MaxPatrol EPP версия 8.3

Начало работы

Дата редакции документа: 01.11.2025

Содержание

1. Об этом документе

Это руководство содержит информацию и инструкции для первоначальной настройки MaxPatrol Endpoint Protection Platform (далее также — MaxPatrol EPP).

Комплект документации MaxPatrol EPP включает в себя следующие документы:

— Этот документ.

— Руководство администратора — содержит справочную информацию и инструкции по развертыванию, настройке и администрированию MaxPatrol EPP.

— Руководство разработчика — содержит справочную информацию и инструкции для специалистов, разрабатывающих модули агентов в MaxPatrol EPP.

2. О MaxPatrol EPP

MaxPatrol Endpoint Protection Platform — система, предназначенная для защиты конечных устройств от киберугроз. Собирая и анализируя данные из множества систем, MaxPatrol EPP выявляет в IT-инфраструктуре организации сложные целевые атаки и автоматически реагирует на них. MaxPatrol EPP встроен в экосистему продуктов Positive Technologies и позволяет:

— отправлять данные о системных событиях и событиях ИБ в MaxPatrol 10;

— отправлять подозрительные файлы на проверку в PT Sandbox и использовать полученные вердикты одновременно на всех конечных устройствах;

— запускать на конечных устройствах сканирование в режиме аудита и отправлять результаты в MaxPatrol VM.

При обнаружении угроз MaxPatrol EPP имеет возможность выполнить следующие автоматические действия:

— удалить файл;

— завершить один или несколько процессов;

— заблокировать сетевой трафик;

— заблокировать учетную запись;

— запустить проверку файлов и процессов на основе YARA-правил;

— отправить файл на проверку в PT Sandbox;

— запустить сканирование в режиме аудита и отправить результаты в MaxPatrol VM;

— заблокировать все сетевые соединения по IP-адресу;

— перенаправить DNS-запросы на IP-адрес;

— изолировать файл в зашифрованном хранилище.

Кроме того, администратор или оператор системы может в любой момент времени вручную запустить на конечном устройстве реагирование на угрозу.

3. Архитектура и алгоритм работы MaxPatrol EPP

MaxPatrol EPP состоит из серверной части и агентов, устанавливаемых на конечные устройства. Серверная часть MaxPatrol EPP состоит из двух программных компонентов — управляющего сервера и сервера агентов.

Управляющий сервер — основной компонент системы, который позволяет конфигурировать ее через веб-интерфейс. Сервер агентов — приложение для управления агентами и модулями, а также для взаимодействия с внешними системами (MaxPatrol SIEM, MaxPatrol VM, PT Sandbox, syslog-сервер).

Агент — приложение, которое устанавливается на конечное устройство для обеспечения работы модулей и связи с сервером агентов. Модуль — приложение, которое запускается на конечном устройстве для выполнения основных функций продукта.

Существуют две конфигурации MaxPatrol EPP — односерверная и многосерверная. Многосерверную конфигурацию вы можете использовать для распределения нагрузки при большом количестве конечных устройств в вашей организации. В этой конфигурации на основном сервере устанавливаются все компоненты, а на других только сервер агентов, СУБД PostgreSQL и объектное хранилище MinIO.

Алгоритм работы MaxPatrol EPP:

1. Сервер агентов передает на агенты модули и их конфигурацию.
2. Модули доставки и установки устанавливают и настраивают приложения на конечном устройстве, например Sysmon.
3. Модули сбора собирают данные о системных событиях, кэшируют их в памяти агента, передают в модули обнаружения и при необходимости на syslog-сервер или в MaxPatrol SIEM.
4. Модули обнаружения анализируют файлы, процессы, собранные события, обнаруживают подозрительную активность на конечном устройстве — и регистрируют события ИБ.
5. Модули реагирования пресекают подозрительную и вредоносную активность, выполняя действия в соответствии с политикой или по команде пользователя.
6. Модули интеграции обеспечивают интеграцию с внешними системами.
7. Данные о событиях ИБ кэшируются в памяти агента и пересылаются на сервер агентов, в базу данных MaxPatrol SIEM или на syslog-сервер.
8. Агент передает метрики и данные трассировки на сервер агентов.
9. Управляющий сервер получает обновления продукта и пакетов экспертизы с сервера обновлений.

Взаимодействие компонентов

При обычной установке управляющий сервер в системе один, а серверов агентов может быть несколько. При установке в отказоустойчивом кластере компонент `api` управляющего сервера может быть установлен на нескольких серверах. Компоненты Observability для снижения сетевого трафика могут быть установлены на одних серверах с серверами агентов.

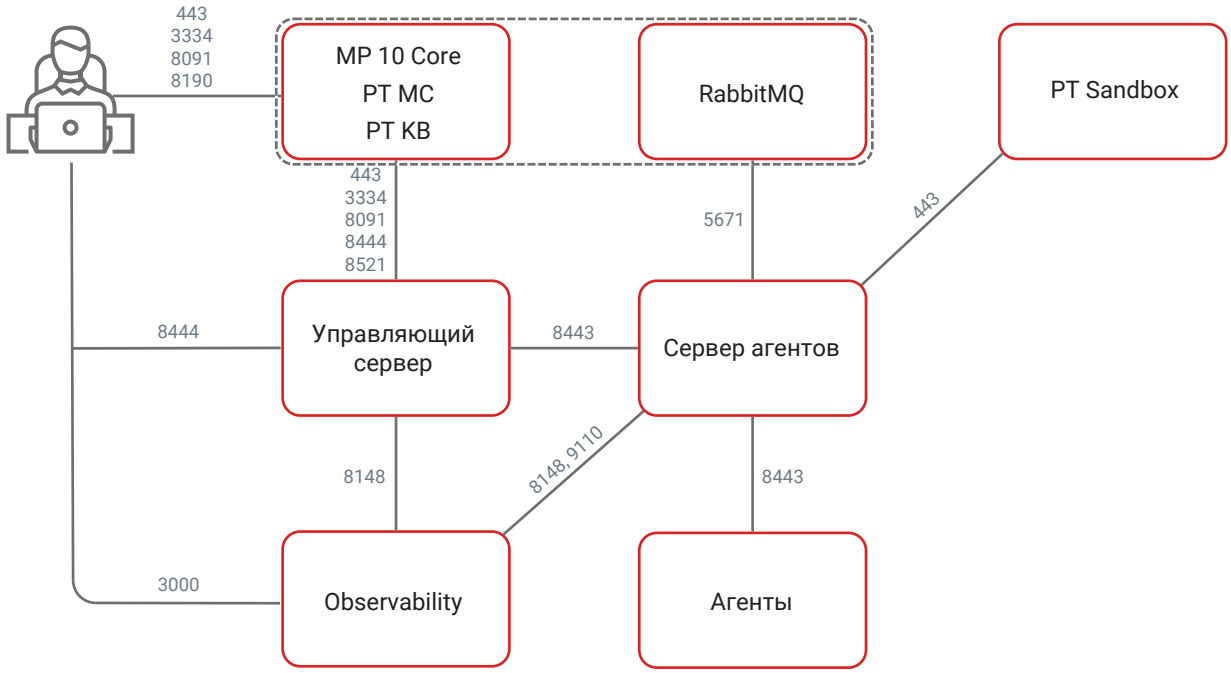

Рисунок 1. Взаимодействие компонентов MaxPatrol EPP

Для обеспечения сетевого взаимодействия компонентов MaxPatrol EPP должны быть доступны перечисленные ниже порты.

Примечание. Если какие-либо компоненты MaxPatrol EPP расположены на одном сервере, то обеспечивать внешнюю доступность портов при их взаимодействии необязательно. Например, при установке всех компонентов на один сервер открывать порты 8148, 8443, 9047, 9110 не требуется.

Примечание. В таблице приведены порты, используемые по умолчанию.

Таблица 1. Компоненты и порты взаимодействия

Источник	Получатель	Протокол	TCP-порт
Управляющий сервер	Сервер агентов	HTTPS	8443
Управляющий сервер	MP 10 Core	HTTPS	443, 3334, 8521

Источник	Получатель	Протокол	TCP-порт
Управляющий сервер	Компонент Observability	gRPC	8148
Управляющий сервер	Сервис пользовательской экспертизы (компонент `custom_expertise`)	HTTPS	9047 (при установке в отказоустойчивом кластере)
MP 10 Core	Управляющий сервер	HTTPS	8444
Сервер агентов	PT Sandbox	HTTPS	443
Сервер агентов	Сервер RabbitMQ	AMQP	5671
Сервер агентов	Компонент Observability	gRPC	8148
Сервер агентов	Компонент Observability	HTTPS	9110
Агент	Сервер агентов	WSS	8443
Рабочая станция пользователя	Управляющий сервер	HTTPS	8444
Рабочая станция пользователя	Управляющий сервер	SSH	22 (при необходимости для удаленного доступа по протоколу SSH)
Рабочая станция пользователя	Сервер агентов	SSH	22 (при необходимости для удаленного доступа по протоколу SSH)
Рабочая станция пользователя	MP 10 Core	HTTPS	443, 3334, 8091, 8190, 8444
Рабочая станция пользователя	Компонент `observability`	HTTPS	3000 (веб-интерфейс Grafana)
Внешние системы (взаимодействие через публичный API)	Управляющий сервер	HTTPS	8444
Сервер с ролью Deployer (если эта роль установлена отдельно от компонента MP 10 Core)	Управляющий сервер Сервер агентов Компонент Observability	TCP	22

4. Вход в MaxPatrol EPP через PT MC

Сервис управления пользователями и доступом PT MC обеспечивает механизм единого входа (технология single sign-on) в приложения Positive Technologies. Перед входом в MaxPatrol EPP запросите у администратора PT MC логин и пароль вашей учетной записи и убедитесь, что в браузере разрешены всплывающие окна.

► Чтобы войти в MaxPatrol EPP:

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

   Откроется страница входа в PT MC.

2. Выполните одно из следующих действий:

   - Если вы входите под локальной учетной записью, то на вкладке **Локальный** укажите логин локальной учетной записи.
   - Если вы входите 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 MaxPatrol EPP длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

4. Нажмите **Войти**.

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

5. Интерфейс MaxPatrol EPP

После входа в веб-интерфейс открывается страница **Агенты**.

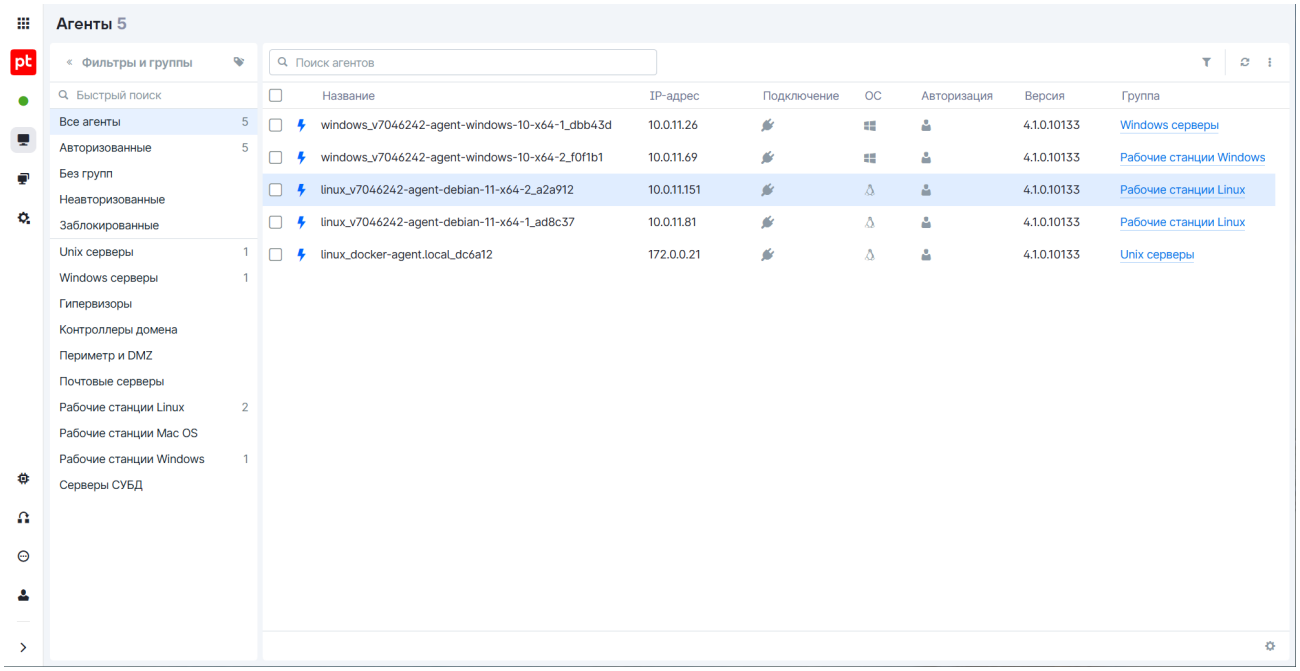

Рисунок 2. Страница **Агенты**

Веб-интерфейс MaxPatrol EPP состоит из главного меню, панели инструментов и рабочей области. Главное меню содержит раскрывающийся список для выбора сервера агентов (если их в системе несколько), разделы для перехода к страницам продукта, а также кнопку для перехода к другим приложениям.

Панель инструментов содержит кнопки. С их помощью вы можете выполнять действия (в том числе групповые) с данными, представленными в рабочей области.

6. Порядок настройки MaxPatrol EPP

После установки MaxPatrol EPP и агентов вам нужно:

1. Авторизовать агенты (см. раздел 7). При авторизации агент добавляется в группу. Вы можете использовать стандартные группы или добавить свои.
2. Создать политики с помощью встроенных шаблонов (см. раздел 8).
3. Настроить модули в политиках (см. раздел 9). В частности, вам нужно настроить интеграцию с PT Sandbox, а также модули «Коррелятор» и «WinEventLog: сбор данных из журнала событий Windows».
4. В параметрах политики назначить автоматические действия (см. раздел 10), которые будут выполняться при регистрации событий ИБ.
5. Назначить политики на группы агентов (см. раздел 11). Сразу после назначения политик на агентах будут установлены и запущены модули.

7. Авторизация агента

После установки агента он отображается в MaxPatrol EPP со статусом **Неавторизован**. Для дальнейшей работы с агентом вам нужно авторизовать его. При авторизации агент добавляется в группу.

- Чтобы авторизовать агент:

  1. В главном меню выберите **Агенты**.
  2. Выберите фильтр **Неавторизованные**.
  3. Нажмите на название агента.
  4. Нажмите **Авторизовать**.
  5. Выберите группу, в которую вы хотите добавить агент.
  6. Нажмите **Применить**.

8. Создание политики

Вы можете создавать политики на базе шаблонов или пустые. В политиках, которые созданы на базе шаблонов, добавлены модули для решения определенных задач и настроены автоматические действия. Политики на базе шаблонов для обнаружения угроз или реагирования можно сразу использовать на агентах. В политиках с модулями интеграции вам предварительно нужно настроить подключение к внешним системам. После создания пустой политики вам нужно добавить в нее модули, сконфигурировать их (см. раздел 9) и настроить автоматические действия (см. раздел 10).

- Чтобы создать политику:

  1. В главном меню выберите **Политики**.
  2. Нажмите **Создать политику**.
  3. Выберите шаблон, на базе которого вы хотите создать политику.

     Примечание. Для создания пустой политики вы можете выбрать значение **Не выбран**.
  4. Введите название политики.
  5. Выберите версии модулей для автоматического обновления или отключите его.
  6. Выберите существующие метки для быстрого поиска политики или задайте свои.
  7. Нажмите **Создать**.

Вы также можете создавать копии существующих политик.

9. Информация о модулях и их настройка

Далее приведена подробная информация о модулях и даны инструкции по их настройке.

В этом разделе

9.1. Системные модули

В этом разделе приведена информация о системных модулях.

Ядро (внутренний сервис)

Этот модуль предоставляет библиотеку среды выполнения для работы модулей и является обязательным в системе.

Работа с файлами и процессами

Этот модуль предоставляет интерфейс для операций с файлами и процессами.

9.2. Модули доставки и установки

В этом разделе приведена информация по модулям доставки и установки.

В этом разделе

9.2.1. Установщик Sysmon

Модуль «Установщик Sysmon» устанавливает и конфигурирует утилиту Sysmon. Удаление модуля с агента не повлияет на конфигурацию Sysmon на конечном устройстве.

Внимание! Конфигурация утилиты Sysmon подготовлена экспертами Positive Technologies. При необходимости вы можете изменить конфигурацию под особенности вашей инфраструктуры. Исключение большого количества событий может существенно повлиять на работу модуля «Коррелятор».

Таблица 2. Параметры модуля «Установщик Sysmon»

Параметр или блок параметров	Описание
Заменить исполняемый файл Sysmon на агенте	Определяет, заменять ли исполняемый файл, если Sysmon уже установлен на конечном устройстве
Заменить файл конфигурации на агенте	Определяет, заменять ли файл конфигурации, если Sysmon уже установлен на конечном устройстве
Файл конфигурации	Файл конфигурации Sysmon, который будет использоваться на конечном устройстве

9.2.2. Установщик auditd

Модуль «Установщик auditd» устанавливает и конфигурирует компонент auditd. При удалении модуля с агента на конечном устройстве очищаются файлы с конфигурацией и правилами компонента.

Внимание! В CentOS Stream 10 невозможна установка компонента auditd с помощью модуля «Установщик auditd».

Примечание. Модуль «Установщик auditd» не рекомендуется использовать на узлах, где уже применяется другое ПО для управления правилами и конфигурацией компонента auditd.

Таблица 3. Параметры модуля «Установщик auditd»

Параметр или блок параметров	Описание
Правила	Правила обработки событий, содержимое файла `/etc/audit/audit.rules`
Конфигурация auditd	Конфигурация auditd, содержимое файла `/etc/audit/auditd.conf`
Заменить конфигурацию и правила auditd на агенте	Заменять ли файлы `audit.rules` и `auditd.conf` на конечном устройстве, если они отличаются от заданных в политике. Проверка выполняется каждые 10 минут

9.2.3. Конфигуратор аудита Windows

Модуль «Конфигуратор аудита Windows» настраивает расширенную политику аудита Windows на контроллерах доменов, серверах и рабочих станциях. Базовая конфигурация политик аудита в модуле подготовлена экспертами Positive Technologies. Такая конфигурация позволяет MaxPatrol EPP получать необходимую информацию для своевременного обнаружения и предотвращения атак на узлах. Модуль каждые 30 минут проверяет параметры политик аудита в операционной системе и обновляет их, если они отличаются от заданных в MaxPatrol EPP.

> **Внимание!** Перед использованием модуля нужно заранее определить инструмент управления конфигурацией расширенной политики аудита Windows. Если на узлах используется групповая политика, во избежание конфликтов конфигурации не рекомендуется устанавливать модуль «Конфигуратор аудита Windows».
>
> **Внимание!** Для работы модуля на агенте должен быть установлен модуль «Ядро (внутренний сервис)» (см. раздел 9.1).
>
> **Примечание.** Рекомендации по настройке политик аудита вы можете найти в документации Microsoft.

9.2.4. Доставщик антивирусных баз

Этот модуль доставляет антивирусные базы на конечное устройство и является обязательным для полноценной работы модуля «Антивирус» (см. раздел 9.2.4).

9.3. Модули сбора

В этом разделе приведена информация о модулях сбора.

В этом разделе

9.3.1. WinEventLog: сбор данных из журнала событий Windows

Модуль «WinEventLog: сбор данных из журнала событий Windows» передает данные из журнала событий Windows в модуль «Нормализатор» и сторонние системы.

► Чтобы настроить модуль «WinEventLog: сбор данных из журнала событий Windows»:

1. В главном меню выберите **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «WinEventLog: сбор данных из журнала событий Windows».
4. Если требуется, в блоке параметров **Каналы журналов** добавьте каналы журнала событий Windows, которые будут обрабатываться модулем.

   Например, `Microsoft-Windows-Sysmon/Operational`.
5. Если из канала необходимо обрабатывать только некоторые события, введите запрос на языке XPath 1.0 к структуре необработанного события.

   Например, если требуется обрабатывать только события с идентификаторами `4698` или `4654`, запрос должен быть следующим: `*[System[EventID=4698 or EventID=4654]]`.
6. Если из обработки необходимо исключить определенные события, которые записываются в канал, введите запрос на языке XPath 1.0 к структуре необработанного события.

   Например, если требуется исключить события, которые связаны с пользователем `Administrator`, запрос должен быть следующим: `*[EventData[Data='Administrator']]`.

   Примечание. Исключения добавляются только для тех событий, которые записываются в выбранный канал.
7. Нажмите **Сохранить**.

9.3.2. ETW: трассировка событий Windows

Модуль «ETW: трассировка событий Windows» запускает в Windows сеанс трассировки событий и подписывается на события трех провайдеров: Microsoft-Windows-WMI-Activity, Microsoft-Windows-Kernel-Process и Microsoft-Windows-Win32k. Необработанные данные передаются в модуль «Нормализатор», а также при необходимости в MaxPatrol SIEM и в сторонние системы. Собираемые события позволяют получить расширенную информацию об активности в операционной системе и выявить в ней подозрительное и вредоносное поведение.

Базовая конфигурация модуля подготовлена экспертами Positive Technologies. При необходимости в параметрах модуля вы можете отменить подписку на определенные типы событий или настроить их фильтрацию по идентификаторам.

Если модуль по каким-либо причинам не смог запустить сеанс трассировки событий, то попытка будет повторена через 30 секунд. После пяти неудачных попыток в системе будет зарегистрировано событие «Не удалось запустить сеанс трассировки событий (ETW)».

Внимание! Для работы модуля на агенте должен быть установлен модуль «Ядро (внутренний сервис)» (см. раздел 9.1).

9.3.3. Сбор данных из файлов журналов

Модуль «Сбор данных из файлов журналов» передает данные из заданных журналов в модуль «Нормализатор» и сторонние системы. Список журналов, которые будут обрабатываться модулем, задается в параметрах модуля. Поддерживаются файлы журналов из Linux и Windows. Если вы хотите обрабатывать из журнала только некоторые события или, наоборот, исключить определенные события, вы можете сделать это с помощью регулярных выражений (regex).

Примечание. Журнал модуля на конечном устройстве может занимать до 2,5 ГБ.

Таблица 4. Параметры модуля «Сбор данных из файлов журналов»

Параметр или блок параметров	Описание
Путь к файлу	Полный путь к файлу журнала
Регулярное выражение для выбора событий	Определяет события, которые будут обрабатываться модулем
Регулярное выражение для исключений	Определяет события, которые будут исключаться модулем
Кодировка файла	Кодировка файла журнала: UTF-8, UTF-16BE или UTF-16LE
Разделитель строк	Символ или последовательность символов для определения конца строки в файле журнала. Для перевода строки в Linux обычно используется символ LF, в Windows — последовательность символов CR и LF

9.3.4. Сбор данных о состоянии системы

Модуль «Сбор данных о состоянии системы» собирает информацию о состоянии операционной системы агента в момент регистрации события ИБ или по запросу пользователя. Это помогает проанализировать ситуацию на конечном устройстве и выбрать подходящее реагирование. С помощью модуля можно создать дамп памяти процесса, а также получить списки:

- запущенных процессов;
- активных сетевых соединений;
- учетных записей;
- автозагрузки.

Таблица 5. Параметры модуля «Сбор данных о состоянии системы»

Параметр или блок параметров	Описание
Защищать архив паролем	Использовать ли пароль для архива с данными
Пароль для архива	Пароль, который будет установлен для скачанного архива с данными
Размер хранилища данных на сервере, МБ	Размер хранилища собранных данных (в мегабайтах) на сервере без учета дампов процессов. При заполнении хранилища из него будут удаляться самые старые данные
Размер хранилища дампов на агенте, МБ	Размер хранилища созданных дампов процессов на агенте (в мегабайтах). При заполнении хранилища из него будут удаляться самые старые дампы. После скачивания дампа он удаляется из хранилища на агенте
Размер хранилища дампов на сервере, МБ	Размер хранилища созданных дампов процессов на сервере (в мегабайтах). При заполнении хранилища из него будут удаляться самые старые дампы

9.3.5. Нормализатор

Модуль «Нормализатор» выполняет нормализацию необработанных событий от модулей «WinEventLog: сбор данных из журнала событий Windows», «ETW: трассировка событий Windows» и «Сбор данных из файлов журналов» для последующей обработки и анализа в других модулях и отправки в MaxPatrol SIEM. Системные события, для которых нет правил нормализации, будут отправлены в MaxPatrol SIEM в необработанном виде. Кроме того, в параметрах модуля вы можете полностью отключить нормализацию событий. В этом случае все события будут передаваться в необработанном виде и вы сможете нормализовать их в MaxPatrol SIEM собственными правилами.

> **Внимание!** Для работы некоторых модулей требуются нормализованные события. При отключении нормализации модули «Коррелятор» и «Обнаружение подозрительных файлов» работать не будут. Модуль «Проверка файлов по хеш-сумме» будет работать только по событиям ИБ от других модулей. Также невозможна отправка необработанных событий на syslog-сервер с помощью соответствующего модуля.

9.4. Модули обнаружения

В этом разделе приведена информация о модулях обнаружения.

В этом разделе

Коррелятор (см. раздел 9.4.1)

YARA-сканер (см. раздел 9.4.2)

Проверка файлов по хеш-сумме (см. раздел 9.4.3)

Обнаружение подозрительных файлов (см. раздел 9.4.4)

Антивирус (см. раздел 9.4.5)

9.4.1. Коррелятор

Модуль «Коррелятор» выполняет корреляцию потока событий от модуля «Нормализатор». При обнаружении вредоносных или подозрительных действий регистрирует события ИБ (корреляционные события). Кроме того, при регистрации определенных корреляционных событий в MaxPatrol 10 автоматически регистрируются инциденты. В системе есть два отдельных коррелятора для Windows и Linux.

Вы можете добавлять исключения для правил корреляций. Это позволит уменьшить количество ложных срабатываний правил, которые могут возникать из-за особенностей вашей инфраструктуры. Исключения реализуются двумя способами: с помощью табличных списков из PT KB и с помощью регулярных выражений (regex) в формате PCRE2 в параметрах модуля.

Исключения с помощью табличных списков

Если MaxPatrol EPP используется совместно с системой MaxPatrol 10, вы можете управлять исключениями в модуле «Коррелятор» с помощью стандартных табличных списков базы знаний PT KB: Common_blacklist_regex, Common_blacklist_value, Common_IP_Subnet_Whitelist, Common_whitelist_auto, Common_whitelist_auto_swap, Common_whitelist_auto_thresholds, Common_whitelist_for_labeling, Common_whitelist_for_labeling_regex, Common_whitelist_regex и Common_whitelist_value. После добавления записей в эти табличные списки они будут учтены модулем после установки пакета экспертизы в MaxPatrol SIEM и синхронизации с MaxPatrol EPP (выполняется автоматически каждые 30 минут). Подробная информация о работе с табличными списками в MaxPatrol 10 приведена в справке по этому продукту.

Примечание. Записи в табличные списки могут также добавляться на основе данных события ИБ. В этом случае для их актуализации в MaxPatrol EPP не требуется установка пакета экспертизы в MaxPatrol SIEM. При этом обновление данных на агенте может занять до 10 минут.

Примечание. Записи в остальных табличных списках будут обновляться при обновлении пакета экспертизы в MaxPatrol EPP.

При необходимости вместо стандартных табличных списков вы можете использовать собственные с такой же структурой (например, если у вас есть отдельный список с разрешенными IP-адресами и они не дублируются в стандартном списке). Для этого вам нужно выбрать пользовательский список вместо стандартного в параметрах модуля.

Исключения с помощью регулярных выражений

- Чтобы добавить исключение:

1. В главном меню выберите **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Коррелятор».
4. В блоке параметров **Список исключений** нажмите **Добавить**.
5. В поле **Переменные** укажите одну или несколько переменных для первого условия в регулярном выражении.

   В регулярном выражении указанные переменные будут разделяться логическим оператором ИЛИ. Например, если вы хотите исключить срабатывания правила корреляции на внутреннюю утилиту, вы можете указать переменные, в которых передается имя исполняемого файла: `object.fullpath`, `object.process.cmdline`, `object.name`.

   Внимание! Переменные `event_src.id`, `event_src.ip`, `event_src.rule`, `event_src.fqdn`, `event_src.hostname`, `event_src.host`, `recv_ipv4`, `recv_host` использовать для исключений невозможно.

   Примечание. Подробную информацию о событии модуля «Коррелятор» вы можете посмотреть на странице **События** в панели **Сводка**.
6. В поле **Регулярное выражение** введите регулярное выражение, которое будет применяться к списку заданных переменных.

   Например, вы можете ввести имя исполняемого файла вашей утилиты. В этом случае первое условие в исключении сработает, если хотя бы в одной заданной переменной будет содержаться указанное имя файла.

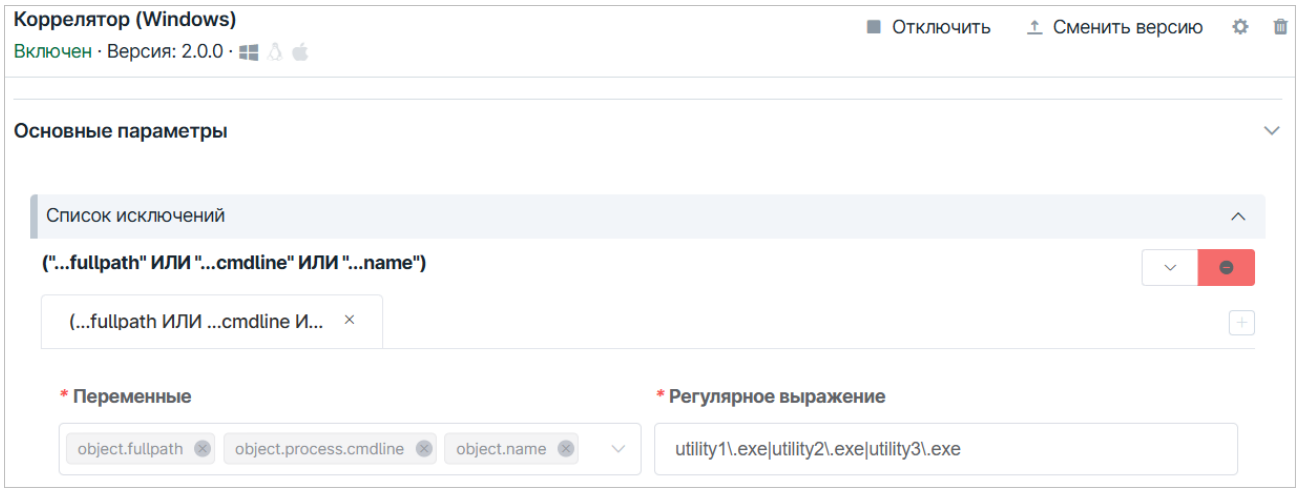

Рисунок 3. Добавление исключения

7. Если требуется, нажмите + и настройте второе условие, повторив шаги 5—6.

   В регулярном выражении условия будут разделяться логическим оператором И. Во втором условии вы можете указать правило, которое дает ложное срабатывание. Для этого в поле **Переменные** нужно ввести `correlation_name`, а в поле **Регулярное выражение** — имя правила.

8. Если требуется, настройте дополнительные условия.
9. Нажмите **Сохранить**.

Передача данных в модуль «Коррелятор»

Модуль «Коррелятор» использует для работы данные из журнала событий Windows. Для корректной работы модуля вам нужно:

- назначить на группу агентов с модулем «Коррелятор» политику с модулями «WinEventLog: сбор данных из журнала событий Windows» и «Установщик Sysmon»;
- добавить канал `Microsoft-Windows-Sysmon/Operational` в список каналов, обрабатываемых модулем «WinEventLog: сбор данных из журнала событий Windows» (см. раздел 9.3.1).

Передача данных в модуль «Коррелятор (Linux)»

Модуль «Коррелятор (Linux)» использует для работы данные из журналов auditd. Для корректной работы модуля вам нужно:

- вручную установить и настроить на конечных устройствах компонент auditd;
- назначить на группу агентов с модулем «Коррелятор (Linux)» политику с модулем «Сбор данных из файлов журналов».

Покрываемые техники MITRE ATT&CK

При настройке модулей «Коррелятор (Windows)» и «Коррелятор (Linux)» для каждого события отображаются покрываемые техники из матрицы MITRE ATT&CK. Это помогает правильно настроить автоматическое реагирование и выбрать одинаковые действия для одинаковых техник.

Вы также можете просмотреть всю матрицу MITRE ATT&CK, на которой отмечены техники, покрываемые MaxPatrol EPP. При необходимости вы можете отфильтровать техники по операционной системе, перейти к описанию техники или тактики на сайте attack.mitre.org, а также выгрузить матрицу в формате JSON или XLSX.

- Чтобы просмотреть покрываемые техники,

  в главном меню выберите **Система** → **Матрица MITRE ATT&CK**.

9.4.2. YARA-сканер

Модуль «YARA-сканер» выполняет сигнатурный анализ на основе YARA-правил. При обнаружении вредоносных или подозрительных файлов и процессов выносит вердикты и регистрирует события ИБ. Сканирование может запускаться вручную, автоматически по расписанию или при регистрации подходящего события. Если при запуске проверки по расписанию на агенте уже выполняется сканирование, проверка будет запущена после завершения всех текущих задач.

Частый запуск сигнатурного анализа файлов и процессов на основе правил YARA вызывает чрезмерное потребление ресурсов конечного устройства. Это может привести к увеличению продолжительности проверок, образованию очереди и, как следствие, медленному реагированию на угрозы.

Чтобы избежать таких ситуаций, в MaxPatrol EPP результаты проверок кэшируются. Срок хранения результатов сканирования файлов не ограничен, срок хранения результатов сканирования процессов вы можете задать в конфигурации политики. Перед запуском новой проверки MaxPatrol EPP проверяет сохраненные результаты и использует их, если такой файл или процесс уже проверялся. MaxPatrol EPP идентифицирует файлы по хеш-сумме, а процессы по идентификатору и пути к исполняемому файлу.

Таблица 6. Параметры модуля «YARA-сканер»

Параметр или блок параметров	Описание
Максимальный размер файла для проверки, МБ	Максимальный размер файла (в мегабайтах), которой может быть проверен модулем. Ограничение актуально: — при автоматическом реагировании — в этом случае в системе будет зарегистрировано событие «Не удалось проверить файл: превышен максимальный размер»; — ручной проверке, если проверяется более одного файла одновременно, — в этом случаи крупные файлы будут пропущены без регистрации события. Файл, размер которого превышает заданный, вы можете проверить, запустив вручную проверку только этого файла
Список исключений для проверок в Linux	Список файлов и каталогов, которые не будут проверяться модулем в Linux
Список исключений для проверок в Windows	Список файлов и папок, которые не будут проверяться модулем в Windows. Задать путь вы можете в форматах DOS и UNC, а также с помощью переменных окружения. **Примечание.** Агент MaxPatrol EPP запускается под системной учетной записью, поэтому значение переменной окружения `%userprofile%` — `C:\Windows\System32\config\systemprofile`

Параметр или блок параметров	Описание
Список исключений для YARA-правил	Список названий YARA-правил, которые не будут использоваться для проверок (значение параметра `rule_name`). Например, `tool_mem_ZZ_Emotet__Downloader__Stager`
Параметры быстрой проверки файлов в Linux	Список файлов и каталогов для быстрой проверки в Linux
Параметры быстрой проверки файлов в Windows	Список файлов и папок для быстрой проверки в Windows
Параметры быстрой проверки процессов в Linux	Список процессов для быстрой проверки в Linux
Параметры быстрой проверки процессов в Windows	Список процессов для быстрой проверки в Windows
Классы вредоносного ПО	Список классов вредоносного ПО, при обнаружении которых модуль вынесет вердикт «вредоносный файл». Не рекомендуется изменять стандартный список классов
Время хранения результатов сканирования процесса (в минутах)	Время хранения результатов сканирования процесса (в минутах). При перезагрузке модуля результаты сканирования очищаются
Максимальное количество используемых потоков при сканировании	Максимальное количество ядер процессора, которое модуль может задействовать для одной задачи сканирования
День недели	Дни недели, в которые будет запускаться проверка по расписанию
Месяцы	Месяцы, в которые будет запускаться проверка по расписанию
День месяца	Дни месяца, в которые будет запускаться проверка по расписанию
Время в часовом поясе агента	Время в часовом поясе агента, в которое будет запускаться проверки по расписанию. **Примечание.** Изменение часового пояса на агенте не повлияет на время запуска ближайшей запланированной проверки. Однако, это изменение будет учтено при запуске последующих проверок или после внесения изменений в расписание в модуле

Параметр или блок параметров	Описание
Область проверки	Область проверки по расписанию
Глубина проверки	Глубина проверки по расписанию: важные системные файлы и процессы (быстрая) или все файлы и процессы (полная)

См. также

Настройка автоматического реагирования (см. раздел 10)

9.4.3. Проверка файлов по хеш-сумме

Модуль «Проверка файлов по хеш-сумме» ищет хеш-суммы файлов (MD5 и SHA-256) в базе данных новых угроз. На такие угрозы еще не срабатывают YARA-правила и для них не написаны правила корреляции. Автоматическое действие проверки файла может быть назначено на подходящие события от модулей сбора. MaxPatrol EPP регулярно получает обновления базы данных новых угроз. Кроме того, вместо стандартной базы данных вы можете использовать собственные данные об угрозах из табличного списка.

Таблица 7. Параметры модуля «Проверка файлов по хеш-сумме»

Параметр или блок параметров	Описание
Максимальный размер файла для проверки, МБ	Максимальный размер файла, который может быть проверен (в мегабайтах). Ограничение относится только к автоматическому реагированию
Экспертиза	Определяет, какую экспертизу будет использовать модуль: стандартную или из табличного списка базы знаний PT KB. Применение экспертизы из табличных списков возможно, если MaxPatrol EPP используется совместно с системой MaxPatrol 10
Табличный список	Табличный список со значениями хеш-сумм подозрительных файлов. В табличном списке должны быть поля `hash_md5`, `hash_sha256` и `threat_type`. Например, подойдет список repListHashes. **Внимание!** Синхронизация табличных списков с PT KB выполняется раз в 30 минут. При создании нового списка в PT KB, он может быть не сразу доступен в MaxPatrol EPP. **Примечание.** В MaxPatrol EPP учитываются только 100 тысяч записей в табличном списке. Если новая версия модуля установлена в MaxPatrol EPP версии 8.1 или ниже, учитываться будут 10 тысяч записей

9.4.4. Обнаружение подозрительных файлов

Модуль «Обнаружение подозрительных файлов» анализирует нормализованные события и обнаруживает появление в системе подозрительных файлов. Файл считается подозрительным, если его расширение специально задано в конфигурации модуля, а также он был обнаружен в заданной папке или был создан заданным процессом.

Таблица 8. Параметры модуля «Обнаружение подозрительных файлов»

Параметр или блок параметров	Описание
Максимальный размер файла для проверки, МБ	Максимальный размер файла (в мегабайтах), который будет учитываться модулем
Правила обнаружения для Windows → Расширения	Список расширений файлов в Windows, которые будут учитываться модулем
Правила обнаружения для Windows → Системные папки	Системные папки Windows, в которых будет отслеживаться появление файлов
Правила обнаружения для Windows → Папки	Список папок в Windows, в которых будет отслеживаться появление файлов
Правила обнаружения для Windows → Процессы	Список процессов в Windows, которые будут отслеживаться на предмет создания файлов
Правила обнаружения для Linux → Расширения	Список расширений файлов в Linux, которые будут учитываться модулем
Правила обнаружения для Linux → Каталоги	Список каталогов в Linux, в которых будет отслеживаться появление файлов
Правила обнаружения для Linux → Процессы	Список процессов в Linux, которые будут отслеживаться на предмет создания файлов

9.4.5. Антивирус

Модуль «Антивирус» обнаруживает и обезвреживает вирусы и вредоносные программы в операционной системе. Проверка выполняется автоматически при операциях с файлами на конечном устройстве, а также может запускаться вручную, автоматически по расписанию или при регистрации подходящего события. При обнаружении угрозы модуль зарегистрирует событие, на которое может быть назначено автоматическое действие, например удаление файла. Кроме того, модуль может заблокировать операции с файлом (кроме его удаления) и попытаться его вылечить.

Модуль устанавливает на конечном устройстве службу и драйвер антивируса, которые работают независимо от соединения с сервером MaxPatrol EPP. Удалить антивирус на узле (см. раздел 9.4.5) можно только из интерфейса MaxPatrol EPP.

Внимание! Для полноценной работы антивируса на агенте должен быть установлен модуль «Доставщик антивирусных баз» (см. раздел 9.2.4).

Таблица 9. Параметры модуля

Параметр	Описание
Лечить файлы загрузочного сектора	Определяет, лечить ли зараженные файлы загрузочного сектора EFI (boot)
Лечить файлы	Определяет, лечить ли зараженные файлы
Устанавливать зависимости в Linux	Определяет, устанавливать или нет зависимости cc-multilib, libnotify, ayatana-app-indicator в Linux. Эти зависимости нужны для корректной работы модуля
Блокировать вредоносные файлы	Определяет, блокировать ли действия с зараженным файлом
Исключения для проверок → Глобальные	Список файлов и каталогов, которые не будут проверяться антивирусом при любых проверках. Каждый путь должен быть с новой строки и заканчиваться символом `;`
Исключения для проверок → В реальном времени	Список файлов и каталогов, которые не будут проверяться антивирусом во время операций с файлами на конечном устройстве. Каждый путь должен быть с новой строки и заканчиваться символом `;`
Исключения для проверок → По запросу	Список файлов и папок, которые не будут проверяться антивирусом при автоматическом реагировании, а также при проверках, запущенных вручную или по расписанию. Каждый путь должен быть с новой строки и заканчиваться символом `;`
Максимальный размер файлов для проверки, МБ	Максимальный размер файла (в мегабайтах), которой может быть проверен антивирусом
Запуск	Периодичность запуска проверки по расписанию
День недели	Дни недели, в которые будет запускаться проверка по расписанию
Месяцы	Месяцы, в которые будет запускаться проверка по расписанию
День месяца	Дни месяца, в которые будет запускаться проверка по расписанию
Время в часовом поясе агента	Время в часовом поясе агента, в которое будет запускаться проверка по расписанию

Параметр	Описание
Тип проверки	Определяет тип проверки по расписанию: полная (все файлы на конечном устройстве и объекты в оперативной памяти) или быстрая (важные системные файлы, выбранные экспертами Positive Technologies)

Удаление антивируса

Вы можете управлять состоянием антивируса на агенте из веб-интерфейса модуля. Например, вы можете удалить или заново установить антивирус.

- Чтобы удалить антивирус на агенте:

  1. В главном меню выберите **Агенты**.
  2. В столбце **Модули** для выбранного агента нажмите **Антивирус**.
  3. Нажмите **Удалить антивирус**.

Вы также можете удалить антивирус, отключив или удалив модуль из политики.

9.5. Модули реагирования

В этом разделе приведена информация о модулях реагирования.

В этом разделе

9.5.1. Блокировка учетных записей

Модуль «Блокировка учетных записей» блокирует и завершает сеансы локальных учетных записей в операционной системе. Длительность блокировки задается в параметрах соответствующего действия.

> **Примечание.** Для работы модуля на конечных устройствах под управлением операционной системы Linux требуется утилита who.

Таблица 10. Параметры модуля «Блокировка учетных записей»

Параметр или блок параметров	Описание
Исключения	Список учетных записей, которые не будут блокироваться и сеансы которых не будут завершаться
Длительность блокировки, мин (параметр действий)	Время в минутах, на которое будет заблокирована учетная запись. По умолчанию 120 минут

9.5.2. Изоляция узлов

Модуль «Изоляция узлов» блокирует сетевой трафик на узлах. Вы можете изолировать узел, на котором установлен агент, двумя способами — полностью, отключив все сетевые адаптеры, или частично, сохранив для него связь с сервером агентов и адресами из списка исключений.

> **Внимание!** Для работы версии модуля 3.0.0 на агенте должен быть установлен модуль «Ядро (внутренний сервис)» (см. раздел 9.1). Версия модуля 2.0.0 работает только в Windows.
>
> **Примечание.** В конфигурации модуля вы можете настроить исключения — параметры сетевого трафика, который не будет блокироваться модулем. Добавлять в исключения сервер MaxPatrol EPP не требуется: обмен данных с ним не будет блокироваться.

9.5.3. Перенаправление DNS-запросов (sinkholing)

Модуль «Перенаправление DNS-запросов (sinkholing)» перенаправляет трафик с подозрительных и вредоносных доменов на заданный IP-адрес с помощью файла `hosts`.

Таблица 11. Параметры модуля «Перенаправление DNS-запросов (sinkholing)»

Параметр или блок параметров	Описание
IP-адрес, на который перенаправлять трафик	IP-адрес, на который следует перенаправлять трафик. Это может быть специальный сервер, на котором входящие данные будут анализироваться, или неиспользуемый внутренний IP-адрес для блокировки трафика, например `0.0.0.0`
Префиксы доменных имен	Один или несколько префиксов, которые будут добавляться к доменным именам
Домены, с которых перенаправлять трафик	Один или несколько доменов, трафик с которых будет перенаправляться. **Примечание.** В файл `hosts` будут добавлены записи со всеми сочетаниями заданных префиксов и доменов

► Чтобы настроить модуль «Перенаправление DNS-запросов (sinkholing)»:

1. В главном меню выберите **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Перенаправление DNS-запросов (sinkholing)».
4. В поле **IP-адрес, на который перенаправлять трафик** введите IP-адрес, на который будет перенаправляться трафик.

   Это может быть адрес специального сервера, на котором входящие данные будут анализироваться, или неиспользуемый внутренний IP-адрес для блокировки трафика, например `127.0.0.1` или `0.0.0.0`.
5. В поле **Домены, с которых перенаправлять трафик** введите один или несколько доменов, трафик с которых будет перенаправляться.

   Трафик будет перенаправляться со всех адресов заданных доменов.
6. Если требуется, в поле **Префиксы доменных имен** введите один или несколько префиксов, которые будут добавляться ко всем доменным именам.

   Например, если вы хотите перенаправлять трафик с адресов mail.example.com и mail.example.net, вам нужно добавить `example.com` и `example.net` в список доменов, а `mail` в список префиксов.
7. Нажмите **Сохранить**.

9.5.4. Карантин

Модуль «Карантин» изолирует подозрительные файлы в зашифрованном хранилище на время их проверки с помощью YARA-правил или в PT Sandbox. При этом в карантин помещается не сам файл, а его копия. Из-за этого в целях безопасности исходный файл рекомендуется удалять модулем «Удаление файла». Сценарий настройки системы с модулем «Карантин» может быть следующим:

1. На подходящие события модуля «Коррелятор» назначаются действия «Поместить копию файла в карантин», «Отправить файл на проверку в PT Sandbox» и «Удалить файл».
2. На событие «Файл проверен в PT Sandbox. Вердикт: безопасный» назначается действие «Восстановить файл из карантина».
3. Если файл признан вредоносным, файл удаляется из карантина по ротации, вручную или выгружается для исследования экспертами.

Таблица 12. Параметры модуля «Карантин»

Параметр или блок параметров	Описание
Пароль для архива	Пароль, который будет установлен для скачанного из карантина архива с файлами
Исключения → Папки и файлы	Путь до файла или путь до папки, файлы в которой не будут помещаться в карантин
Исключения для расширений файлов	Список расширений файлов, которые не будут помещаться в карантин
Максимальный размер файла в карантине, МБ	Максимальный размер файла, который может быть помещен в карантин (в мегабайтах)
Размер хранилища, МБ	Размер хранилища файлов в карантине (в мегабайтах). При заполнении хранилища из него будут удаляться самые старые файлы
Запасная папка для восстановления	Папка, в которую будет восстановлен файл, если его невозможно восстановить в изначальную папку

9.5.5. Запуск командной оболочки

Модуль «Запуск командной оболочки» позволяет выполнять команды в PowerShell или Bash на конечном устройстве из веб-интерфейса MaxPatrol EPP. Это помогает проводить расследование инцидентов, собирать необходимые данные и устранять нарушения независимо от того, где находится конечное устройство. Все выполненные команды сохраняются в журнал.

Таблица 13. Параметры модуля «Запуск командной оболочки»

Параметр или блок параметров	Описание
Защищать архив паролем	Использовать ли пароль для архива с журналом выполненных команд
Пароль для архива	Пароль, который будет установлен для скачанного архива с журналом

9.6. Модули интеграции

В этом разделе приведена информация о модулях интеграции.

В этом разделе

9.6.1. Проверка файлов в PT Sandbox

Модуль «Проверка файлов в PT Sandbox» отправляет файлы на проверку в PT Sandbox и сохраняет результат проверки в локальные БД всех агентов с такой же политикой. Перед отправкой файла на проверку проверяется наличие актуального результата проверки в локальной БД. Если актуальный результат есть, то файл в PT Sandbox не отправляется. Результат проверки считается актуальным в течение семи дней.

Таблица 14. Параметры модуля «Проверка файлов в PT Sandbox»

Параметр или блок параметров	Описание
Токен доступа	Токен доступа к публичному API PT Sandbox. Инструкции по созданию токена доступа PT Sandbox приведены в технической документации продукта
Максимальный размер файла	Максимальный размер файла, который вы можете отправить на проверку в PT Sandbox
MaxPatrol EPP подключен как источник	Определяет способ интеграции с PT Sandbox. Если MaxPatrol EPP подключен как источник, нужно установить флажок
Классы вредоносного ПО	Список классов вредоносного ПО, при обнаружении которых PT Sandbox вынесет вердикт «вредоносный файл». При обнаружении вредоносного ПО, относящегося к другому классу, будет вынесен вердикт «безопасный файл». Не рекомендуется изменять стандартный список классов
Адрес сервера	Адрес сервера PT Sandbox (FQDN или IP-адрес без протокола)
Максимальное время ожидания результатов проверки	Время в минутах, в течение которого вам хотелось бы получить результат проверки файла. Если результат не будет получен за заданное время, то будет сгенерировано событие «Истекло время ожидания результата проверки файла». Проверка при этом не отменяется и результат будет получен позднее

Перед настройкой модуля необходимо в PT Sandbox создать токен доступа к публичному API с разрешенным действием **Проверка с параметрами источника**, добавить MaxPatrol EPP как источник объектов и настроить его.

► Чтобы настроить модуль «Проверка файлов в PT Sandbox»:

1. В главном меню выберите **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Проверка файлов в PT Sandbox».
4. Введите адрес сервера PT Sandbox, на который вы хотите отправлять файлы.
5. Введите токен доступа к публичному API PT Sandbox.
6. Если MaxPatrol EPP добавлен в PT Sandbox как источник объектов, установите соответствующий флажок.

   Примечание. Если вы используете старую версию PT Sandbox или старую конфигурацию источников, флажок устанавливать не нужно. В этом случае токен доступа должен быть с разрешенным действием **Проверка с передаваемыми параметрами**.
7. Если требуется, задайте дополнительные параметры модуля.
8. Если требуется, выберите действия, которые будут выполняться при регистрации событий ИБ (см. раздел 10).
9. Нажмите **Сохранить**.

9.6.2. Сканирование в режиме аудита (MaxPatrol VM)

Модуль «Сканирование в режиме аудита (MaxPatrol VM)» выполняет аудит узлов методом белого ящика. Модуль определяет детальную конфигурацию операционной системы, установленной на узле, перечень установленного программного обеспечения, список открытых портов, перечень зарегистрированных пользователей и передает данные в MaxPatrol VM для формирования перечня уязвимостей и карты сети.

Внимание! В текущей версии MaxPatrol EPP невозможно сканирование в режиме аудита на узлах под управлением следующих ОС: Windows 11, Astra Linux Common Edition 2.12 («Орел»), «РЕД ОС Рабочая станция» 7.3, AlterOS Desktop 7.5, «ОСнова» 2.0 «Оникс», «Альт Сервер» 9, 10.1, 10.2, «Альт Рабочая станция» 10.2 и «МОС» 12.

Таблица 15. Параметры модуля «Сканирование в режиме аудита (MaxPatrol VM)»

Параметр или блок параметров	Описание
Версия MaxPatrol 10	Версия MaxPatrol 10, в которой будут обрабатываться результаты сканирования. Для корректной обработки необходимо выбрать используемую версию MaxPatrol 10. Если вы выберете версию ниже используемой, то в результатах будут неполные данные. Если выше — результаты сканирования обработаны не будут.

Параметр или блок параметров	Описание
	Внимание! Для агентов, установленных на Debian 12 и Ubuntu 24.04 LTS, необходимо всегда выбирать версию версию 27.2 или выше, на Red Hat Enterprise Linux 7 (при использовании MaxPatrol 10 версии 26.2) — версию 25.1
Пропускаемые классы модели активов	Фильтрация данных при заполнении модели активов: имена классов модели активов, которые не будут заполняться при сборе данных, через точку с запятой
Классы модели активов для сбора данных	Фильтрация данных при заполнении модели активов: имена классов модели активов, которые будут заполняться при сборе данных, через точку с запятой
Маски модели активов для сбора данных	Фильтрация данных при заполнении модели активов: маски модели активов для сбора данных через точку с запятой
Запуск	Периодичность запуска сканирования по расписанию
День недели	Дни недели, в которые будет запускаться сканирование по расписанию
Месяцы	Месяцы, в которые будет запускаться сканирование по расписанию
День месяца	Дни месяца, в которые будет запускаться сканирование по расписанию
Время в часовом поясе агента	Время в часовом поясе агента, в которое будет запускаться сканирование по расписанию
Макс. загрузка ЦП	Доля загрузки процессора конечного устройства, при которой сканирование будет отложено. Модуль учитывает среднюю загрузку за последние 100 секунд. Параметр учитывается только при автоматическом запуске сканирования
Ждать не более	Максимальное время в часах, на которое модуль будет откладывать сканирование из-за превышения заданной загрузки процессора. Параметр учитывается только при автоматическом запуске сканирования
Пауза между повторными сканированиями	Время после успешного окончания сканирования, в течение которого не будет запускаться новое сканирование. Параметр учитывается только при автоматическом запуске сканирования

Настройка модуля

Вы можете настроить запуск сканирования в режиме аудита по расписанию или при регистрации события ИБ, а также запускать его вручную. Ориентировочное время сканирования около 10 минут, обработка результатов в MaxPatrol VM — до 30 минут. При сильной нагрузке на сервер MaxPatrol VM время обработки результатов может увеличиться.

При потере соединения между агентом и сервером MaxPatrol EPP сканирование по расписанию будет запускаться в обычном порядке. Результаты сканирования будут храниться в локальной базе данных агента и будут отправлены в MaxPatrol VM после восстановления связи.

Внимание! Сканирование в режиме аудита может существенно влиять на загрузку процессора конечного устройства. Не рекомендуется настраивать частый запуск сканирования по расписанию, а также назначать его на события ИБ, которые регистрируются постоянно.

► Чтобы настроить модуль «Сканирование в режиме аудита (MaxPatrol VM)»:

1. В главном меню выберите **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
4. В раскрывающемся списке **Версия MaxPatrol 10** выберите используемую версию MaxPatrol 10.
5. В блоке параметров **Расписание** настройте запуск сканирования по расписанию.
6. Если требуется, настройте частичный сбор данных об узлах:
   - Если вы хотите фильтровать данные по классам модели активов, в соответствующих полях введите имена классов, которые нужно заполнять или пропускать.
   - Если вы хотите фильтровать данные по маскам модели активов, в соответствующем поле введите маски для сбора данных.

     Примечание. Фильтрация данных возможна только одним способом: либо по классам модели активов, либо по маскам.
7. Если требуется, задайте дополнительные параметры модуля.
8. Если требуется, выберите действия, которые будут выполняться при регистрации событий ИБ (см. раздел 10).
9. Нажмите **Сохранить**.

9.6.3. Отправка событий на syslog-сервер

Внимание! В MaxPatrol EPP версии 8.1 отправка событий на syslog-сервер выполняется без участия модуля. Для отправки событий нужно задать параметры syslog-сервера в манифесте и обновить систему, установить отправку событий заданному получателю в параметрах группы и удалить модуль «Отправка событий на syslog-сервер» из политики.

9.6.4. Отправка файлов

Модуль «Отправка файлов» отправляет файлы с конечного устройства во внешнюю систему, адрес которой задан в конфигурации. Например, это может быть песочница.

Таблица 16. Параметры модуля «Отправка файлов»

Параметр или блок параметров	Описание
Максимальный размер файла, МБ	Максимальный размер файла, который вы можете отправить во внешнюю систему
Адрес внешней системы и метод HTTP-запроса	Адрес внешней системы и метод HTTP-запроса, с помощью которого будут отправляться файлы
Список заголовков запроса	Заголовки запроса, которые будут добавляться к HTTP-запросам

10. Настройка автоматического реагирования

Для настройки автоматического реагирования вам нужно назначить действия, которые будут выполняться при регистрации того или иного события ИБ. После добавления модуля в политику для всех событий ИБ, которые он регистрирует, назначено только одно автоматическое действие — **Сохранить в БД**. Назначить действия на события модуля вы можете двумя способами:

— выбрав для события необходимые действия (см. раздел 10.1);

— выбрав для действия события, при регистрации которых его нужно выполнять (см. раздел 10.2).

Примечание. Для автоматического выполнения действий модулям требуются данные, которые передаются с помощью переменных в событиях. Вы не сможете назначить действие на событие, если это событие не содержит необходимых данных.

Если на одно событие назначено несколько действий, то порядок их выполнения определяется приоритетом. Каждое действие имеет приоритет от 1 до 100 в условных единицах. Если у двух действий одинаковый приоритет, то они будут выполняться в случайном порядке.

Далее приведены инструкции по назначению действий на события.

В этом разделе

10.1. Назначение действий на событие модуля

► Чтобы назначить действия на событие модуля:

1. В главном меню выберите **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль, на события которого вы хотите назначить действия.
4. В блоке параметров **События** напротив нужного события нажмите .

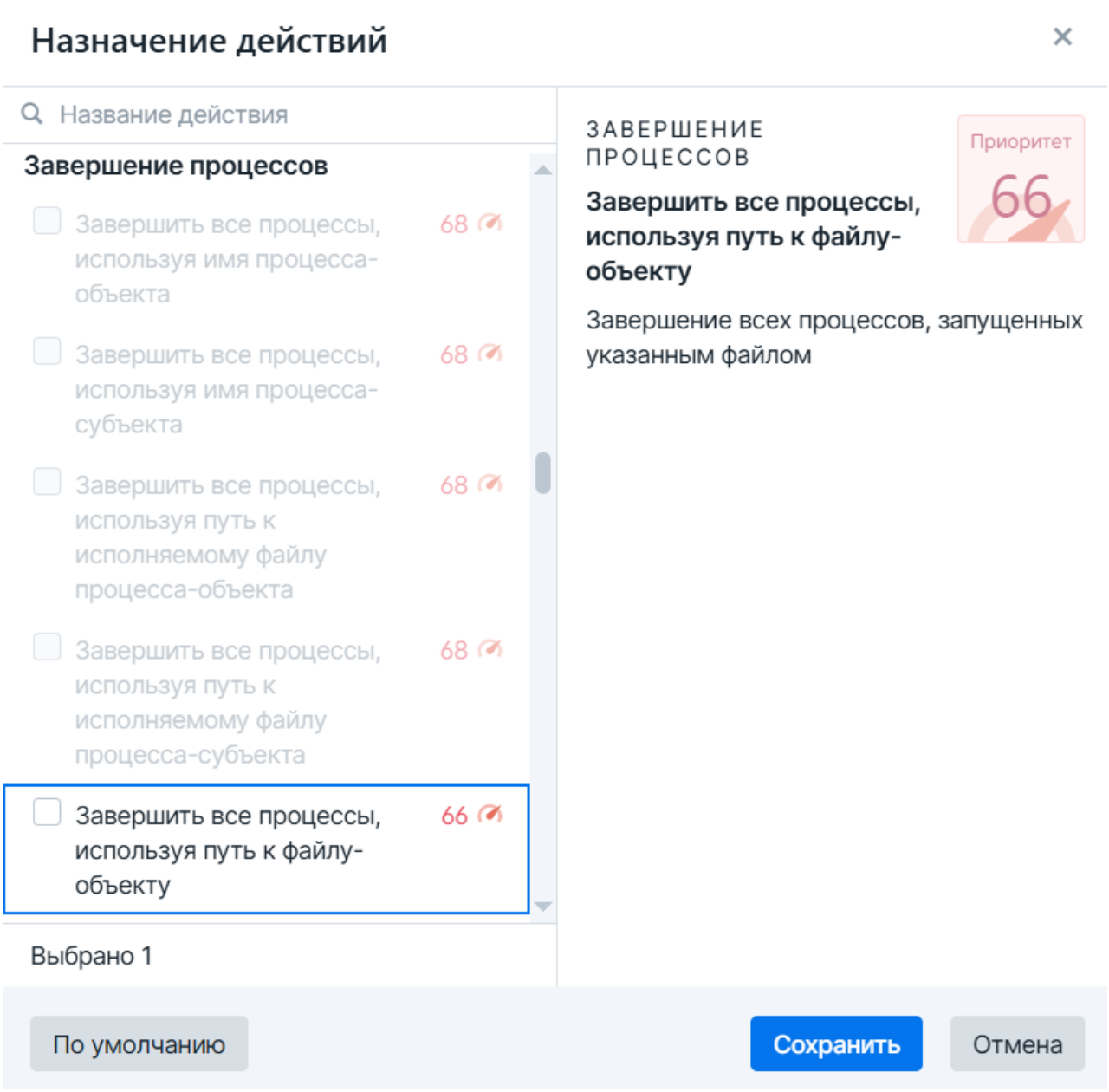

Рисунок 4. Назначение действий

5. Установите флажки напротив тех действий, которые нужно автоматически выполнять при регистрации этого события.
6. Нажмите **Сохранить**.

10.2. Массовое назначение действия на события модуля

Вы можете назначить конкретное действие на выбранные события модуля или сразу на все с помощью мастера назначения действий.

- Чтобы назначить действие на события модуля:

1. В главном меню выберите **Политики**.
2. Выберите политику.
3. В списке **Включенные** выберите модуль, на события которого вы хотите назначить действия.
4. Нажмите **Мастер назначения действий**.

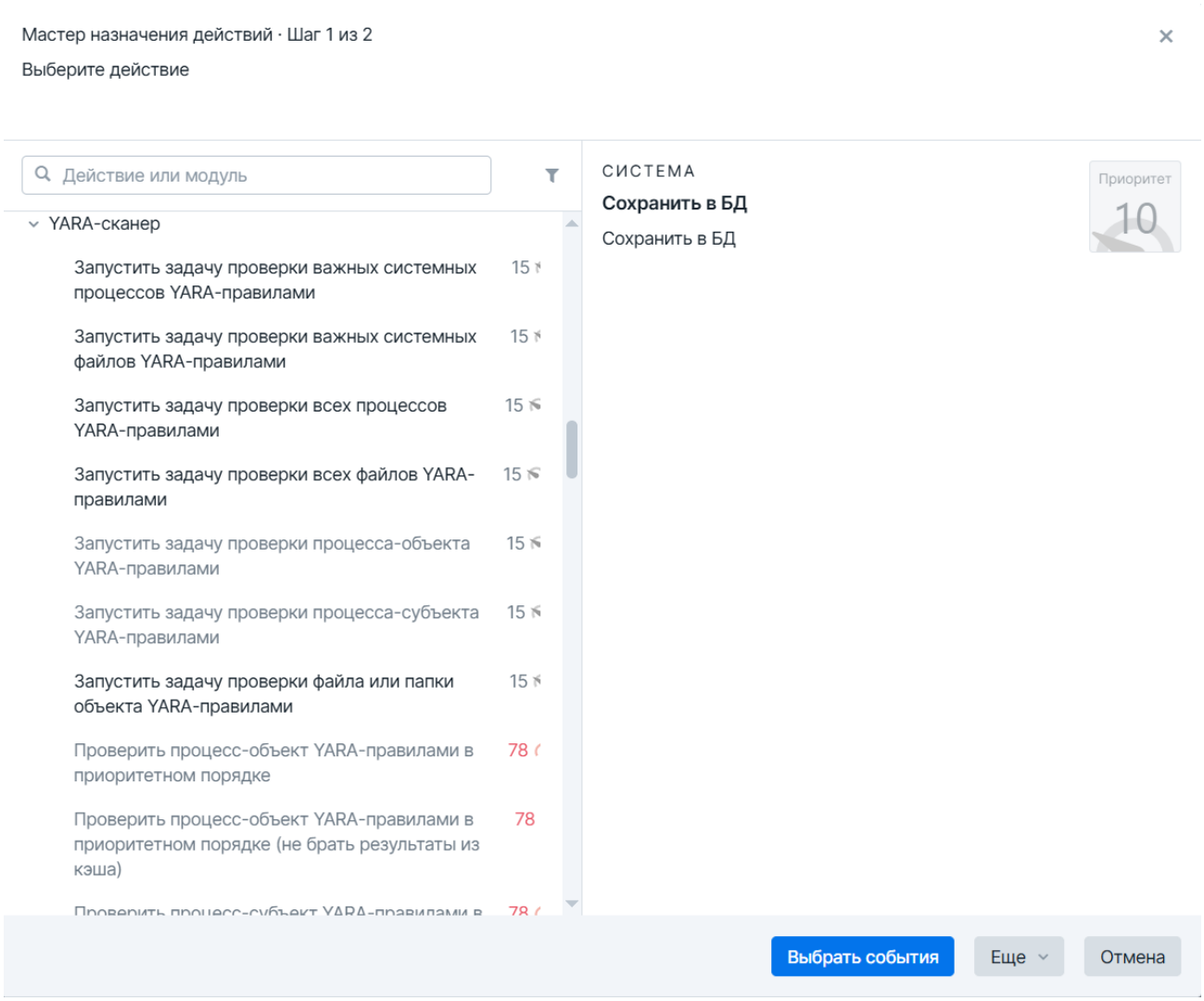

Рисунок 5. Выбор действия

5. Выберите действие, которое вы хотите назначить на события.

   Примечание. Вы можете отфильтровать действия и изменить их группировку по кнопке .

6. Нажмите **Выбрать события**.

Примечание. Вы можете назначить действие на все доступные события модуля сразу, нажав **Еще** и в раскрывшемся меню выбрав пункт **Назначить на все доступные события**.

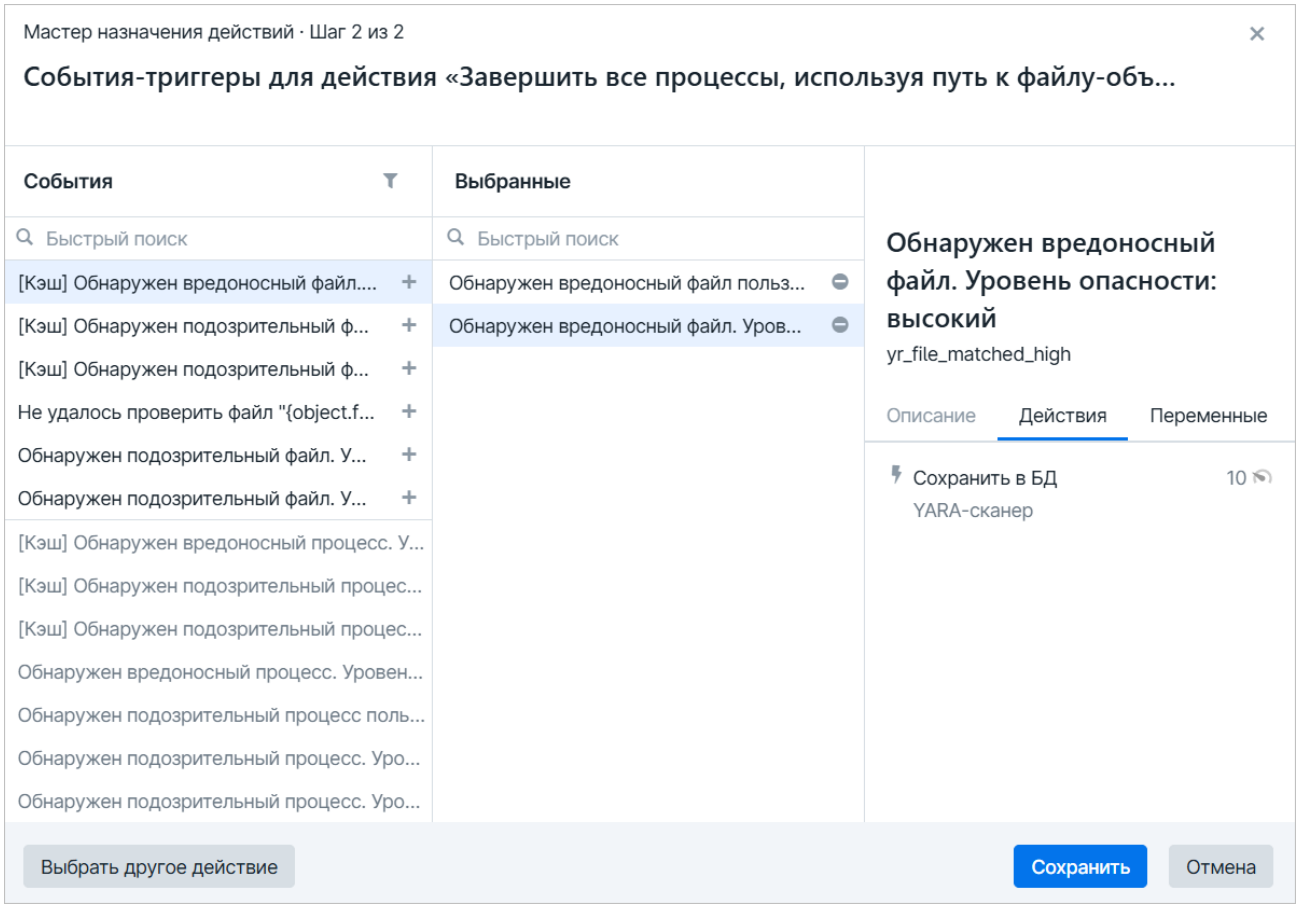

Рисунок 6. Выбор событий

7. Нажмите + напротив тех событий, при регистрации которых нужно выполнять выбранное действие.
8. Нажмите **Сохранить**.

11. Назначение политики на группу агентов

Для установки модулей на агенты необходимо назначить политику на группу агентов. Одну политику можно назначить на множество групп, а на одну группу — несколько разных политик. Вы не можете назначить политику на группу, если в этой политике есть модуль, который уже работает на агентах этой группы (входит в другую политику). В таких случаях вам нужно отключить модуль в политике или снять политику с группы.

- Чтобы назначить политику на группу:

  1. В главном меню выберите **Политики**.
  2. Выберите политику.
  3. Нажмите **Связь с группами**.
  4. Напротив группы, на которую вы хотите назначить политику, нажмите .

12. О технической поддержке

Базовая техническая поддержка доступна для всех владельцев действующих лицензий на MaxPatrol EPP 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 технической 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 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 порталу 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.

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения технической 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 технической 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 технической 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 технической 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 17. 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 технической 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 конечном устройстве для обеспечения работы модулей и связи с сервером агентов.

группа агентов

Один или несколько агентов, объединенных по определенному принципу для назначения им одних и тех же политик.

действие модуля

Операция, которую модуль выполняет на конечном устройстве. Запуск операции может выполняться по команде пользователя или автоматически при регистрации того или иного события ИБ.

зависимость

Условие, которое должно выполняться для корректной работы модуля агента.

конечное устройство

Оборудование, имеющее ценность для организации и подлежащее защите от киберугроз.

модуль агента

Приложение, которое запускается на агенте для выполнения основных функций продукта. Есть пять типов модулей: модули доставки и установки, сбора, интеграции, обнаружения, реагирования.

модуль доставки и установки

Модуль агента, который устанавливает и настраивает приложения, а также управляет конфигурацией ОС на конечном устройстве.

модуль обнаружения

Модуль агента, который анализирует собранные события, обнаруживает подозрительную и вредоносную активность на конечном устройстве — и регистрирует события ИБ.

модуль реагирования

Модуль агента, который пресекает подозрительную и вредоносную активность на конечном устройстве, выполняя действия в соответствии с политикой модуля обнаружения.

модуль сбора

Модуль агента, который собирает данные о событиях на конечном устройстве и передает их в модули обнаружения и в SIEM-системы.

поведенческий анализ

Технология выявления атак и киберугроз, основанная на анализе поведения файлов, приложений и пользователя в информационной системе.

политика конфигурации модулей агентов

Механизм управления поставкой модулей агентов в заданной конфигурации на конечные устройства. Политика состоит из перечня модулей и описания их конфигурации, который назначается группе агентов.

приоритет действия

Условная величина, которая определяет порядок выполнения действий при регистрации того или иного события ИБ.

сервер агентов

Серверное приложение, предназначенное для управления агентами и модулями.

управляющий сервер

Серверное приложение, предназначенное для управления конфигурацией системы.

positive technologies

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.