continue**.
5. На этапе выбора местонахождения выберите страну, в которой располагается сервер, и нажмите **Продолжить**.
6. Выберите клавиатурную раскладку и нажмите **Продолжить**.
7. Если на этапе разметки дисков появится запрос **Выполнить установку в UEFI?** (предупреждение о ранее установленной ОС в режиме совместимости с BIOS), выберите **Да** и нажмите **Продолжить**.
8. На этапе разметки дисков выберите вариант **Авто — использовать весь диск** и нажмите **Продолжить**.
9. Выберите диск для установки и нажмите **Продолжить**.
10. В случае появления окна выбора схемы разметки выберите **Все файлы в одном разделе (рекомендуется новичкам)** и нажмите **Продолжить**.
11. Выберите **Закончить разметку и записать изменения на диск** и нажмите **Продолжить**.
12. Подтвердите запись изменений, выбрав **Да** и нажав **Продолжить**.
13. Если на этапе разметки дисков появится ошибка **Operation not permitted during write on '/dev/mapper/ventoy'**, нажмите **Пропустить**.
14. Если в процессе установки появится ошибка **Не удастся создать файловую систему efі на разделе #1 устройства /dev/*nvme***, выполните форматирование раздела (см. раздел 9.1) и перезапустите установку.
Начнется установка Debian. По окончании установки устройство будет отключено.
15. Отключите установочный носитель.

6.2. Установка мобильного модуля PT Dephaze

► Чтобы установить мобильный модуль PT Dephaze:

1. После установки операционной системы Debian включите ноутбук.
2. Войдите в ОС, используя логин `dephaze` и пароль `dePh@ze2025!`.
3. Снова введите `dePh@ze2025!` и дважды укажите новый пароль.

Примечание. Пароль должен содержать не менее 16 символов, включая буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы.

4. Откройте приложение Terminal.
5. Запустите установку мобильного модуля PT Dephaze:
`bash dephaze-installer-<Версия PT Dephaze>.run`
6. В окне выбора языка установщика выберите **RU** и подтвердите выбор.
7. Примите условия лицензионного соглашения.
8. Согласитесь с выполнением установки.
9. Введите пароль, который задали ранее.
10. По завершении установки перезагрузите устройство.

Теперь вы можете перейти к настройке ОС.

6.3. Настройка операционной системы

► Чтобы настроить операционную систему:

1. Откройте параметры операционной системы.
2. В главном меню выберите **Настройки** → **Расширенная конфигурация сети**, выберите проводное подключение и нажмите .
3. На вкладке **IPv4** выключите метод IPv4.
4. На вкладке **IPv6** выключите метод IPv6.

Теперь вы можете перейти к инициализации PT Dephaze.

6.4. Инициализация PT Dephaze

После установки ОС и PT Dephaze необходимо выполнить его инициализацию.

► Чтобы выполнить инициализацию PT Dephaze:

1. Откройте приложение Terminal.
2. Запустите сценарий установки PT Dephaze:
`./dephaze-init.bin`
3. Сохраните логины и пароли для доступа к сервисам PT Dephaze.
4. Откройте браузер на базе Chromium и перейдите по ссылке `https://127.0.0.1/`.
5. Если отобразится сообщение `The password you use to log in to your computer no longer matches that of your login keyring`, введите пароль `dePh@ze2025!`.

Примечание. При разворачивании PT Dephaze для его сайта автоматически устанавливается самоподписанный сертификат, поставляемый в составе дистрибутива. При попытке подключения к сайту вы получите предупреждение о том, что создаваемое подключение не защищено. В окне предупреждения требуется нажать **Дополнительно** и подтвердить переход.

6. Введите логин и пароль, которые вы указали при установке PT Dephaze.

Теперь вы можете перейти к установке и настройке виртуальной машины с атакующим узлом.

6.5. Импорт и настройка виртуальной машины с атакующим узлом

Внимание! Перед каждым выключением ноутбука рекомендуется завершать работу виртуальной машины PT Dephaze. Для этого необходимо в системе виртуализации в контекстном меню машины выбрать **Power** → **Shut Down Guest**. При последующем включении ноутбука необходимо запускать виртуальную машину снова (**Power** → **Power On**).

Если ноутбук не оснащен встроенным сетевым адаптером, до начала импорта виртуальной машины необходимо подключить внешний сетевой адаптер.

Импорт виртуальной машины

► Чтобы импортировать образ виртуальной машины с атакующим узлом:

1. Запустите VMware Workstation.
2. В окне **VMware Kernel Module Updater** нажмите **Install**.
3. Примите условия лицензионного соглашения и нажмите **Next**.
4. Откажитесь от проверки обновлений и нажмите **Next**.
5. Откажитесь от участия в программе улучшения качества (CEIP) и нажмите **Finish**.
6. В окне VMware Workstation выберите **Open a Virtual Machine**.
7. Перейдите в каталог `/home/dephaze/attack-vm`.

8. Выберите OVF-файл с образом ВМ и нажмите **Открыть**.

9. Нажмите **Import**.

По завершении импорта виртуальной машины вы можете перейти к ее настройке.

Настройка виртуальной сети

► Чтобы настроить виртуальную сеть:

1. В главном меню выберите **Edit** → **Virtual Network Editor**.
2. Выберите сеть **vmnet1**.
3. В поле **Subnet IP** введите **192.168.200.0**.
4. Выберите сеть **vmnet0**.
5. В поле **Bridged to** выберите физический сетевой адаптер, который будет использоваться для взаимодействия с тестируемым сегментом сети (например, **eth0**).
6. Нажмите **Save**.

Настройка виртуальной машины

► Чтобы настроить виртуальную машину с атакующим узлом:

1. Откройте параметры импортированной виртуальной машины.
2. Выберите вкладку **Processors** и укажите количество виртуальных ядер в соответствии с [аппаратными требованиями \(см. раздел 4\)](#).
3. Выберите вкладку **Memory** и укажите объем памяти (ГБ) по формуле: доступный объем памяти / 3.

Примечание. Допустимый объем памяти — 8 ГБ и выше.

4. Выберите вкладку **Hardware** и нажмите **Add**.
5. Выберите **Network Adapter** и нажмите **Finish**.
6. В списке устройств выберите **Network Adapter** и в блоке **Network Connection** выберите вариант **Custom: Specific virtual network**.
7. В раскрывающемся списке выберите **/dev/vmnet0**.
8. На вкладке **Network Adapter 2** выберите вариант **Custom: Specific virtual network**.
9. В раскрывающемся списке выберите **/dev/vmnet1**.
10. Нажмите **Save**.
11. В контекстном меню виртуальной машины выберите **Power** → **Power On**.
12. Подключитесь к консоли виртуальной машины.

13. Войдите в учетную запись ОС, используя логин dephaze и пароль dePh@ze2025!.

14. Снова введите dePh@ze2025! и дважды укажите новый пароль.

Примечание. Пароль должен содержать не менее 16 символов, включая буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы.

15. Нажмите **Applications** и выберите **Settings** → **Advanced Network Configuration**.

16. Двойным щелчком мыши выберите **Wired connection 1** и в поле **Connection name** введите External.

17. В поле **Device** выберите ens33 и нажмите **Save**.

18. В окне **Network Connections** двойным щелчком мыши выберите **Wired connection 2**.

19. В поле **Connection name** введите Internal.

20. В поле **Device** выберите ens34.

21. На вкладке **IPv4 Settings** выберите **Method** → **Manual**.

22. В поле **Addresses** нажмите **Add** и введите 192.168.200.10.

23. В поле **Netmask** введите 24 и нажмите **Save**.

24. Нажмите Dephaze и выберите **Log Out** → **Restart**.

Атакующий узел перезагружен.

См. также

[Аппаратные и программные требования \(см. раздел 4\)](#)

6.6. Подключение атакующего узла к серверу PT Dephaze

► Чтобы подключить атакующий узел к серверу PT Dephaze:

1. Подключитесь к консоли виртуальной машины.
2. Введите логин dephaze и пароль, который вы установили ранее.
3. Откройте приложение Terminal Emulator.
4. Запустите сценарий:

```
./dephaze-init.bin
```
5. Введите имя агента и нажмите клавишу Enter.
6. Введите IP-адрес сервера PT Dephaze — 192.168.200.1 и нажмите клавишу Enter.
7. По завершении установки завершите сеанс учетной записи dephaze.

Теперь вы можете перейти к проверке подключения к сети.

6.7. Проверка подключения к сети

После установки и настройки мобильного модуля PT Dephaze вы можете проверить работоспособность сети, а также доступность DNS-сервера и контроллеров домена.

► Чтобы проверить подключение к сети:

1. Подключитесь к атакующему узлу:

```
ssh dephaze@192.168.200.10
```

2. Выполните команду для отображения всех IP-адресов, присвоенных сетевым интерфейсам системы:

```
ip a | grep inet
```

3. Если сетевой интерфейс атакующего узла не получил IP-адрес тестируемого сегмента, перезапустите атакующий узел и повторите проверку.

4. Проверьте корректность параметров DNS-серверов:

```
cat /etc/resolv.conf
```

5. Если данные DNS-серверов указаны неверно, запустите [установку атакующего узла \(см. раздел 5.3\)](#) и выполните его настройку снова.

6. Выполните запрос к DNS-серверу на разрешение доменного имени:

```
nslookup <FQDN узла тестируемого сегмента>
```

7. Выполните запрос к DNS-серверу на разрешение имени контроллера домена:

```
nslookup <FQDN контроллера домена тестируемого сегмента>
```

8. Если разрешение доменных имен не выполнено, запустите [установку атакующего узла \(см. раздел 5.3\)](#) и выполните его настройку снова.

7. Лицензирование

Для работы PT Dephaze и его защиты от нелегального использования нужно активировать лицензию.

Тестирование на проникновение (пентест) выполняется только при наличии действующей лицензии. В PT Dephaze доступно два типа лицензий: серверная и мобильная. Серверная предназначена для установки на сервер, мобильная — на ноутбук (например, для тестирования изолированных сегментов или удаленных площадок). Лицензии различаются сроком действия, числом атакующих узлов и количеством тестируемых активов. Учитываются только уникальные IP-адреса: узлы, проверенные ранее, не расходуют лицензионный лимит. По истечении срока действия лицензии проведение пентестов становится недоступным, но вы можете работать с результатами тестирования, полученными ранее. Просмотреть параметры лицензии вы можете на странице **Настройка системы**.

Активация лицензии

Активация лицензии выполняется в веб-интерфейсе PT Dephaze.

► Чтобы активировать лицензию:

1. В главном меню нажмите .
2. Нажмите **Запросить ключ**.

Файл с ключом для активации лицензии сохранится в локальной папке.

3. Передайте полученный файл с ключом поставщику продукта.
4. Получите от поставщика код активации.
5. Нажмите **Ввести код активации**.
6. Введите код и нажмите **Активировать**.

В панели **Активная** отобразится номер лицензии со сроком ее действия.

8. Обновление PT Dephaze

Обновление сервера PT Dephaze и атакующего узла выполняется посредством обновления дистрибутива ранее установленной версии продукта.

Внимание! Обновление сервера и атакующего узла может выполняться только при отсутствии пентестов в статусах **Активный** или **На паузе**.

В этом разделе

[Обновление сервера \(см. раздел 8.1\)](#)

[Обновление атакующего узла до версии 2026.3.0 \(см. раздел 8.2\)](#)

[Обновление мобильного модуля \(см. раздел 8.3\)](#)

8.1. Обновление сервера

► Чтобы обновить сервер PT Dephaze:

1. Запросите пакет для обновления сервера [в службе технической поддержки](#).
2. Загрузите полученный пакет на сервер:
`scp update-dephaze-<Версия продукта>.run dephaze@<IP-адрес сервера PT Dephaze>:~/`
3. Подключитесь к серверу:
`ssh dephaze@<IP-адрес сервера PT Dephaze>`
4. Запустите обновление:
`bash update-dephaze-<Версия продукта>.run`
5. Если система запросит пароль для выполнения команды `sudo`, введите его.

Новые образы импортируются в Docker, контейнеры `dephaze-server` и `dephaze-frontend` перезапускаются автоматически.

8.2. Обновление атакующего узла до версии 2026.3.0

Для обновления атакующего узла до версии 2026.3.0 необходимо:

1. Запросить образ виртуальной машины атакующего узла версии 2026.3.0.0 [в службе технической поддержки](#).
2. Распаковать архив и импортировать каждый файл в систему виртуализации.
3. [Настроить атакующий узел \(см. раздел 5.3\)](#).

С версии PT Dephaze 2026.3.0.0 атакующие узлы версий 2026.2.0.0 и ниже не поддерживаются.

Примечание. Если вы не обновляете сервер и атакующий узел, вы можете продолжать использовать предыдущие версии. При обновлении сервера до версии 2026.3.0 необходимо обновить и атакующий узел.

8.3. Обновление мобильного модуля

Для обновления мобильного модуля PT Dephaze необходимо обратиться в Positive Technologies и получить дистрибутивы с новыми версиями сервера и атакующего узла.

Внимание! Обновление сервера и атакующего узла может выполняться только при отсутствии активных пентестов (в статусах **Активный** или **На паузе**).

Обновление сервера

► Чтобы обновить сервер PT Dephaze:

1. Запросите пакет для обновления сервера [в службе технической поддержки](#).
2. Загрузите полученный пакет на внешний носитель.
3. Вставьте в USB-порт ноутбука внешний носитель с новой версией сервера PT Dephaze.
4. Скопируйте файл `update-dephaze-<Версия PT Dephaze>.run` в папку `/home/dephaze`.
5. Запустите сценарий обновления:

```
bash update-dephaze-<Версия PT Dephaze>.run
```
6. Примите условия лицензионного соглашения дважды.
7. Если система запросит пароль для выполнения команды `sudo`, введите его.

Новые образы импортируются в Docker. Контейнеры `dephaze-server`, `dephaze-frontend` и `dephaze-reports` перезапускаются автоматически.

Обновление атакующего узла

Для обновления атакующего узла до версии 2026.3.0 необходимо:

1. Запросить образ виртуальной машины атакующего узла версии 2026.3.0.0 [в службе технической поддержки](#).
2. Удалить виртуальную машину атакующего узла предыдущей версии (любой версии ниже 2026.3.0).
3. Загрузить полученный образ на внешний носитель.
4. Вставить в USB-порт ноутбука внешний носитель с новой версией атакующего узла.
5. [Импортировать и настроить виртуальную машину с атакующим узлом \(см. раздел 6.5\)](#).

- ▶ Чтобы удалить виртуальную машину атакующего узла версии 2026.2.0 или ниже:
 1. Запустите приложение VMware Workstation.
 2. Выберите виртуальную машину `pt-dephaze-attack-node-<Версия 2026.2.0 или ниже>`.
 3. В контекстном меню виртуальной машины выберите **Manage** → **Delete from Disk**.
 4. Подтвердите действие.

9. Решение проблем

В этом разделе приведены возможные проблемы в работе PT Dephaze и варианты их решения.

В этом разделе

[Ошибки при установке мобильного модуля \(см. раздел 9.1\)](#)

[Не открывается веб-интерфейс PT Dephaze \(см. раздел 9.2\)](#)

[Агент не отображается в списке доступных \(см. раздел 9.3\)](#)

9.1. Ошибки при установке мобильного модуля

Проблема

При установке Debian возникает ошибка «Не удастся создать файловую систему efi на разделе #1 устройства /dev/*nvme*».

Возможные причины

На ноутбуке уже была ранее установлена операционная система, отличная от Debian.

Решение

Необходимо выполнить форматирование системного раздела EFI (ESP).

► Чтобы выполнить форматирование EFI:

1. При возникновении ошибки на экране установщика Debian нажмите **Продолжить**.
2. В блоке **Разметка дисков** выберите вариант с пометкой **ESP** и нажмите клавишу Enter.
3. Выберите **Стирание данных на этом разделе** и нажмите клавишу Enter.
4. Выберите **Да** и нажмите **Продолжить**.
5. Выберите **Настройка раздела завершена** и нажмите клавишу Enter.
6. Выберите **Закончить разметку и записать изменения на диск** и нажмите клавишу Enter.
7. Если по завершении установки появится ошибка записи GRUB, нажмите **Вернуться**, выберите **Отмена установки** и снова запустите [установку операционной системы \(см. раздел 6.1\)](#).

Если после форматирования раздела EFI ошибка сохраняется, необходимо выполнить разметку диска.

► Чтобы выполнить разметку диска:

1. При возникновении ошибки на экране установщика Debian нажмите **Продолжить**.
2. В блоке **Разметка дисков** выберите диск и нажмите клавишу Enter.
3. В блоке **Создать новую пустую таблицу разделов на этом устройстве?** выберите **Да**.
4. В таблице разделов выберите вариант с пометкой **Свободное место** и нажмите клавишу Enter.
5. Выберите **Создать новый раздел** и нажмите клавишу Enter.
6. Укажите новый размер раздела — 1 GB и нажмите клавишу Enter.
7. Выберите тип нового раздела **Первичный** и нажмите клавишу Enter.
8. Выберите местоположение нового раздела — **Начало** и нажмите клавишу Enter.
9. В блоке **Использовать как** выберите **Системный раздел EFI** и нажмите клавишу Enter.
10. В блоке **Метка 'загрузочный'** выберите **вкл**.
11. Если отображается блок **Стирание данных на этом разделе**, выберите в нем **Да** и нажмите **Продолжить**.
12. Выберите **Настройка раздела завершена** и нажмите клавишу Enter.
13. В таблице разделов выберите вариант с пометкой **Свободное место** и нажмите клавишу Enter.
14. Выберите **Создать новый раздел** и нажмите клавишу Enter.
15. Оставьте без изменений размер раздела и нажмите клавишу Enter.
16. Выберите **Настройка раздела завершена** и нажмите клавишу Enter.
17. Выберите **Закончить разметку и записать изменения на диск** и нажмите клавишу Enter.
18. Если отобразятся сообщения **Вы не указали ни одного раздела для пространства подкачки?** и **Хотите вернуться в меню разметки?**, выберите **Нет** и нажмите **Продолжить**.
19. В ответ на сообщение **Записать изменения на диск?** выберите **Да** и нажмите **Продолжить**.

9.2. Не открывается веб-интерфейс PT Dephaze

Проблема

Сервер PT Dephaze не получил IP-адрес, и в браузере не открывается веб-интерфейс.

Возможные причины

1. Особенности сетевых параметров в вашей организации. Например, для серверной части не используется DHCP-сервер и требуется ручная настройка сети на сервере PT Dephaze.
2. Не разрешено входящее подключение к порту TCP 443.
3. Не запущен Docker-контейнер веб-интерфейса PT Dephaze.

Решение

Выполните следующие действия:

1. Обратитесь к ответственным за управление сетевым доступом в вашей организации.
2. Разрешите входящее подключение к порту TCP 443.
3. Проверьте, что Docker-контейнер `dephaze-frontend` запущен на сервере PT Dephaze:
`docker ps -a`
4. Если Docker-контейнер остановлен, запустите его:
`docker compose up -d`
5. Если Docker-контейнер циклически перезапускается, создайте его снова:
`docker stop dephaze-frontend && docker rm dephaze-frontend && docker compose up -d`

9.3. Агент не отображается в списке доступных

Проблема

При создании пентеста агент не отображается в списке доступных агентов в интерфейсе PT Dephaze.

Возможные причины

1. Агент не был запущен на атакующем узле.
2. Агент не установил соединение с сервером PT Dephaze через порт TCP 16956.

Решение

1. Разрешите входящее подключение к порту TCP 16956.
2. Проверьте, что агент запущен на атакующем узле:
`ps aux | grep bombas`
3. Если агент не запущен, выполните [настройку атакующего узла](#) (см. раздел 5.3).

10. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на PT Dephaze 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 гарантийной 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 и сроки 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 portalу 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.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления гарантийной поддержки

Для получения гарантийной 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 гарантийной 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 гарантийной 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 гарантийной 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 7. 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 службы 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.

Глоссарий

Агент

Приложение, которое устанавливается на атакующем узле для выполнения атакующих действий в заданной области тестирования.

Артефакт

Объект, полученный в процессе проведения пентеста и необходимый для дальнейшего развития атаки (например, учетная запись или файл с важной информацией).

Пентест

Совокупность атакующих действий в отношении выбранной области тестирования.

Цель

IP-адрес или диапазон IP-адресов инфраструктуры и критерий достижимости, которые определяют момент завершения тестирования на проникновение.



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.