MaxPatrol Endpoint Security версия 10.1

Начало работы

Дата редакции документа: 27.07.2026

Содержание

1. Об этом документе

Это руководство содержит информацию и инструкции для первоначальной настройки MaxPatrol Endpoint Security (далее также — MaxPatrol ES).

Комплект документации MaxPatrol ES включает в себя следующие документы:

— Этот документ.

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

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

2. О MaxPatrol ES

MaxPatrol ES — решение, предназначенное для комплексной защиты конечных устройств и остановки злоумышленника на любом этапе атаки. MaxPatrol ES обеспечивает многоуровневую защиту IT-инфраструктуры организации благодаря совместной работе систем MaxPatrol EDR и MaxPatrol EPP. Решение встроено в экосистему продуктов Positive Technologies и позволяет:

— отправлять данные о событиях ОС и событиях ИБ в MaxPatrol SIEM;

— 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 ES имеет возможность выполнить следующие автоматические действия:

— попытаться вылечить файл или заблокировать его;

— 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 ES

MaxPatrol ES состоит из серверной части и агентов, устанавливаемых на конечные устройства. Серверная часть MaxPatrol ES 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 ES — 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 ES:

1. Сервер агентов передает на агенты модули и их конфигурацию.
2. Модули выполняют на конечных устройствах основные функции системы: сбор данных, обнаружение и предотвращение угроз, реагирование и другие.
3. Данные о событиях ОС кэшируются в памяти агента и передаются при необходимости на syslog-сервер или в MaxPatrol SIEM.
4. Данные о событиях ИБ кэшируются в памяти агента и пересылаются в хранилище событий, в базу данных MaxPatrol SIEM или на syslog-сервер.
5. Агент передает метрики и данные трассировки на сервер агентов.
6. 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.

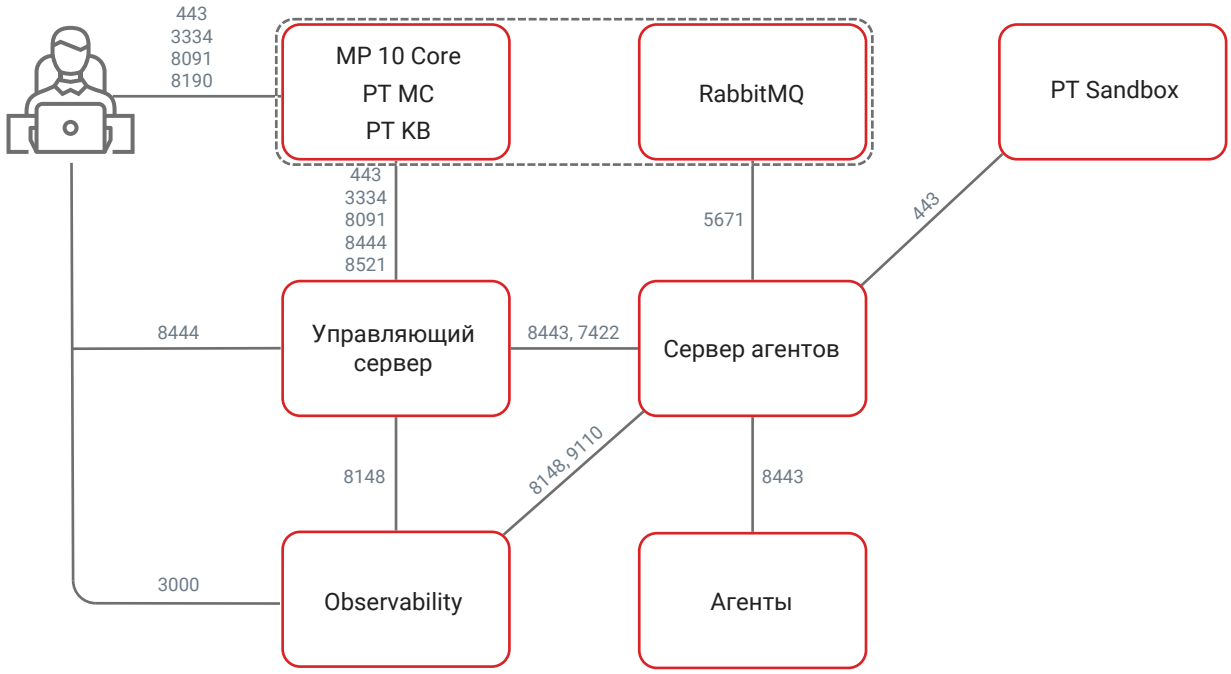

Рисунок 1. Взаимодействие компонентов MaxPatrol ES при установке совместно с системой MaxPatrol 10

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

Примечание. Если какие-либо компоненты MaxPatrol ES 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, 7422, 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	Сервер агентов	NATS (leaf node)	7422
Управляющий сервер	MP 10 Core	HTTPS	443, 3334, 8521
Управляющий сервер	Компонент Observability	gRPC	8148

Источник	Получатель	Протокол	TCP-порт
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 ES 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 ES запросите у администратора PT MC логин и пароль вашей учетной записи и убедитесь, что в браузере разрешены всплывающие окна.

Примечание. В PT MC вы можете настроить аутентификацию и авторизацию пользователей через сторонние SSO-системы по протоколам SAML 2.0 и LDAP. Такой способ аутентификации и авторизации позволяет не хранить учетные данные пользователей в PT MC, а обращаться за ними в SSO-систему, используемую в вашей компании.

► Чтобы войти в MaxPatrol ES:

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

   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 ES 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 ES. Если вы указали неверные данные, отобразится сообщение об ошибке.

5. Интерфейс MaxPatrol ES

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

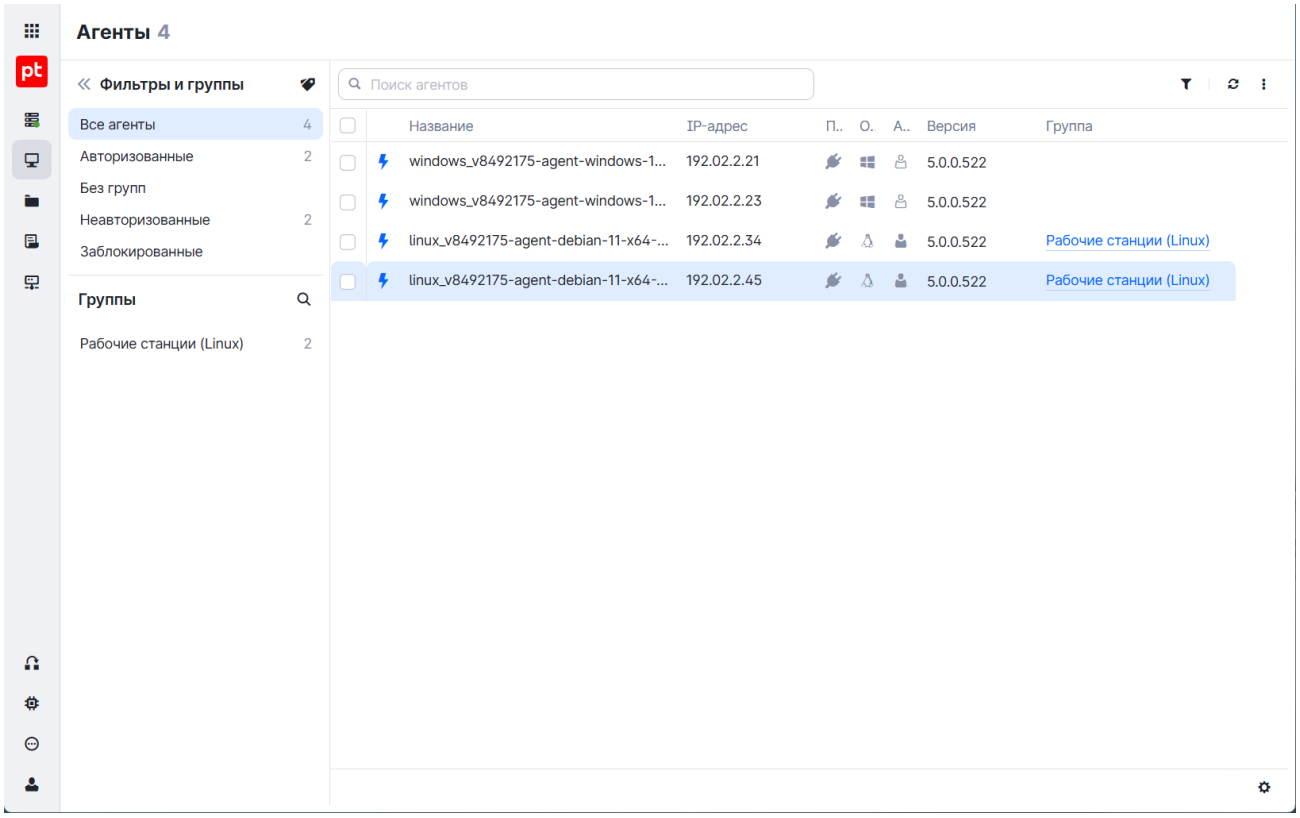

Рисунок 2. Страница **Агенты**

Веб-интерфейс MaxPatrol ES 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 ES

После установки MaxPatrol ES и агентов вам нужно:

1. Создать политики с помощью встроенных шаблонов (см. раздел 8).
2. Настроить модули в политиках. В частности, вам нужно настроить интеграцию с PT Sandbox, а также модули «Коррелятор» и «WinEventLog: сбор данных из журнала событий Windows».
3. В параметрах политики назначить автоматические действия (см. раздел 9), которые будут выполняться при регистрации событий ИБ.
4. Назначить политики на группы агентов (см. раздел 10).
5. Если в системе несколько серверов агентов, распространить группы агентов на них.
6. Авторизовать агенты (см. раздел 7). При авторизации агент добавляется в группу. После этого на агенте сразу будут установлены модули из всех политик, назначенных на эту группу.

См. также

Назначение политики на группу агентов (см. раздел 10)

Авторизация агента (см. раздел 7)

7. Авторизация агента

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

> **Примечание.** Вы можете автоматизировать авторизацию агентов с помощью планировщика задач.

- 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 и настроить автоматические действия (см. раздел 9).

- Чтобы создать политику:

  1. В главном меню выберите **Политики**.

     Примечание. Если в системе есть старые политики, в меню нужно выбрать **Политики** → **На управляющем сервере**.

  2. Нажмите +.
  3. Выберите шаблон, на базе которого вы хотите создать политику.
  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. 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 9.1);

— выбрав для действия события, при регистрации которых его нужно выполнять (см. раздел 9.2).

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

9.1. Назначение действий на событие модуля

► Чтобы назначить действия на событие модуля:

1. В главном меню выберите **Политики**.

   Примечание. Если в системе есть старые политики, в меню нужно выбрать **Политики** → **На управляющем сервере**.

2. Выберите политику.
3. Выберите модуль, на события которого вы хотите назначить действия.
4. В блоке параметров **События** напротив нужного события нажмите .

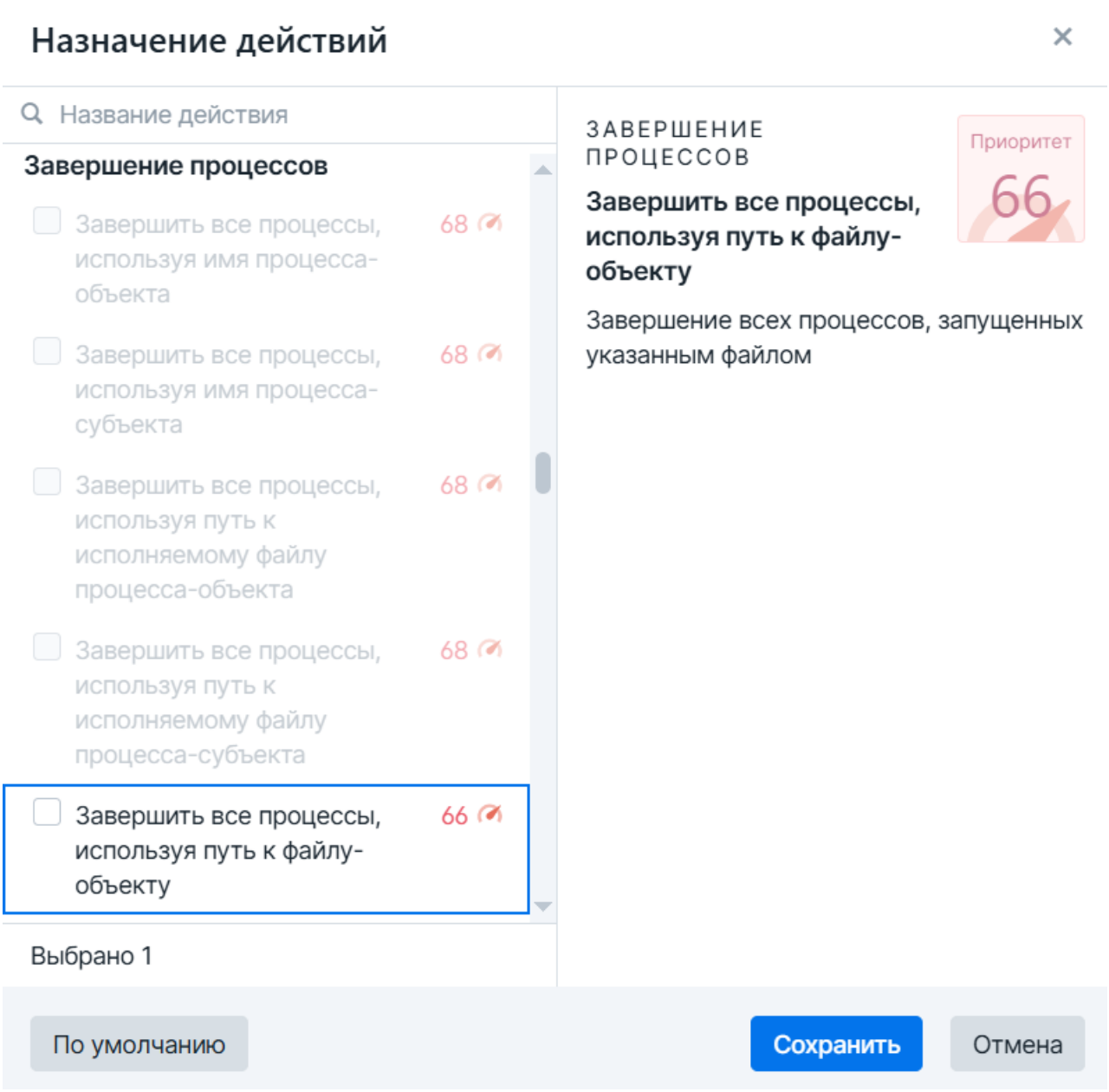

Рисунок 3. Назначение действий

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

9.2. 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**.

   Примечание. Если в системе есть старые политики, в меню нужно выбрать **Политики** → **На управляющем сервере**.

2. Выберите политику.
3. Выберите модуль, на события которого вы хотите назначить действия.
4. Нажмите **Мастер назначения действий**.

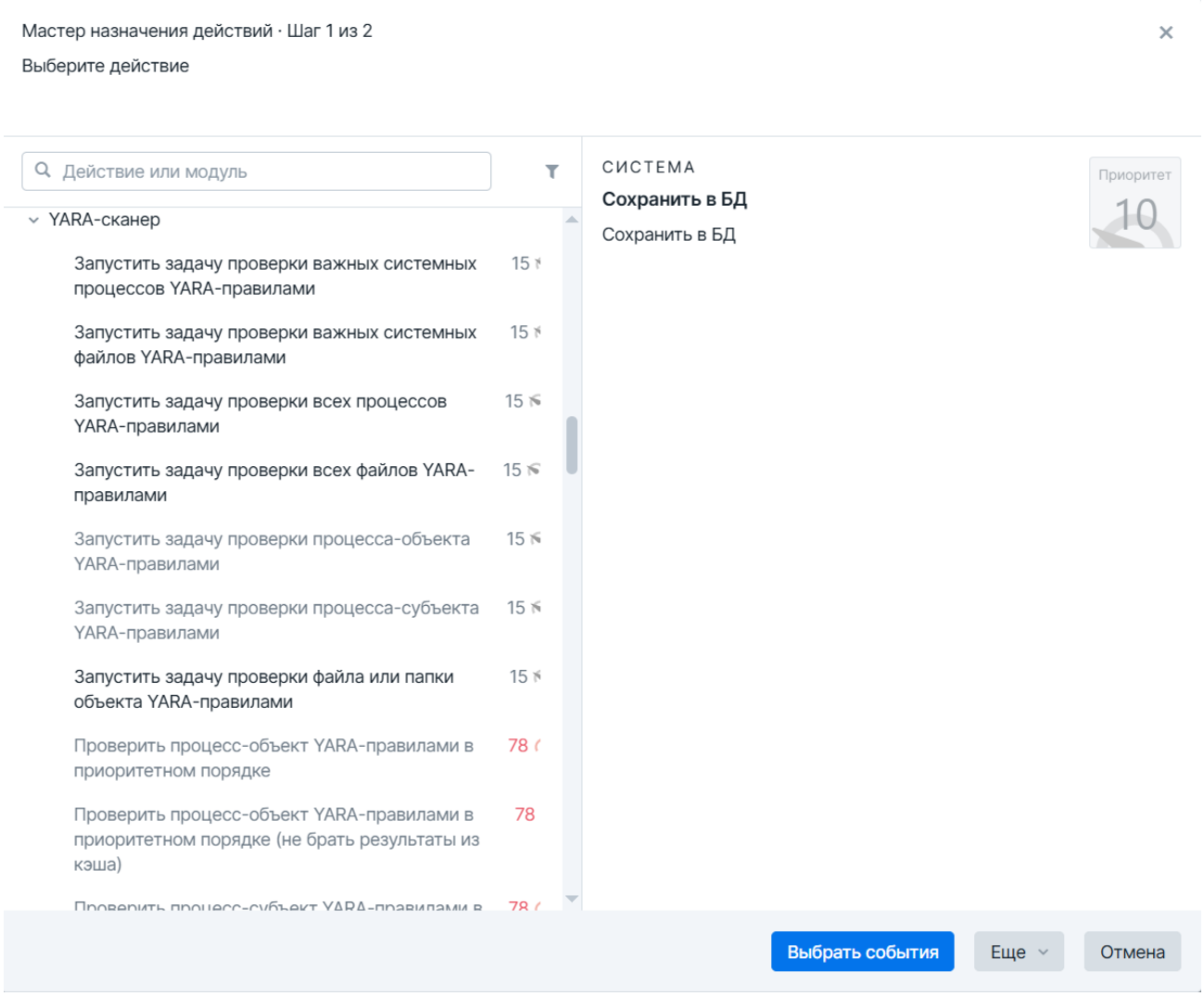

Рисунок 4. Выбор действия

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**.

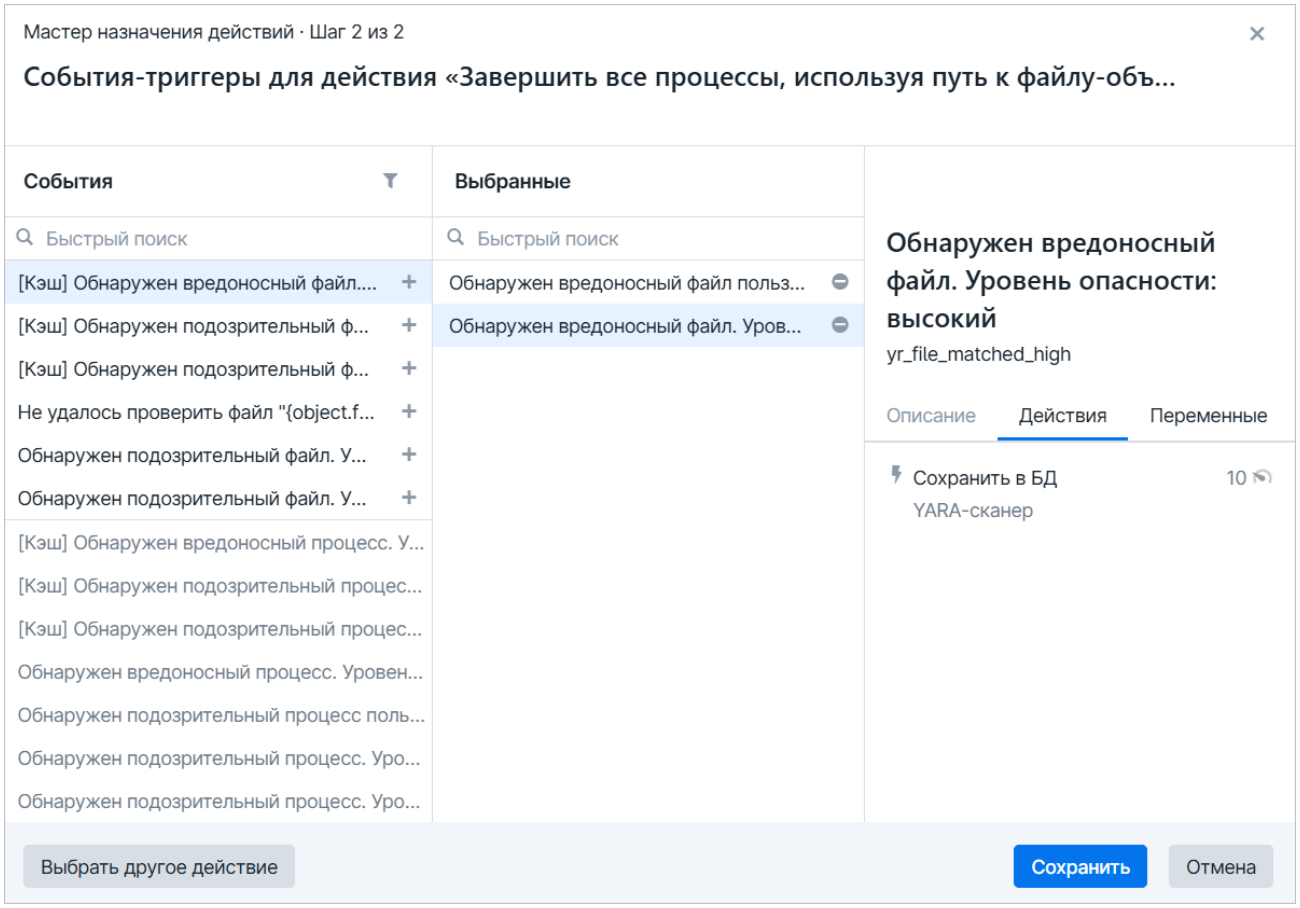

Рисунок 5. Выбор событий

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

10. 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.

Назначение политики на группы

- Чтобы назначить политику на группы:

  1. В главном меню выберите **Политики**.

     Примечание. Если в системе есть старые политики, в меню нужно выбрать **Политики** → **На управляющем сервере**.
  2. Выберите политику.
  3. Выберите вкладку **Группы**.
  4. Выполните одно из следующих действий:
     - Если политика еще не назначена на группы, нажмите **Назначить**.
     - Если политика уже назначена на некоторые группы, нажмите **Назначить на группы**.
  5. Выберите одну или несколько групп.
  6. Нажмите **Назначить**.

Назначение политик на группу

- Чтобы назначить политики на группу:

  1. В главном меню выберите **Группы агентов**.

     Примечание. Если в системе есть старые группы, в меню нужно выбрать **Группы агентов** → **На управляющем сервере**.
  2. Выберите группу.
  3. Выберите вкладку **Политики**.
  4. Выполните одно из следующих действий:
     - Если на группу еще не назначены политики, нажмите **Назначить**.
     - Если на группу назначены некоторые политики, нажмите +.

5. Выберите одну или несколько политик.
6. Нажмите **Назначить**.

11. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на MaxPatrol ES в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках гарантийной поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

> **Примечание.** Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы и сроки ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются на портале технической поддержки.

Портал технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к 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.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку на портале технической поддержки и предоставить следующие данные:

— номер лицензии на использование продукта;

— файлы журналов и наборы диагностических данных, которые требуются для анализа;

— снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг гарантийной поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по гарантийной поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 2. Время реакции на заявку

Уровень значимости заявки	**Критерии значимости заявки**	**Время реакции на заявку**
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

— о ходе диагностики по заявленной проблеме и ее результатах;

— планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

  Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

Глоссарий

агент

Приложение, которое устанавливается на конечном устройстве для обеспечения работы модулей и связи с сервером агентов.

актив

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

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.

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.