Positive Technologies Platform 187

Версия 1.153

Руководство по внедрению

POSITIVE TECHNOLOGIES

Дата редакции документа: 09.10.2020

Версия документа: 4

Содержание

1. Об этом документе

Руководство по внедрению содержит информацию для подключения сервера с установленным Positive Technologies Platform 187 в инфраструктуре организации.

Руководство адресовано руководителям и специалистам IT-подразделения организации, которые планируют и выполняют внедрение PT Platform 187 в инфраструктуре организации.

Комплект документации PT Platform 187 включает в себя следующие документы:

— Этот документ.

— Руководство оператора безопасности — содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности.

— Руководство по масштабированию — содержит схемы масштабирования продукта для использования продукта в крупных ИТ-инфраструктурах.

— Комплекты документов для каждого из продуктов, входящих в PT Platform 187 (см. раздел 3).

2. О PT Platform 187

PT Platform 187 (далее также — платформа) — это программно-аппаратный комплекс, предназначенный для реализации основных мер по обеспечению безопасности объектов критической информационной инфраструктуры (КИИ) и взаимодействия с главным центром государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее также — ГосСОПКА). PT Platform 187 содержит технические средства, которые выполняют требования законодательства по защите КИИ, автоматизируют процессы информационной безопасности и значительно повышают их эффективность.

PT Platform 187 рекомендуется для использования как небольшими организациями (с ИТ-инфраструктурой до 250 сетевых узлов), так и территориальными подразделениями крупных организаций (как часть сегмента ГосСОПКА).

3. Архитектура PT Platform 187

PT Platform 187 состоит из пяти продуктов "Позитив Текнолоджиз":

- Система обнаружения и предотвращения вторжений Positive Technologies Network Attack Discovery (далее также PT NAD).
- Система многопоточной проверки файловых ресурсов Positive Technologies MultiScanner (далее также PT MS).
- Система контроля защищенности и соответствия стандартам MaxPatrol (далее также MaxPatrol).
- MaxPatrol Security Information and Event Management (далее также PT MaxPatrol SIEM).
- Ведомственный центр (далее также "ПТ ВЦ").

В составе системы эти продукты уже интегрированы друг с другом и выполняют следующие задачи:

- PT NAD анализирует сетевой трафик и выявляет атаки, сетевые аномалии, скрытое присутствие и активность вредоносного ПО.
- PT MS проводит многопоточную проверку входящих файлов и предотвращает распространение вредоносного ПО.
- MaxPatrol проводит непрерывную инвентаризацию информационных ресурсов, анализирует их защищенность, выявляет уязвимости и автоматизирует процесс управления ими, поддерживает в актуальном состоянии сведения об ИТ-инфраструктуре.
- PT MaxPatrol SIEM анализирует события безопасности из различных источников и выявляет инциденты.
- "ПТ ВЦ" обеспечивает управление процессом реагирования на инциденты и проведение расследования, взаимодействие с главным центром ГосСОПКА.

Взаимодействие продуктов в PT Platform 187 отражено на схеме.

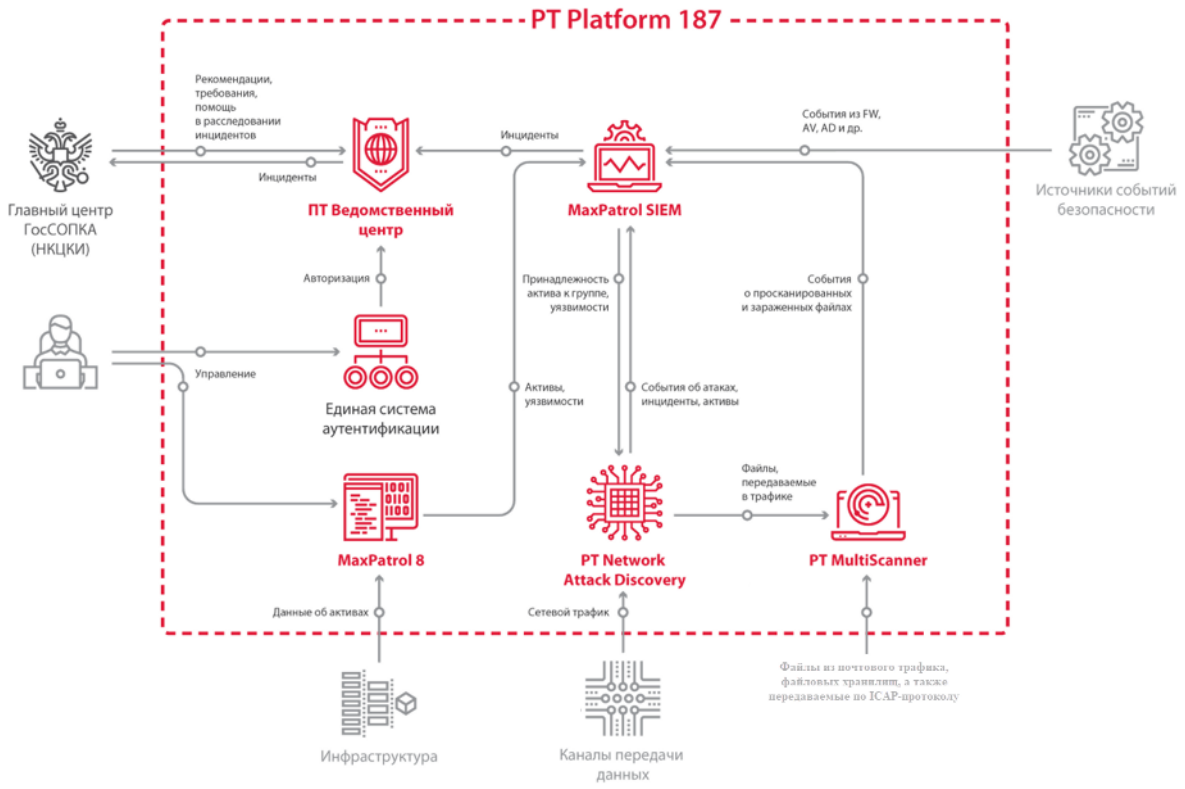

Рисунок 1. Схема взаимодействия продуктов в PT Platform 187

Алгоритм взаимодействия:

1. MaxPatrol сканирует IT-инфраструктуру предприятия, получает сведения о найденных активах, анализирует их защищенность и выявляет уязвимости. Сведения об обнаруженных активах и их уязвимостях MaxPatrolпередает в PT MaxPatrol SIEM.
2. PT NAD захватывает и анализирует сетевой трафик для выявления аномальной сетевой активности и сложных целенаправленных атак. Сведения об обнаруженных атаках PT NAD передает в PT MaxPatrol SIEM. Файлы, пересылаемые по протоколам прикладного уровня, PT NAD извлекает из трафика и передает для анализа в PT MS.
3. PT MS в рамках защиты почтового трафика, веб-трафика, файловых хранилищ и веб-порталов выявляет зараженные объекты в различных потоках данных и агрегирует однотипные элементы атаки в одну угрозу. Сведения о просканированных и зараженных файлах PT MS передает в PT MaxPatrol SIEM.
4. PT MaxPatrol SIEM собирает события из различных источников, в том числе из PT NAD и PT MS, и по правилам корреляции выявляет инциденты. Сведения об инцидентах PT MaxPatrol SIEM передает в "ПТ ВЦ". Также PT MaxPatrol SIEM передает в PT NAD данные об уязвимостях для расчета результативности сетевых атак.
5. Пользователь "ПТ ВЦ" регистрирует инцидент, проводит расследование и отправляет результаты в главный центр ГосСОПКА.

В этом разделе

Интеграция продуктов внутри платформы (см. раздел 3.1)

3.1. Интеграция продуктов внутри платформы

Продукты внутри PT Platform 187 взаимодействуют между собой в соответствии со схемой.

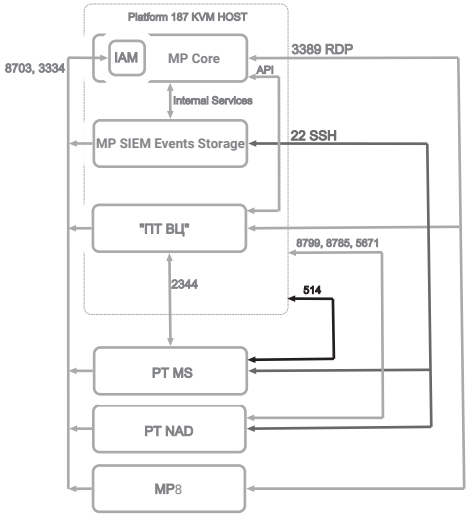

Рисунок 2. Взаимодействие продуктов внутри PT Platform 187

Таблица 1. Взаимодействие продуктов внутри платформы

Продукты	Взаимодействие	Порт
PT NAD и PT MS	Протокол ICAP	2344
PT MS и PT MaxPatrol SIEM	Syslog	514
PT NAD и PT MaxPatrol SIEM	Pgsql	8799
	Обмен по активам	8785
	Sensor agent	5671
	IAM SSO PORTS	8703, 3334

4. Аппаратные требования

Аппаратные требования к серверу PT Platform 187 приведены ниже.

Таблица 2. Аппаратные требования к серверу

Компонент сервера	Минимальное требование
Центральный процессор	2 процессора с тактовой частотой 2,2 ГГц; 18 ядер и 36 потоков на каждый процессор
Память (ОЗУ)	256 ГБ
Жесткие диски и свободное дисковое пространство	4 x 960 ГБ SSD и 4 x 4 ТБ HDD

Перед установкой PT Platform 187 необходимо подключить и настроить сетевые интерфейсы:

- для SPAN-интерфейса;
- для управления;
- для доступа в интернет.

Внимание! Соответствие сервера аппаратным требованиям обязательно.

5. Технические особенности PT Platform 187

Продукты, входящие в PT Platform 187, предустановлены на сервер в "Позитив Текнолоджиз". PT Platform 187 поставляется в виде, готовом для внедрения в ИТ-инфраструктуре организации.

PT Platform 187 имеет следующие ограничения:

— охватывает ИТ-инфраструктуру размера до 250 узлов включительно;

— пропускная способность PT NAD до 100 Мбит/с;

— пропускная способность PT MS до 3000 файлов/час.

6. Интеграция PT Platform 187 с ИТ-инфраструктурой предприятия

Интеграция PT Platform 187 с ИТ-инфраструктурой предприятия заключается в настройке сетевых параметров системы и DNS-сервера предприятия.

Перед настройкой сетевых параметров системы необходимо установить сервер в стойку, подключить сетевые интерфейсы и включить питание (см. Руководство по развертыванию систем на базе унифицированных аппаратных платформ).

Этот раздел содержит описание сетевых интерфейсов PT Platform 187, инструкции по настройке сетевых параметров системы и DNS-сервера предприятия.

В этом разделе

6.1. О сетевых интерфейсах PT Platform 187

PT Platform 187 взаимодействует с ИТ-инфраструктурой предприятия через сетевой интерфейс eth0 и интерфейс выделенной сетевой карты.

Физический интерфейс eth0 предназначен для отправки данных в сеть и получения трафика из сети предприятия, для доступа к графическому интерфейсу продуктов. PT MaxPatrol SIEM, PT MS, PT NAD и "ПТ ВЦ" взаимодействуют с сетью предприятия через виртуальные сетевые интерфейсы, для которых eth0 работает в режиме сетевого моста. MP взаимодействует с сетью предприятия через eth0 напрямую. Имена сетевых интерфейсов перечислены в таблице ниже.

Таблица 3. Имена сетевых интерфейсы продуктов PT Platform 187

Продукт	Интерфейс
MP	eno1
PT MaxPatrol SIEM	siem
PT MS	ms
PT NAD	nad
"ПТ ВЦ"	dc

В интерфейс выделенной сетевой карты поступает копия трафика из сети предприятия от оборудования, применяющего технологию SPAN (SwИTch Port Analyzer). Этот трафик сканируется продуктом PT NAD.

Примечание. Для работы через интерфейс eno1 необходимо подключить сервер к сети предприятия через сетевой порт Gb1 (см. Руководство по развертыванию систем на базе унифицированных аппаратных платформ).

6.2. Настройка сетевых параметров PT Platform 187

По умолчанию система настроена на автоматическое присвоение IP-адресов по DHCP для сетевых интерфейсов. Вы можете также назначать статические IP-адреса для сетевых интерфейсов и шлюза по умолчанию.

Настройка сетевых параметров PT Platform 187 состоит из следующих шагов:

1. Назначения статических IP-адресов для сетевых интерфейсов и шлюза по умолчанию или настройки их автоматического присвоения.
2. Добавления IP-адреса сервера для пересылки DNS-запросов.

   Примечание. Внутренний DNS-сервер PT Platform 187 обеспечивает взаимодействие между продуктами по доменным именам внутри только той подсети, к которой принадлежат IP-адреса сетевых интерфейсов продуктов. Поэтому для своевременного обновления продуктов необходимо обеспечить для сервера системы соединение с интернетом и добавить в систему IP-адрес сервера для пересылки DNS-запросов.

Настройку сетевых параметров PT Platform 187 необходимо выполнять с помощью конфигуратора. Также с помощью конфигуратора вы можете просматривать текущие значения сетевых параметров системы (например, значения IP-адреса продуктов требуются для настройки межсетевого экрана и DNS-сервера предприятия (см. раздел 6.3)).

Все серверы в локальной сети должны синхронизироваться по времени.

В этом разделе

6.2.1. Вход в главное меню конфигуратора

► Чтобы войти в главное меню конфигуратора:

1. Подключите монитор и клавиатуру к серверу PT Platform 187 (см. Руководство по развертыванию систем на базе унифицированных аппаратных платформ).
2. В интерфейсе терминала Debian укажите логин — `configurator` и пароль — `configurator`.

   Интерфейс терминала Debian отобразит главное меню конфигуратора.

Рисунок 3. Вход в главное меню конфигуратора

Вход в главное меню конфигуратора выполнен.

Примечание. Главное меню конфигуратора также доступно удаленно по протоколу SSH (порт 22/TCP).

6.2.2. Просмотр значений сетевых параметров системы

► Чтобы просмотреть значений сетевых параметров системы:

1. В главном меню конфигуратора введите `1 (Show current appliance configuration)`.
2. В меню выбора параметров для отображения введите `1 (Show brief configuration)`.

   Интерфейс конфигуратора отобразит значения сетевых параметров системы (значения IP-адресов сетевых интерфейсов продуктов, шлюза по умолчанию, сервера для пересылки DNS-запросов).

6.2.3. Назначение статического IP-адреса для сетевого интерфейса продукта

Внимание! Все пять IP-адресов для сетевых интерфейсов системы необходимо назначать из одной подсети. Межсетевой экран должен предоставлять входящие соединения в эту подсеть на перечисленные ниже порты. В противном случае продукты системы не смогут взаимодействовать с IT-инфраструктурой предприятия.

Таблица 4. Продукты PT Platform 187, сетевые интерфейсы и порты взаимодействия

Продукт	Интерфейс	TCP-порт
MP	eno1	2002
PT MaxPatrol SIEM	siem	443, 514, 3333, 3334, 8091, 8190
PT MS	ms	25, 80, 443, 445, 1344 (или 2344, зависит от версии PT MS)
PT NAD	nad	443
"ПТ ВЦ"	dc	443

Для работы с виртуальными машинами и веб-интерфейсом управления необходимо открыть TCP-порты 80, 443, 8080.

► Чтобы назначить статический IP-адрес для сетевого интерфейса продукта:

1. В главном меню конфигуратора введите `2 (Change IP address)`.
2. В меню выбора сетевого интерфейса введите порядковый номер пункта меню с именем того сетевого интерфейса, для которого необходимо назначить статический IP-адрес.
3. В меню типа адресации введите `2 (Static)`.
4. Введите IP-адрес сетевого интерфейса продукта.

Статический IP-адрес для сетевого интерфейса продукта назначен.

6.2.4. Назначение статического IP-адреса для шлюза по умолчанию

► Чтобы назначить статический IP-адрес для шлюза по умолчанию:

1. В главном меню конфигуратора введите `3 (Change default Gateway)`.
2. Введите IP-адрес шлюза по умолчанию.

Статический IP-адрес для шлюза по умолчанию назначен.

6.2.5. Настройка автоматического присвоения IP-адреса для сетевого интерфейса продукта

► Чтобы настроить автоматическое присвоение IP-адреса для сетевого интерфейса продукта:

1. В главном меню конфигуратора введите `2 (Change IP address)`.
2. В меню выбора сетевого интерфейса введите порядковый номер пункта меню с именем того сетевого интерфейса, для которого необходимо присвоить IP-адрес автоматически.
3. В меню типа адресации введите `1 (DHCP)`.
4. Введите `y`.

Автоматическое присвоение IP-адреса для сетевого интерфейса продукта настроено.

6.2.6. Добавление IP-адреса сервера для пересылки DNS-запросов

► Чтобы добавить IP-адрес сервера для пересылки DNS-запросов:

1. В главном меню конфигуратора введите `4`.
2. Введите IP-адрес сервера для пересылки DNS-запросов.

   Примечание. Если вы хотите добавить IP-адреса нескольких серверов, необходимо вводить IP-адреса через пробел.

IP-адрес сервера для пересылки DNS-запросов добавлен.

6.3. Настройка DNS-сервера предприятия

Для отображения графического интерфейса продуктов необходимо на DNS-сервере предприятия добавить доменную зону gossopka.local и указать записи типа "A" для доменных имен продуктов системы:

— siem.gossopka.local для PT MaxPatrol SIEM;

— ms.gossopka.local для PT MS;

— nad.gossopka.local для PT NAD;

— dc.gossopka.local для "ПТ ВЦ".

Примечание. IP-адреса, соответствующие доменным именам продуктов, вы можете посмотреть в интерфейсе встроенного конфигуратора (см. раздел 6.2.2).

6.4. Проверка корректности интеграции

► Чтобы проверить корректность интеграции PT Platform 187 с ИТ-инфраструктурой предприятия,

в адресной строке браузера для каждого из продуктов PT Platform 187 введите доменное имя, определенное в разделе Настройка DNS-сервера предприятия (см. раздел 6.3).

На странице браузера отобразится интерфейс единой системы аутентификации PT IAM. Если интерфейс PT IAM отсутствует на странице браузера, PT Platform 187 интегрирован некорректно, и вам необходимо обратиться в службу технической поддержки.

7. Обновление продуктов, входящих в состав PT Platform 187

PT Platform 187 — программно-аппаратный комплекс, состоящий из пяти продуктов. Для взаимной интеграции продуктов в составе комплекса важна их версионность.

> Внимание! Не допускается автоматическое обновление до новой версии продуктов в составе комплекса. Перед обновлением одного или нескольких продуктов в составе комплекса обязательно обратитесь к вендору. Вендор сообщит вам, возможно ли обновление, а также, если необходимо, предоставит документацию для обновления.

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 на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

8.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по телефону +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языках.

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 5).

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

Таблица 5. Время реакции на запрос и время его обработки

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

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
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.

Приложение А. Роли специалистов, обслуживающих информационную защиту объекта КИИ

В таблице описаны роли и функции специалистов, обслуживающих информационную защиту объекта КИИ.

Таблица 6. Список ролей

Номер	Роль	Функции
Специалисты первой линии		
1.1	Специалист по взаимодействию с персоналом и пользователями	Прием сообщений персонала информационных ресурсов, подготовка информации для ГосСОПКА, взаимодействие с ГосСОПКА
1.2	Специалист по обнаружению компьютерных атак и инцидентов	Анализ событий безопасности, регистрация инцидентов
1.3	Специалист по обслуживанию технических и программных средств	Обеспечение функционирования технических и программных средств для функционирования PT Platform 187
Специалисты второй линии		
2.1	Специалист по оценке защищенности	Проведение инвентаризации информационных ресурсов, анализ выявленных уязвимостей и угроз, установление соответствия требований по информационной безопасности принимаемым мерам
2.2	Специалист по ликвидации последствий инцидентов информационной безопасности	Координация действий при реагировании на инциденты
2.3	Специалист по установлению причин инцидентов информационной безопасности	Установление причин инцидентов, анализ последствий инцидентов
Специалисты третьей линии		
3.1	Аналитик-методист	Анализ информации, предоставляемой специалистами первой и второй линий; разработка нормативных документов и методических рекомендаций по выполнению функций сегмента ГосСОПКА; разработка рекомендаций по доработке нормативных и методических документов по вопросам информационной безопасности

3.2	Технический эксперт	Экспертная поддержка в соответствии со специализацией (например, вредоносное программное обеспечение, настройка средств защиты, применение специализированных технических средств, оценка защищенности)
3.3	Юрист	Нормативно-правовое сопровождение деятельности сегмента ГосСОПКА
3.4	Руководитель	Управление деятельностью сегмента ГосСОПКА

О компании

"Позитив Текнолоджиз" уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявить, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга "Эксперт-400".

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com