Positive Technologies Platform 187

Версия 1.153

Руководство оператора

POSITIVE TECHNOLOGIES

© АО "Позитив Текнолоджиз", 2020.

Настоящий документ является собственностью АО "Позитив Текнолоджиз" (далее также — "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: 09.10.2020

Версия документа: 1 (черновик)

Содержание

1. Об этом документе

Руководство оператора содержит пошаговые инструкции и справочную информацию об использовании PT Platform 187 для защиты и управления информационными активами организации. В руководстве вы также найдете инструкции по настройке ключевых и дополнительных функций продукта для выполнения конкретных задач. Руководство не содержит инструкций по установке, первоначальной настройке и администрированию PT Platform 187.

Руководство адресовано руководителям и специалистам, ответственным за обеспечение информационной безопасности, контроль и расследование инцидентов.

Комплект документации PT Platform 187 включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации.
- 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.

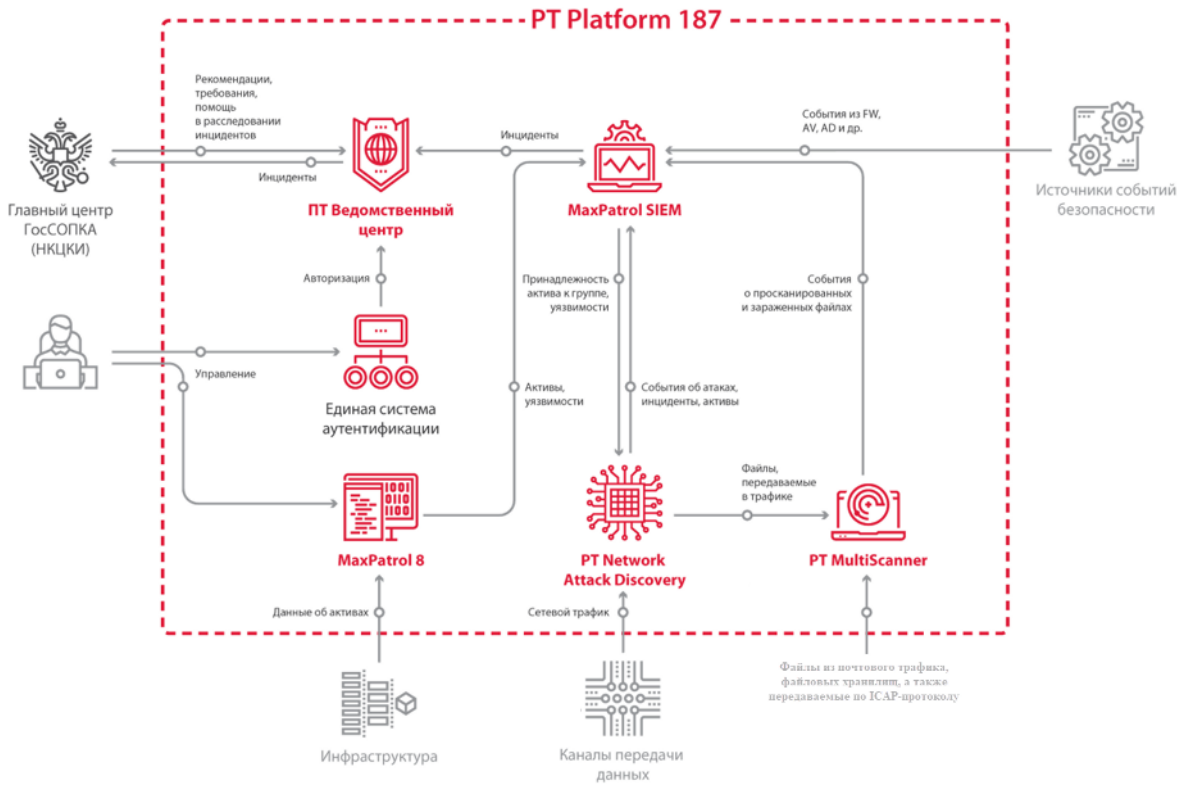

Рисунок 1. Схема взаимодействия продуктов в PT Platform 187

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.

4. Вход в PT Platform 187

Вход во все продукты, входящие в состав PT Platform 187, кроме MaxPatrol, осуществляется с помощью сервиса управления пользователями и доступом Positive Technologies Identity and Access Management (PT IAM). PT IAM обеспечивает механизм единого входа (технология single sign-on) в приложения "Позитив Текнолоджиз".

Перед доставкой в вашу организацию аппаратного обеспечения с установленным на него PT Platform 187, вам предоставляют для заполнения анкету для создания пилотной зоны комплексной системы обеспечения информационной безопасности PT Platform 187. В этом документе к моменту доставки аппаратного обеспечения с установленным на него PT Platform 187 сотрудники "Позитив Текнолоджиз" предоставляют:

— имя пользователя и пароль для входа в MaxPatrol;

— ссылка для входа в интерфейс PT MaxPatrol SIEM, из главного меню которого вы сможете переходить в интерфейс других продуктов PT Platform 187 (см. раздел 3);

— информация о типе учетной записи (локальная или доменная);

— логин и пароль вашей учетной записи пользователя.

Примечание. Убедитесь, что в браузере разрешены всплывающие окна, а также отключена функция Compatibility view для браузеров Microsoft Edge и Microsoft Internet Explorer.

► Чтобы войти в PT MaxPatrol SIEM:

1. В адресной строке браузера введите ссылку для входа в интерфейс PT MaxPatrol SIEM.

   Откроется страница входа в PT MC.

2. Выполните одно из следующих действий:

   - Если вы выполняете вход под локальной учетной записью, то на вкладке **Локальный** укажите логин учетной записи.
   - Если вы выполняете вход под доменной учетной записью, то на вкладке **LDAP** укажите логин доменной учетной записи.

3. В поле **Пароль** введите пароль вашей учетной записи.

   Примечание. Стандартная сессия пользователя в PT Platform 187 длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

4. Нажмите кнопку **Войти**.

PT IAM проверяет введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница с системным дашбордом PT MaxPatrol SIEM. Если вы указали неверные данные, отобразится сообщение об ошибке.

Главное меню PT MaxPatrol SIEM содержит пункты с названиями продуктов, входящих в состав PT Platform 187.

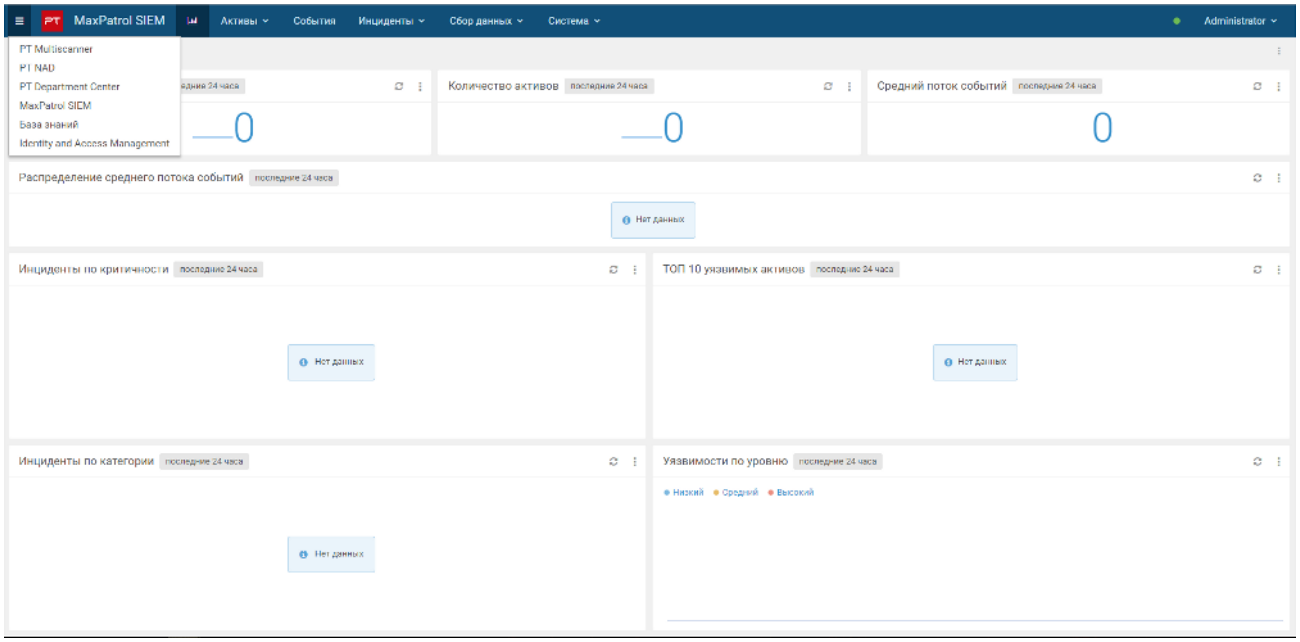

Рисунок 2. Главное меню PT MaxPatrol SIEM

► Чтобы перейти в интерфейс нужного продукта,

в главном меню PT MaxPatrol SIEM выберите пункт с названием продукта.

Переход в интерфейс продукта выполнен.

► Чтобы войти в консоль MaxPatrol:

1. По нажатию напрямую или на ярлык исполняемого файла `PTConsole` запустите консоль MaxPatrol.

   Откроется окно **Соединение**.

2. Введите имя пользователя и пароль.
3. Нажмите **Подключиться**.

Вход в консоль выполнен.

5. Требования по обеспечению безопасности объектов КИИ

В таблице отображены требования, которые необходимо решать согласно федеральному закону от 26.07.2017 № 187-ФЗ, и продукты, входящие в состав PT Platform 187, выполняющие эти требования. Наименования и идентификаторы требований взяты из приложения к требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом ФСТЭК России от 26 декабря 2017 г. № 239.

Таблица 1. Требования ФЗ от 26.07.2017 № 187-ФЗ и продукты "Позитив Текнолоджиз"

ID требования	Требование	Продукт
Аудит безопасности		
АУД.1	Инвентаризация информационных ресурсов	MaxPatrol, MaxPatrol SIEM
АУД.2	Анализ уязвимостей и их устранение	MaxPatrol
АУД.4	Регистрация событий безопасности	MaxPatrol SIEM
АУД.5	Контроль и анализ сетевого трафика	MaxPatrol SIEM, PT NAD
АУД.6	Защита информации о событиях безопасности	MaxPatrol SIEM
АУД.7	Мониторинг безопасности	MaxPatrol SIEM
АУД.8	Реагирование на сбои при регистрации событий безопасности	MaxPatrol SIEM
АУД.10	Проведение внутренних аудитов	MaxPatrol
АУД.11	Проведение внешних аудитов	MaxPatrol
Реагирование на компьютерные инциденты		
ИНЦ.1	Выявление компьютерных инцидентов	MaxPatrol SIEM
ИНЦ.2	Информирование о компьютерных инцидентах	MaxPatrol SIEM
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	MaxPatrol SIEM
Предотвращение вторжений (компьютерных атак)		
СОВ.1	Обнаружение и предотвращение компьютерных атак	PT NAD
СОВ.2	Обновление базы решающих правил	PT NAD
Антивирусная защита		
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	PT MS

ID требования	Требование	Продукт
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов	PT MS
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	PT MS
АВЗ.5	Использование средств антивирусной защиты различных производителей	PT MS
Защита информационной (автоматизированной) системы и ее компонентов		
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")	PT MS

6. Инвентаризация и анализ уязвимости активов объекта КИИ

Инвентаризация — сбор сведений об активах с целью получить представление об ИТ-инфраструктуре объекта КИИ. Анализ данных об активах и связях между ними помогает принимать решения по управлению ИТ-инфраструктурой.

Актив — базовая единица, которая представляет собой сканируемый сетевой узел.

После инвентаризации активов требуется анализ их уязвимости с целью предупредить нежелательные воздействия на активы.

Инвентаризацию активов и анализ их уязвимости обеспечивают продукты PT MaxPatrol SIEM и MaxPatrol.

Для сбора информации об активах ИТ-инфраструктуры средствами PT MaxPatrol SIEM, пользователь создает задачу для инвентаризации активов и настраивает расписание ее запуска. Пользователь использует тип задачи Сбор данных, предварительно создает и настраивает профиль для сбора данных об активах.

> **Примечание.** Подробнее читайте в разделе про работу с активами в Руководстве оператора PT MaxPatrol SIEM.

Для сбора информации об активах ИТ-инфраструктуры средствами MaxPatrol, пользователь создает задачу инвентаризации и настраивает расписание ее запуска. В качестве примера параметров задачи пользователь использует предустановленный профиль сканирования (Pentest) Inventory.

Сбор с помощью MaxPatrol данных об уязвимостях активов и соответствии активов требованиям политик и стандартов безопасности состоит из этапов:

1. Создание задачи поиска уязвимостей и настройка расписания ее запуска. В качестве примера параметров задачи используются предустановленные профили сканирования на уязвимости, в названии которых присутствует слово scan. Рекомендуется запускать задачу с периодичностью раз в месяц.
2. Создание задачи для контроля соблюдения требований политик и стандартов безопасности, предъявленных к объекту КИИ. В качестве примера параметров задачи используется предустановленный профиль сканирования (Pentest) PCI DSS ASV. Рекомендуется запускать задачу с периодичностью раз в квартал.

Подробнее о создании, планировании и запуске задач читайте в Справке и Руководстве по быстрому старту для системы MaxPatrol.

> **Примечание.** Эти документы хранятся в подкаталоге doc установочного каталога системы (например, `C:\Program Files\Positive Technologies\ MaxPatrol\doc`).

7. Антивирусная защита и предотвращение атак

Антивирусную защиту и предотвращение атак в объектах КИИ обеспечивают продукты PT MS и PT NAD.

PT NAD — это программно-аппаратный комплекс, который захватывает и анализирует сетевой трафик, чтобы выявить аномальную сетевую активность и сложные целенаправленные атаки в сетевых взаимодействиях и заблокировать такие взаимодействия.

PT NAD извлекает из сетевого трафика все файлы и передает на антивирусную проверку в PT MS.

PT MS — это программный комплекс, предназначенный для проверки файлов и электронных писем на предмет угрозы информационной безопасности. С помощью PT MS пользователи и операторы безопасности могут получить оценку опасности, исходящей от файлов, получаемых извне информационной системы либо уже находящихся внутри нее.

Передача в PT MS файлов, извлеченных из сетевого трафика с помощью PT NAD, настроена по умолчанию. Подробнее о настройке передачи файлов из сетевого трафика в PT MS читайте в разделе про добавление источников для сканирования в Руководстве администратора PT MS.

8. Сбор и анализ событий безопасности

Для сбора и анализа событий безопасности рекомендуем использовать PT MaxPatrol SIEM. Система обеспечивает комплексный мониторинг информационной безопасности ИТ-инфраструктуры объекта КИИ, анализирует события безопасности из различных источников и выявляет инциденты.

Как источники, передающие данные о событиях безопасности в PT MaxPatrol SIEM, в составе PT Platform 187 работают:

— PT NAD интегрирован с PT MaxPatrol SIEM с целью обмена данными о сессиях и атаках. В PT NAD на основе сессий и атак вы можете инициировать создание инцидента в PT MaxPatrol SIEM.

  Подробнее читайте в разделе про создание инцидента на основе сессий и атак в Руководстве оператора PT NAD.

— PT MS может выступать в качестве источника сообщений о событиях безопасности для системного журнала syslog. Для передачи сообщений системного журнала syslog в PT MaxPatrol SIEM в настройках PT MS требуется указать PT MaxPatrol SIEM в качестве внешнего syslog-сервера.

  Подробнее читайте в разделе про настройку передачи сообщений в системный журнал в Руководстве администратора PT MS.

— MaxPatrol интегрирован с PT MaxPatrol SIEM с целью передачи данных об активах и уязвимостях активов.

9. Работа с инцидентами информационной безопасности

Инцидент информационной безопасности (также инцидент) — это одно или несколько нежелательных или неожиданных событий, которые могут повлиять на информационную безопасность организации.

Примерами инцидентов ИБ могут служить несанкционированное изменение данных, установка запрещенного ПО, обнаружение вируса, сканирование сет, спам, утечка данных.

Для работы с инцидентами предназначены системы "ПТ ВЦ" и PT MaxPatrol SIEM.

"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.

Процесс работы с инцидентами средствами PT MaxPatrol SIEM состоит из следующих этапов:

1. Выявление инцидентов.
2. Приоритизация инцидентов.
3. Анализ инцидентов.
4. Расследование инцидентов.

Подробнее о работе с инцидентами средствами PT MaxPatrol SIEM читайте в Руководстве оператора PT MaxPatrol SIEM.

Подробнее о работе с инцидентами средствами "ПТ ВЦ" читайте в Руководстве оператора "ПТ ВЦ".

В этом разделе

9.1. Выявление инцидентов

Этап выявления инцидентов необходимо, чтобы узнать о появлении инцидента (если он создан автоматически) или, если вы обнаружили его самостоятельно, внести информацию о нем в "ПТ ВЦ".

Источником информации об инцидентах для "ПТ ВЦ" является система PT MaxPatrol SIEM. При возникновении события безопасности инцидент создается автоматически на основе информации, полученной из PT MaxPatrol SIEM. Вы узнаете об инциденте из уведомления, пришедшего на вашу электронную почту. Статус созданного в системе инцидента — **Новый**. Вы можете просматривать карточку инцидента в "ПТ ВЦ" и из нее переходить в карточку инцидента в PT MaxPatrol SIEM.

Если событие безопасности произошло в системе, информация о которой отсутствует в PT MaxPatrol SIEM, или если о событии сообщил пользователь, то инцидент необходимо создавать вручную в "ПТ ВЦ" .

Далее следует приоритизировать имеющиеся в системе инциденты.

9.2. Приоритизация инцидентов

► Чтобы выбрать инциденты, которые вам нужно взять в работу в первую очередь:

1. Отсортируйте и отфильтруйте инциденты с помощью имеющихся в "ПТ ВЦ" возможностей:
   - Если необходимо, отсортируйте инциденты по параметрам, отображающимся в рабочей области. Например, по приоритету, дате обновления, статусу.
   - Если необходимо, отсортируйте инциденты с помощью фильтров по группе, субъектам, объектам и ИТС, отображающихся в панели **Группы**.
2. Выполните диагностику инцидентов. В ходе диагностики вы принимаете решение о том, нужен ли дальнейший анализ и расследование инцидента:
   - Если инцидент является ложным срабатыванием, вы изменяете его статус с **Новый** на **Закрыт**. Инцидент будет храниться в системе со статусом **Закрыт (ложное срабатывание)**, изменение этого статуса невозможно.
   - Если инцидент не является ложным срабатыванием, вы изменяете его статус с **Новый** на **Утвержден**.

Инциденты выбраны.

Далее следует проанализировать инциденты.

9.3. Анализ инцидентов

► Чтобы расширить контекст инцидента и принять решение, нужно ли дальнейшее расследование:

1. Проанализируйте связи инцидента; события и активы, привязанные к инциденту; данные из карточки.
2. Решите, нужно ли дальнейшее расследование:
   - Если инцидент был разрешен без вашего участия (например, был создан инцидент **Обнаружение вируса**, но к этапу анализа антивирус уже успел удалить вредоносное ПО), измените статус инцидента с **Утвержден** на **Закрыт**.
   - Если нужно дальнейшее расследование, измените статус инцидента с **Утвержден** на **В работе**.

Решение принято.

Далее следует проводить расследование инцидентов со статусом **В работе**.

9.4. Расследование инцидентов

► Чтобы определить источник угроз, выявить обстоятельства, которые привели к возникновению инцидента, собрать доказательства инцидента, дать рекомендации по устранению инцидента и закрыть инцидент:

1. Типизируйте инцидент. Оцените ситуацию и предварительно присвойте инциденту тип на основе информации, доступной вам на момент выявления инцидента: например, **Эксплуатация уязвимостей** или **Запрещенный контент**.
2. Локализуйте инцидент:
   - Если источником информации об инциденте является PT MaxPatrol SIEM, перейдите в карточку инцидента в PT MaxPatrol SIEM. В карточке инцидента просмотрите топологию инцидента и достижимости, чтобы определить, какие активы вовлечены в инцидент.
   - Если инцидент создан вручную в "ПТ ВЦ", информацию о вовлеченных в инцидент активах просмотрите в карточке инцидента в "ПТ ВЦ".
   - Поставьте задачи по инциденту. Вы можете поставить задачу на другого сотрудника, чтобы привлечь его к расследованию инцидента, сбору доказательств по инциденту или восстановлению работоспособности системы. В рамках расследования каждого инцидента вы можете создавать несколько задач.
   - Проконтролируйте выполнение задач по инциденту. После выполнения все задачи, относящиеся к инциденту, должны иметь статус **Закрыта**.

3. Разработайте план для предотвращения повторных инцидентов. После того, как вы исследовали все обстоятельства инцидента и устранили его последствия, вам нужно разработать план и дать рекомендации вовлеченным в инцидент сотрудникам, чтобы предотвратить повторное возникновение выявленного инцидента. Затем измените статус инцидента с **В работе** на **Разрешен**.
4. Проконтролируйте исполнение рекомендаций:
   - Если ваши рекомендации выполнены, а инцидент и последствия устранены, измените статус инцидента с **Разрешен** на **Закрыт**. Принятые меры по инциденту зафиксируйте в карточке инцидента.
   - Если ваши рекомендации не выполнены либо принятых мер оказалось недостаточно и инцидент возникает повторно, измените статус инцидента с **Разрешен** на **В работе**.

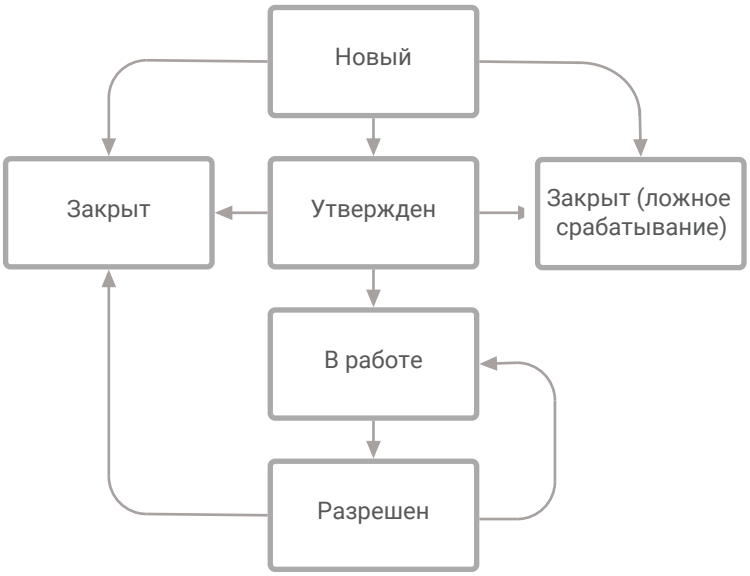

Рисунок 3. Статусная модель инцидента

Подробнее о средствах "ПТ ВЦ" для работы с инцидентами читайте в руководстве оператора "ПТ ВЦ".

10. 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

10.1. 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.

10.2. 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.

10.3. 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.

10.4. 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

10.4.1. 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.

10.4.2. 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.

10.4.3. Время реакции и приоритизация запросов

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

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

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 2).

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

Таблица 2. Время реакции на запрос и время его обработки

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта 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).

10.4.4. 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 3. 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