

Позитив Текнолоджиз Ведомственный центр

Версия 0.9



Руководство администратора

POSITIVE TECHNOLOGIES

© АО "Позитив Текнолоджиз", 2018.

Настоящий документ является собственностью АО "Позитив Текнолоджиз" (далее — "Позитив Текнолоджиз") 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 "Позитив Текнолоджиз".

Документ может быть изменен без предварительного уведомления.

Positive Technologies, Positive Hack Days, PTSECURITY, MaxPatrol, XSpider, SurfPatrol, N-Scope, Positive Technologies Application Firewall, Positive Technologies Application Inspector, Positive Technologies MultiScanner, Positive Technologies Reporting Portal являются зарегистрированными товарными знаками либо товарными знаками "Позитив Текнолоджиз".

Иные товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям. "Позитив Текнолоджиз" не аффилировано с такими правообладателями и не производит продукцию, маркированную такими знаками.

Дата редакции документа: 28.03.2018

Содержание

1.	Об этом документе	4
1.1.	Условные обозначения	4
1.2.	Другие источники информации о ПТ ВЦ	5
2.	О системе ПТ ВЦ	6
3.	Архитектура ПТ ВЦ	7
4.	Аппаратные и программные требования	9
5.	Установка ПТ ВЦ	11
6.	Удаление ПТ ВЦ	12
7.	Управление пользователями и доступом	13
7.1.	Изменение пароля учетной записи Administrator	14
7.2.	Создание учетной записи пользователя в РТ IAM	15
7.3.	Изменение учетной записи пользователя	15
7.4.	Назначение прав учетным записям	16
7.5.	Блокирование учетной записи пользователя	16
7.6.	Активация учетной записи пользователя	16
8.	Обращение в службу технической поддержки	17
8.1.	Техническая поддержка на портале	17
8.2.	Техническая поддержка по телефону	18
8.3.	Время работы технической поддержки	18
8.4.	Как служба технической поддержки работает с заявками	18
8.4.1.	Предоставление информации для технической поддержки	19
8.4.2.	Типы инцидентов	19
8.4.3.	Время реакции на обращение и приоритизация инцидентов	20
8.4.4.	Выполнение работ по заявке	21

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по развертыванию, настройке и администрированию Позитив Текнолоджиз Ведомственный центр (далее также — ПТ ВЦ). Руководство не содержит инструкций по использованию основных функций продукта.

Руководство адресовано специалистам, выполняющим установку, первоначальную настройку и администрирование ПТ ВЦ.

Комплект документации ПТ ВЦ включает в себя следующие документы:

- Этот документ.
- Руководство по установке — содержит инструкции по установке, первоначальной настройке, обновлению и удалению продукта.
- Руководство оператора безопасности — содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности.

В этом разделе

- [Условные обозначения \(см. раздел 1.1\)](#)
- [Другие источники информации о ПТ ВЦ \(см. раздел 1.2\)](#)

1.1. Условные обозначения

В документе приняты условные обозначения (см. таблицу 1).

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, нажмите кнопку	Начало инструкции выделено специальным значком
Нажмите кнопку ОК	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример текста с условным обозначением	Описание
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 ПТ ВЦ

Вы можете найти дополнительную информацию о ПТ ВЦ на www.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 \(см. раздел 8\)](#).

Вы можете пройти обучение по ПТ ВЦ в одном из учебных центров, авторизованных "Позитив Текнолоджиз". Перечень учебных центров можно найти на www.ptsecurity.com.

2. О системе ПТ ВЦ

Позитив Текнолоджиз Ведомственный центр (далее также — ПТ ВЦ) предназначена для информационного взаимодействия с главным центром ГосСОПКА с целью обнаружения, предотвращения и ликвидации последствий компьютерных атак. С помощью ПТ ВЦ осуществляются:

- сбор данных об инцидентах;
- регистрация инцидентов путем создания заявок на их обработку;
- реагирование на инциденты (координация действий, определение причин, локализация инцидента, планирование мер по ликвидации последствий, контроль ликвидации последствий);
- обмен данными об инцидентах с главным центром ГосСОПКА;
- применение методических рекомендаций главного центра ГосСОПКА в процессе мониторинга информационной безопасности.

3. Архитектура ПТ ВЦ

В комплект поставки ПТ ВЦ входят следующие продукты "Позитив Текнолоджиз":

- ПТ ВЦ в составе:
 - Сервисы ядра ПТ ВЦ.
 - Веб-портал с интерфейсом продукта.
 - База данных на базе Microsoft SQL Server для хранения собственных данных и параметров работы ПТ ВЦ.
 - Коннектор к РТ MaxPatrol SIEM для актуализации информации по активам и импорта инцидентов в ПТ ВЦ.
 - Коннектор для передачи сводной информации по инцидентам в главный центр ГосСОПКА.
- РТ MaxPatrol SIEM в составе компонента MP Core.
- РТ IAM – сервис единого входа в продукты "Позитив Текнолоджиз".

Схема взаимодействия продуктов и компонентов представлена на рисунке ниже.

Алгоритм взаимодействия:

1. ПТ ВЦ обращается к РТ MaxPatrol SIEM для получения информации по активам и инцидентам подведомственной региональной или филиальной инфраструктуры.
2. Данные об активах и существующих инцидентах загружаются из РТ MaxPatrol SIEM в ПТ ВЦ.
3. Оператор подключается к веб-порталу ПТ ВЦ через сервис единого входа РТ IAM для актуализации инфраструктуры и анализа инцидентов.
4. Данные о текущем состоянии ведомственной IT-инфраструктуры передаются в главный центр ГосСОПКА для эскалации инцидентов и получения последующих рекомендаций.

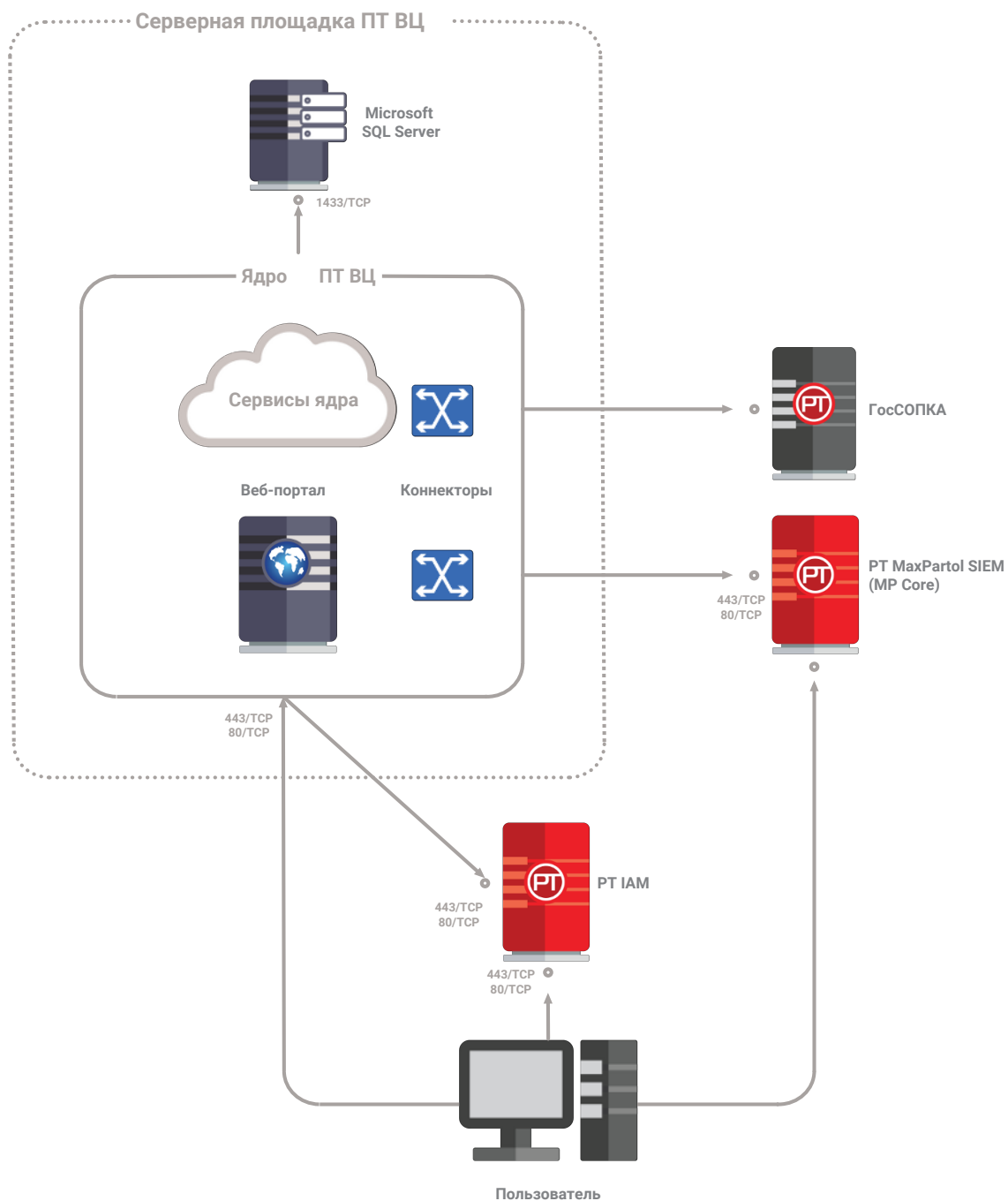


Рисунок 1. Схема взаимодействия компонентов ПТ ВЦ

4. Аппаратные и программные требования

Все компоненты ПТ ВЦ разворачиваются на одном сервере, удовлетворяющем приведенным ниже аппаратным и программным требованиям.

Аппаратные требования для ПТ ВЦ

Таблица 2. Аппаратные требования к серверу для установки ПТ ВЦ

Компонент сервера	Минимальные требования
Центральный процессор	8 ядер с тактовой частотой 2,4 ГГц
Память (ОЗУ)	32 ГБ
Жесткий диск (ОС, компоненты)	2x600 ГБ, SAS, 10000 об/мин, RAID 1
Жесткий диск (локальная база данных)	2x600 ГБ, SAS, 10000 об/мин, RAID 1
Жесткий диск (хранилище артефактов инцидентов)	2x8 ТБ, SATA, RAID 1
Сетевой адаптер	1000 Мбит/с

Программные требования для ПТ ВЦ

- Microsoft Windows Server 2012 R2;
- Microsoft SQL Server 2014 Standart.

Аппаратные требования для РТ MaxPatrol SIEM (MP Core)

Таблица 3. Аппаратные требования к серверу

Компонент сервера	Минимальное требование
Центральный процессор	6 ядер с тактовой частотой 2,4 ГГц
Память (ОЗУ)	32 ГБ
Сетевой адаптер	4 порта со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	Файловая система жестких дисков — NTFS. Для работы ОС и установки компонентов ПТ ВЦ — RAID 1 (10 000 об./мин.), не менее 100 ГБ. Для БД компонентов ПТ ВЦ — RAID 10 (7200 об./мин.), не менее 1,2 ТБ. Для хранилища событий MP SIEM Server — RAID 10 (7200 об./мин., не менее 6 дисков), не менее 1,2 ТБ

Программные требования для РТ MaxPatrol SIEM (MP Core)

- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 R2;
- Google Chrome 63 (и выше).

5. Установка ПТ ВЦ

До начала установки убедитесь, что ваша система соответствует требованиям, предъявляемым к [программному и аппаратному обеспечению](#) (см. раздел 4).

► Чтобы установить ПТ ВЦ:

1. Скопируйте на сервер, где планируется развертывание ПТ ВЦ, в папку `c:\tmpMPX` следующие файлы, входящие в комплект поставки продукта:

- `mp9certportal.nupkg`;
- `csc-sopka.nupkg`;
- `requestmanagementservice.nupkg`;
- `deploy_csc.ps1`;
- `CSC_Public`.

2. Распакуйте архивы.
3. Запустите Windows PowerShell от имени администратора.
4. В окне Windows PowerShell перейдите в каталог с распакованными архивами.

```
cd c:\tmpMPX
```

5. Запустите установку ПТ ВЦ, указав IP-адрес сервера, логин и пароль администратора.

```
deploy_csc.ps1 <ServerIP> <AdministratorUsername> <AdministratorPassword> CSC_Public FALSE  
TRUE TRUE
```

```
deploy_internal.ps1 <ServerIP> none <AdministratorUsername> <AdministratorPassword>  
DepartmentCenter
```

Установка ПТ ВЦ завершена.

6. Удаление ПТ ВЦ

► Чтобы удалить ПТ ВЦ:

1. В панели управления выберите **Программы и компоненты**.
2. В списке установленных программ выберите MaxPatrolRMS и нажмите кнопку **Удалить**.

Откроется окно мастера удаления MaxPatrolRMS.

3. Нажмите кнопку **Uninstall**.
4. Следуйте указаниям мастера.
5. Запустите диспетчер служб IIS.
6. В панели **Подключения** раскройте строку **Сайты**.
7. В контекстном меню службы **Cert_internal** выберите пункт **Deploy** → **Delete Web Site and Content** и подтвердите удаление сайта и контента.

Система ПТ ВЦ удалена.

7. Управление пользователями и доступом

Сервис управления пользователями и доступом PT Identity and Access Management (далее также — PT IAM) обеспечивает механизм единого входа в продуктах "Позитив Текнолоджиз".

Сервис предназначен:

- для создания и настройки учетных записей пользователей;
- назначения ролей, в соответствии с которыми в PT IAM определен состав прав доступа к операциям по работе с сервисом;
- назначения ролей, в соответствии с которыми в ПТ ВЦ определен состав прав доступа к операциям по работе с системой;
- указания информации о пользователе;
- блокировки и активации учетной записи пользователя.

В PT IAM управление пользователями и доступом предусмотрено только для администратора PT IAM. По умолчанию при первом входе в PT IAM вам необходимо в поле **Логин** ввести Administrator, в поле **Пароль** ввести P@ssw0rd. После входа в PT IAM пароль администратора рекомендуется изменить.

Примечание. При изменении пароля администратора PT IAM вам необходимо [прописать новый пароль в конфигурационных файлах системы \(см. раздел 7.1\)](#).

Администратор PT IAM может назначать учетным записям пользователей следующие роли:

- администратора и пользователя — для работы с PT IAM;
- администратора и оператора — для работы с продуктом АО "Позитив Текнолоджиз".

Каждая учетная запись может иметь любое количество ролей. Если ролей несколько, то права суммируются.

Примечание. Учетная запись может не иметь ролей. Если учетная запись не имеет ролей в продукте, то от ее имени невозможно войти в этот продукт.

Для работы с PT IAM существуют две роли — администратор и пользователь. Администратору PT IAM предоставляются права доступа ко всем операциям в PT IAM, включая создание и настройку учетных записей пользователей, назначение ролей, активацию и блокировку учетных записей пользователей. Пользователю PT IAM предоставляются права доступа в личный кабинет для смены пароля, изменения данных профиля пользователя и организационной информации. Также пользователь PT IAM может просматривать список ролей и прав в PT IAM.

Список прав для каждой роли определен в PT IAM и приведен на странице **Роли**.

Для работы с ПТ ВЦ существуют две роли — администратор и оператор. Администратору ПТ ВЦ предоставляются права доступа ко всем операциям в системе. Оператору ПТ ВЦ предоставляются права доступа для работы с системой в зависимости от его производственных задач.

Список прав для каждой роли определен в ПТ ВЦ и приведен на странице **Роли и права доступа**.

Примечание. Роль администратора РТ IAM и роль администратора ПТ ВЦ представляют собой разные роли. Если для учетной записи пользователя назначена роль администратора РТ IAM, то это не означает автоматическое назначение роли администратора ПТ ВЦ.

Для учетной записи пользователя администратор и пользователь РТ IAM могут заполнять профиль пользователя. Эти сведения передаются в ПТ ВЦ. Например, на указанный адрес электронной почты ПТ ВЦ может автоматически отправлять уведомления и отчеты по расписанию.

Учетную запись пользователя администратор РТ IAM может заблокировать или активировать. Удалить учетную запись невозможно.

В этом разделе

- Изменение пароля учетной записи Administrator (см. раздел 7.1)
- Создание учетной записи пользователя в РТ IAM (см. раздел 7.2)
- Изменение учетной записи пользователя (см. раздел 7.3)
- Назначение прав учетным записям (см. раздел 7.4)
- Блокирование учетной записи пользователя (см. раздел 7.5)
- Активация учетной записи пользователя (см. раздел 7.6)

7.1. Изменение пароля учетной записи Administrator

При каждом изменении пароля учетной записи Administrator новый пароль необходимо указывать в конфигурационных файлах ПТ ВЦ для корректной работы системы.

► Чтобы изменить пароль учетной записи Administrator:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Identity and Access Management**.

Откроется страница **Пользователи**.

2. В списке выберите пользователя Administrator.
3. В панели инструментов нажмите кнопку **Редактировать информацию**.

Откроется страница **Редактировать информацию о пользователе**.

4. Измените пароль пользователя.
5. Нажмите кнопку **Сохранить**.
6. На сервере, где установлена ПТ ВЦ, откройте конфигурационный файл C:\Program Files\Positive Technologies\MaxPatrol X Customer Portal\RequestManagementService.Host.exe.config.

7. Укажите новый пароль:

```
<add key="mpx:login" value="Administrator" />  
<add key="mpx:password" value="<Новый пароль>" />
```

8. Откройте конфигурационный файл C:\Program Files\Positive Technologies\CSC\Web.config.


9. Укажите новый пароль:

```
<add key="mpx:login" value="Administrator" />  
<add key="mpx:password" value="<Новый пароль>" />
```

Пароль учетной записи Administrator изменен.

7.2. Создание учетной записи пользователя в PT IAM


► Чтобы создать учетную запись пользователя:

1. В главном меню нажмите  и в раскрывшемся меню выберите PT IAM.
Откроется страница **Пользователи**.
2. В панели инструментов нажмите кнопку **Создать пользователя**.
Откроется страница **Создать пользователя**.
3. В поле **Логин** введите логин.
4. В поле **Пароль** введите пароль учетной записи пользователя.
5. Нажмите кнопку **Сохранить**.

Учетная запись пользователя создана.

7.3. Изменение учетной записи пользователя


► Чтобы изменить учетную запись пользователя:

1. В главном меню нажмите  и в раскрывшемся меню выберите пункт **Identity and Access Management**.
Откроется страница **Пользователи**.
2. Выберите пользователя в списке.
3. В панели инструментов нажмите кнопку **Редактировать информацию**.
Откроется страница **Редактировать информацию о пользователе**.
4. Измените данные пользователя.
5. Нажмите кнопку **Сохранить**.

Учетная запись пользователя изменена.


7.4. Назначение прав учетным записям

► Чтобы назначить права учетной записи:

1. В главном меню нажмите  и в раскрывшемся меню выберите PT IAM.
Откроется страница **Пользователи**.
2. Выберите пользователя в списке.
3. В панели инструментов нажмите кнопку **Роли в приложениях**.
Откроется окно **Роли пользователя <Логин пользователя>**.
4. Выберите продукт и в раскрывшемся меню выберите роль.
5. Нажмите кнопку **Сохранить**.

7.5. Блокирование учетной записи пользователя


► Чтобы заблокировать учетную запись пользователя:

1. В главном меню нажмите  и в раскрывшемся меню выберите PT IAM.
Откроется страница **Пользователи**.
2. Выберите пользователя в списке.
3. В панели инструментов нажмите кнопку **Заблокировать**.

Учетная запись пользователя заблокирована. Напротив заблокированного пользователя отображается значок .

7.6. Активация учетной записи пользователя

► Чтобы активировать учетную запись пользователя:

1. В главном меню нажмите  и в раскрывшемся меню выберите PT IAM.
Откроется страница **Пользователи**.
2. Выберите пользователя в списке.
3. В панели инструментов нажмите кнопку **Разблокировать**.

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. Заявки на портале — основной способ обращений за технической поддержкой.

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

В этом разделе

- [Техническая поддержка на портале \(см. раздел 8.1\)](#)
- [Техническая поддержка по телефону \(см. раздел 8.2\)](#)
- [Время работы технической поддержки \(см. раздел 8.3\)](#)
- [Как служба технической поддержки работает с заявками \(см. раздел 8.4\)](#)

8.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать заявки 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 Текнолоджиз", 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.
- США +1 857 208 7273.
- Италия +39 0 697631532.
- Швеция +46 8 121 111 86.
- Южная Корея +82 264 108 582.
- Россия +7 495 744 01 44.

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 созданной заявке.

Если решить вопрос по телефону в разумное время (15–20 минут) невозможно, создайте заявку на портале support.ptsecurity.com. Заявка на портале, созданная и обновляемая по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

8.3. Время работы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся заявкам 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 заявками

При получении вашей заявки специалист службы технической поддержки классифицирует инцидент, указанный в заявке (присваивает инциденту тип и уровень значимости) и выполняет дальнейшие шаги по разрешению инцидента.

В этом разделе

- Предоставление информации для технической поддержки (см. раздел 8.4.1)
- Типы инцидентов (см. раздел 8.4.2)
- Время реакции на обращение и приоритизация инцидентов (см. раздел 8.4.3)
- Выполнение работ по заявке (см. раздел 8.4.4)

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 заявку.

8.4.2. Типы инцидентов

Специалист технической поддержки относит инцидент в вашей заявке 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" предоставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за инциденты, 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 на обращение и приоритизация инцидентов

Время реакции на ваше обращение рассчитывается как время с момента получения от вас информации по обращению до ответа специалиста технической поддержки с описанием дальнейших шагов по разрешению инцидента. Время реакции зависит от указанного вами уровня значимости инцидента (см. таблицу 4).

Время решения инцидента рассчитывается как время с момента регистрации обращения до ответа специалиста технической поддержки, ведущего к одному из [вариантов решения инцидента](#) (см. раздел 8.4.4).

Специалист технической поддержки может переопределять уровень значимости инцидента по приведенным ниже критериям. Значения сроков являются целевыми и подразумевают стремление и разумные усилия специалистов "Позитив Текнолоджиз" для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 4. Время реакции технической поддержки на обращение и решения инцидента

Уровень значимости инцидента	Критерии значимости инцидента	Время реакции на обращение по инциденту	Время решения инцидента
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку)	До 2 часов	До 2 рабочих дней

Уровень значимости инцидента	Критерии значимости инцидента	Время реакции на обращение по инциденту	Время решения инцидента
	либо оказывающие критическое влияние на бизнес		
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 4 часов	До 3 рабочих дней
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительное влияние на бизнес	До 8 часов	До 6 рабочих дней
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	До 10 рабочих дней

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

8.4.4. Выполнение работ по заявке

По мере выполнения работ по вашей заявке специалист технической поддержки сообщает вам:

- о диагностике инцидента и ее результатах,
- поиске решения или возможности обойти причины возникновения инцидента,
- планировании и выпуске обновления продукта (если требуется для разрешения инцидента).

Если по итогам решения инцидента необходимо внести изменения в продукт, "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по заявке считаются выполненными, если:

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

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.