MaxPatrol EDR версия 8.0

Начало работы

© Positive Technologies, 2025.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 20.05.2025

Содержание

1. Об этом документе ... 5
2. О MaxPatrol EDR ... 6
3. Архитектура и алгоритм работы MaxPatrol EDR ... 7
4. Вход в MaxPatrol EDR через PT MC ... 10
5. Интерфейс MaxPatrol EDR ... 11
6. Порядок настройки MaxPatrol EDR ... 12
7. Авторизация агента ... 13
8. Создание политики ... 14
9. Настройка модулей и работа с ними ... 15
   - 9.1. Системные модули ... 15
   - 9.2. Модули доставки и установки ... 15
     - 9.2.1. Установщик Sysmon ... 15
     - 9.2.2. Установщик auditd ... 16
     - 9.2.3. Конфигуратор аудита Windows ... 16
   - 9.3. Модули сбора ... 17
     - 9.3.1. WinEventLog: сбор данных из журнала событий Windows ... 17
     - 9.3.2. ETW: трассировка событий Windows ... 18
     - 9.3.3. Сбор данных из файлов журналов ... 18
     - 9.3.4. Сбор данных о состоянии системы ... 19
     - 9.3.5. Нормализатор ... 21
   - 9.4. Модули обнаружения ... 22
     - 9.4.1. Коррелятор ... 22
       - 9.4.1.1. О модуле «Коррелятор» ... 22
       - 9.4.1.2. Работа с исключениями ... 23
     - 9.4.2. YARA-сканер ... 25
       - 9.4.2.1. О модуле «YARA-сканер» ... 25
       - 9.4.2.2. О кэшировании результатов проверок ... 27
       - 9.4.2.3. Запуск проверки вручную ... 28
       - 9.4.2.4. Просмотр результатов проверки ... 28
       - 9.4.2.5. Просмотр правил ... 29
     - 9.4.3. Проверка файлов по хеш-сумме ... 29
     - 9.4.4. Обнаружение подозрительных файлов ... 30
   - 9.5. Модули реагирования ... 30
     - 9.5.1. Удаление файлов ... 31
     - 9.5.2. Завершение процессов ... 31
     - 9.5.3. Блокировка учетных записей ... 32
     - 9.5.4. Изоляция узлов ... 33
     - 9.5.5. Блокировка по IP-адресу ... 34
     - 9.5.6. Перенаправление DNS-запросов (sinkholing) ... 35
       - 9.5.6.1. О модуле «Перенаправление DNS-запросов (sinkholing)» ... 35
       - 9.5.6.2. Настройка модуля «Перенаправление DNS-запросов (sinkholing)» ... 35
       - 9.5.6.3. Перенаправление DNS-запросов вручную ... 36
     - 9.5.7. Карантин ... 37

9.5.7.1. О модуле «Карантин» 37
9.5.7.2. Изоляция файла вручную 38
9.5.7.3. Восстановление файла из карантина 38
9.5.7.4. Удаление файла из карантина 39
9.5.7.5. Скачивание файла из карантина 39
9.5.8. Запуск командной оболочки 39
9.5.9. Интерпретатор языка Lua 40
9.6. Модули интеграции 41
9.6.1. Проверка файлов в PT Sandbox 41
9.6.1.1. О модуле «Проверка файлов в PT Sandbox» 41
9.6.1.2. Настройка модуля «Проверка файлов в PT Sandbox» 42
9.6.1.3. Отправка файлов на проверку в PT Sandbox вручную 43
9.6.1.4. Получение данных о проверенных файлах 43
9.6.2. Сканирование в режиме аудита (MaxPatrol VM) 44
9.6.2.1. О модуле «Сканирование в режиме аудита (MaxPatrol VM)» 44
9.6.2.2. Настройка модуля «Сканирование в режиме аудита (MaxPatrol VM)» 45
9.6.2.3. Ручной запуск сканирования 46
9.6.2.4. Отключение запуска сканирования по расписанию 47
9.6.2.5. Просмотр результатов сканирования 48
9.6.3. Отправка событий на syslog-сервер 49
9.6.4. Отправка файлов 49
10. Настройка автоматического реагирования 51
10.1. Назначение действий на событие модуля 51
10.2. Массовое назначение действия на события модуля 52
11. Назначение политики на группу агентов 55
12. О технической поддержке 56
Глоссарий 60

1. Об этом документе

Это руководство содержит информацию и инструкции для первоначальной настройки MaxPatrol Endpoint Detection and Response (далее также — MaxPatrol EDR).

Комплект документации MaxPatrol EDR включает в себя следующие документы:

— Этот документ.

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

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

2. О MaxPatrol EDR

MaxPatrol Endpoint Detection and Response — система на базе платформы MaxPatrol 10, предназначенная для защиты конечных устройств от киберугроз. Собирая и анализируя данные из множества систем, MaxPatrol EDR выявляет в IT-инфраструктуре организации сложные целевые атаки и автоматически реагирует на них.

При обнаружении угроз MaxPatrol EDR 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;
- отправить данные о событиях ИБ на syslog-сервер.

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 EDR

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

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 сервер агентов и 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, сервера агентов и пересылаются в базу данных MaxPatrol SIEM.
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.

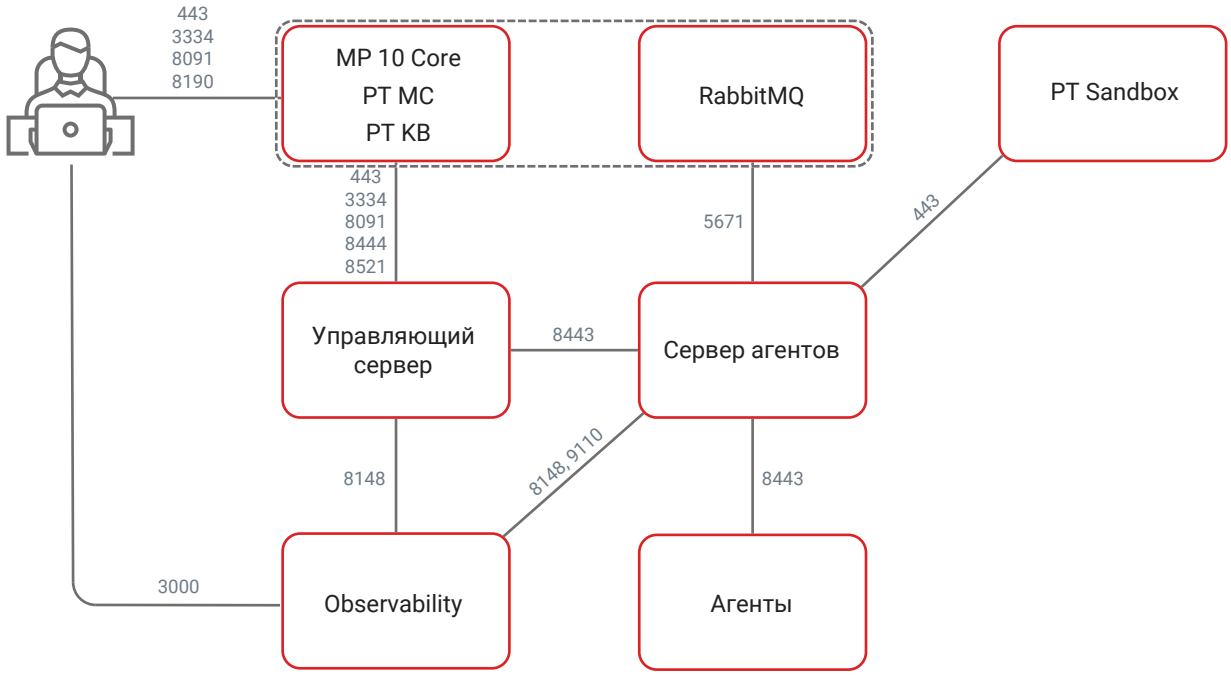

Рисунок 1. Взаимодействие компонентов MaxPatrol EDR

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

Примечание. Если какие-либо компоненты MaxPatrol EDR расположены на одном сервере, то обеспечивать внешнюю доступность портов при их взаимодействии необязательно. Например, при установке всех компонентов на один сервер открывать порты 5431, 8148, 8443, 9000, 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, 8444, 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)
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	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
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 EDR 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 EDR запросите у администратора PT MC логин и пароль вашей учетной записи и убедитесь, что в браузере разрешены всплывающие окна.

► Чтобы войти в MaxPatrol EDR:

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

   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 EDR 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 вами учетные данные. Если вы указали верные данные, откроется стартовая страница с системным дашбордом MaxPatrol EDR. Если вы указали неверные данные, отобразится сообщение об ошибке.

5. Интерфейс MaxPatrol EDR

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

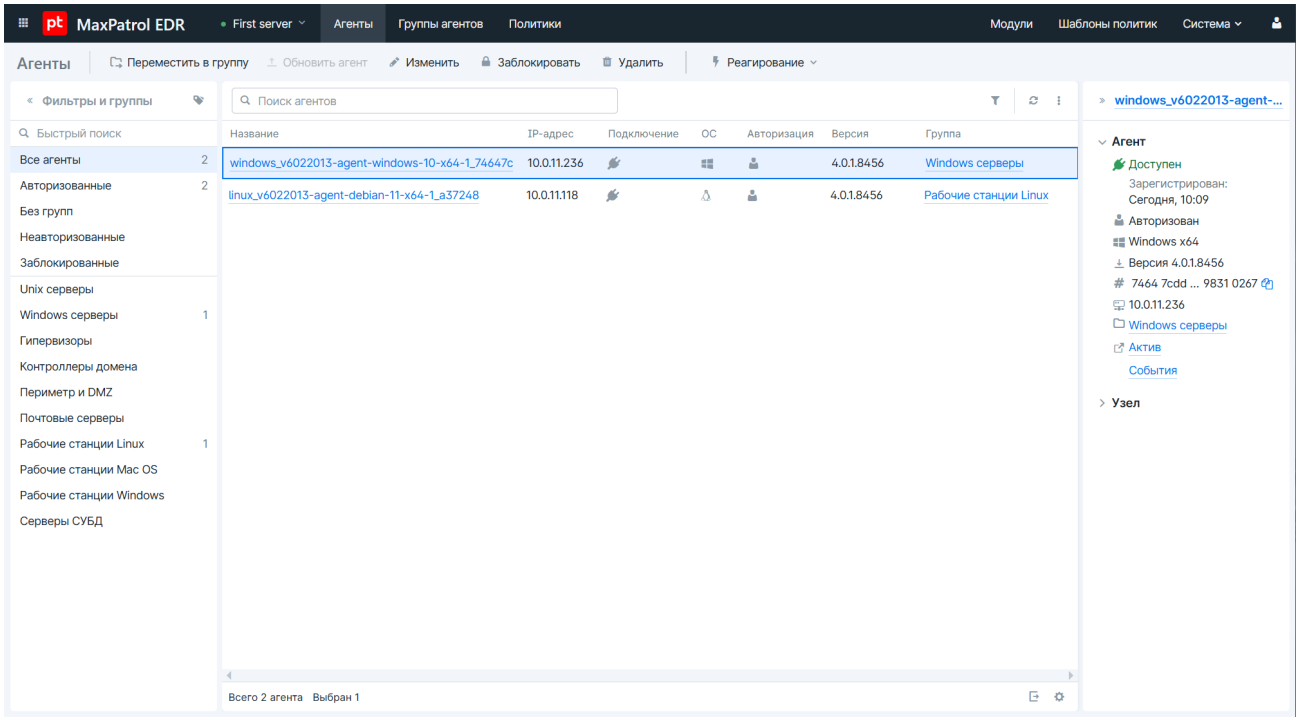

Рисунок 2. Страница **Агенты EDR**

Веб-интерфейс MaxPatrol EDR 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 кнопки:

— для перехода из MaxPatrol EDR к другим приложениям;

— для выбора языка интерфейса и выхода из MaxPatrol EDR.

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 EDR

После установки MaxPatrol EDR 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 EDR 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 раздел **Агенты**.
  2. Выберите фильтр **Неавторизованные**.
  3. Выберите агент.

     Примечание. Вы можете выбрать несколько агентов, удерживая клавишу Ctrl или Shift.
  4. Нажмите **Переместить в группу**.
  5. Выберите группу, в которую вы хотите добавить агент, или введите название новой группы.
  6. Нажмите **Переместить**.

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 **EDR** → **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 существующие метки для быстрого поиска политики или задайте свои.
  6. Нажмите **Создать**.

Вы также можете создавать копии существующих политик.

9. Настройка модулей и работа с ними

Далее приведена подробная информация о каждом модуле, а также даны инструкции по настройке и работе с ними.

В этом разделе

Системные модули (см. раздел 9.1)

Модули доставки и установки (см. раздел 9.2)

Модули сбора (см. раздел 9.3)

Модули обнаружения (см. раздел 9.4)

Модули реагирования (см. раздел 9.5)

Модули интеграции (см. раздел 9.6)

9.1. Системные модули

В этом разделе приведена информация о системных модулях.

Ядро (внутренний сервис)

Этот модуль предоставляет библиотеку среды выполнения для работы модулей «Конфигуратор аудита Windows» и «ETW: трассировка событий Windows».

9.2. Модули доставки и установки

В этом разделе приведена информация по модулям доставки и установки.

В этом разделе

Установщик Sysmon (см. раздел 9.2.1)

Установщик auditd (см. раздел 9.2.2)

Конфигуратор аудита Windows (см. раздел 9.2.3)

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».

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 EDR 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 EDR.

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.

9.3. Модули сбора

В этом разделе приведена информация о модулях сбора.

В этом разделе

WinEventLog: сбор данных из журнала событий Windows (см. раздел 9.3.1)

ETW: трассировка событий Windows (см. раздел 9.3.2)

Сбор данных из файлов журналов (см. раздел 9.3.3)

Сбор данных о состоянии системы (см. раздел 9.3.4)

Нормализатор (см. раздел 9.3.5)

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 **EDR** → **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.

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 4. 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

Сбор данных

- Чтобы собрать данные о состоянии системы вручную:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите собрать данные.
  3. Выберите модуль «Сбор данных о состоянии системы».
  4. Нажмите ⚙.

5. В раскрывающемся списке выберите, какие данные вы хотите собрать.
6. Нажмите **Собрать данные**.

Просмотр данных

- Чтобы просмотреть данные:

1. В главном меню выберите раздел **Агенты**.
2. Нажмите на название агента, на котором установлен модуль «Сбор данных о состоянии системы».
3. Выберите модуль «Сбор данных о состоянии системы».
4. Нажмите ⚙.
5. Выберите вкладку с типом данных.
6. В списке слева выберите отчет о собранных данных.

   Примечание. Если после сбора данных в параметрах политики был изменен параметр **Пароль для архива**, то просмотреть собранные данные в интерфейсе MaxPatrol EDR невозможно.

Скачивание архива с данными

- Чтобы скачать архив с данными:

1. В главном меню выберите раздел **Агенты**.
2. Нажмите на название агента, на котором установлен модуль «Сбор данных о состоянии системы».
3. Выберите модуль «Сбор данных о состоянии системы».
4. Нажмите ⚙.
5. Выберите вкладку с типом данных.
6. Установите флажки напротив отчетов, которые вы хотите скачать.

   Примечание. Если после сбора данных в параметрах политики был изменен параметр **Пароль для архива**, то скачать собранные данные невозможно.
7. Нажмите **Скачать**.

Вы также можете скачать архив с одним отчетом по кнопке ⬇.

Создание дампа памяти процесса

После создания дамп будет сохранен в хранилище на агенте.

- Чтобы создать дамп процесса:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Сбор данных о состоянии системы».
  3. Выберите модуль «Сбор данных о состоянии системы».
  4. Нажмите ⚙.
  5. Введите идентификатор процесса и нажмите **Создать дамп**.

Скачивание дампа памяти процесса

Вы можете скачать только один дамп за один раз. Также невозможно скачивание дампа вместе с другими собранными данными в архиве.

- Чтобы скачать дамп процесса:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Сбор данных о состоянии системы».
  3. Выберите модуль «Сбор данных о состоянии системы».
  4. Нажмите ⚙.
  5. В журнале выберите дамп и нажмите **Скачать дамп**.

     Скачивание дампа начнется после завершения пересылки дампа в хранилище на сервере агентов.

     Примечание. Отправка на сервер дампов большого размера может занимать длительное время.

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)

9.4.1. Коррелятор

Далее приведена информация о модуле «Коррелятор» и инструкции по его настройке.

В этом разделе

О модуле «Коррелятор» (см. раздел 9.4.1.1)

Работа с исключениями (см. раздел 9.4.1.2)

9.4.1.1. О модуле «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.

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».

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 EDR. 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**.

9.4.1.2. Работа с исключениями

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 условий в формате регулярных выражений (regex) в параметрах модуля.

Исключения с помощью табличных списков

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 EDR (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 EDR не требуется установка пакета экспертизы в MaxPatrol SIEM.

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

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 **EDR** → **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.

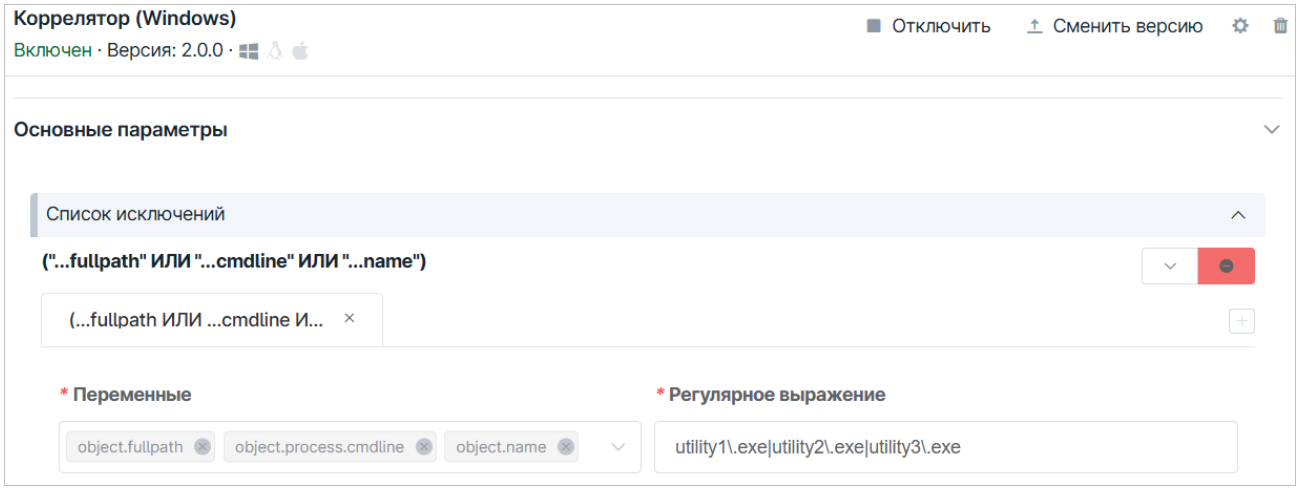

Рисунок 3. Добавление исключения

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 `_rule`, а в поле **Регулярное выражение** — имя правила.

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

9.4.2. YARA-сканер

Далее приведена информация о модуле «YARA-сканер» и инструкции по работе с ним.

В этом разделе

О модуле «YARA-сканер» (см. раздел 9.4.2.1)

О кэшировании результатов проверок (см. раздел 9.4.2.2)

Запуск проверки вручную (см. раздел 9.4.2.3)

Просмотр результатов проверки (см. раздел 9.4.2.4)

Просмотр правил (см. раздел 9.4.2.5)

9.4.2.1. О модуле «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.

Таблица 5. 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 (см. раздел 9.4.2.3)
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 EDR запускается под системной учетной записью, поэтому значение переменной окружения `%userprofile%` — `C:\Windows\System32\config\systemprofile`
Список исключений для YARA-правил	Список идентификаторов YARA-правил, которые не будут использоваться для проверок
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

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

9.4.2.2. О кэшировании результатов проверок

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 EDR 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 EDR проверяет сохраненные результаты и использует их, если такой файл или процесс уже проверялся. MaxPatrol EDR идентифицирует файлы по хеш-сумме, а процессы по идентификатору и пути к исполняемому файлу.

Если модуль взял результат сканирования из кэша, то к названию зарегистрированного события добавляется префикс `[Кэш]`. Для проверки наиболее важных файлов и процессов вы можете использовать специальные действия модуля (см. раздел 10), которые не будут брать результаты из кэша.

9.4.2.3. Запуск проверки вручную

Модуль «YARA-сканер» выполняет сигнатурный анализ на основе правил YARA. Вы можете проверить:

- файл или папку с файлами;
- один или несколько процессов;
- важные системные файлы и процессы (быстрая проверка);
- все файлы и процессы (полная проверка).

По умолчанию для проверки выбраны правила YARA, заданные в конфигурации политики. Вы можете вставить или импортировать свои правила для проверки.

Проверки выполняются в порядке очереди. При этом в конфигурации политики вы можете назначить автоматические проверки, которые будут выполняться в приоритетном порядке, вне очереди.

► Чтобы запустить проверку:

1. В главном меню выберите раздел **Агенты**.
2. Нажмите на название агента, на котором вы хотите запустить проверку.
3. Выберите модуль «YARA-сканер».
4. Нажмите ⚙.
5. Нажмите **Новая проверка**.
6. Задайте параметры проверки.
7. Нажмите **Начать проверку**.

9.4.2.4. Просмотр результатов проверки

Вы можете просмотреть список вредоносных файлов и процессов, которые были найдены с помощью правил YARA. Для каждого файла и процесса указано правило, которым они были обнаружены, и его точность (от 0 до 15). Чем выше точность правила, тем меньше ложных срабатываний оно выдает.

► Чтобы просмотреть результаты проверки:

1. В главном меню выберите раздел **Агенты**.
2. Нажмите на название агента, на котором запускалась проверка модулем «YARA-сканер».
3. Выберите модуль «YARA-сканер».

4. Нажмите ⚙.
5. Нажмите на дату и время начала проверки.

   Отобразятся результаты проверки.

9.4.2.5. Просмотр правил

Вы можете просмотреть список правил YARA и информацию о них. Эта информация может быть полезна при настройке модуля в политике. Например, вы можете отключить проверки на некоторые семейства вредоносного ПО.

- Чтобы просмотреть правила:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «YARA-сканер».
  3. Выберите модуль «YARA-сканер».
  4. Нажмите ⚙.
  5. Выберите раздел **Правила**.

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 EDR регулярно получает обновления базы данных новых угроз.

В конфигурации модуля задается максимальный размер файла, который может быть проверен (в мегабайтах). Это ограничение относится только к автоматическому реагированию.

- Чтобы вручную проверить файл по хеш-сумме:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, файл с которого вы хотите проверить.
  3. Выберите модуль «Проверка файла по хеш-сумме».
  4. Нажмите ⚙.
  5. Введите полный путь к файлу.
  6. Нажмите **Проверить**.

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 6. 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

9.5. Модули реагирования

В этом разделе приведена информация о модулях реагирования.

В этом разделе

Удаление файлов (см. раздел 9.5.1)

Завершение процессов (см. раздел 9.5.2)

Блокировка учетных записей (см. раздел 9.5.3)

Изоляция узлов (см. раздел 9.5.4)

Блокировка по IP-адресу (см. раздел 9.5.5)

Перенаправление DNS-запросов (sinkholing) (см. раздел 9.5.6)

Карантин (см. раздел 9.5.7)

Запуск командной оболочки (см. раздел 9.5.8)

Интерпретатор языка Lua (см. раздел 9.5.9)

9.5.1. Удаление файлов

- Чтобы удалить файл на конечном устройстве:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, установленного на конечном устройстве.
  3. Выберите модуль «Удаление файлов».
  4. Нажмите ⚙.
  5. Нажмите **Выбрать действие** и в раскрывшемся меню выберите действие.
  6. Введите путь к файлу.
  7. Нажмите **Выполнить действие**.

9.5.2. Завершение процессов

Вы можете завершить:

- все процессы, запущенные указанным исполняемым файлом;
- все процессы с указанным именем;
- процесс с указанными именем и идентификатором;
- родительские процессы с указанными именами и идентификаторами;
- дерево процессов (нужно указать имя и идентификатор родительского процесса);
- несколько деревьев процессов (нужно указать имя родительского процесса).

  Примечание. В конфигурации модуля «Завершение процессов» вы можете задать список исполняемых файлов процессов, которые не будут завершаться модулем.

- Чтобы завершить процессы на конечном устройстве:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, установленного на конечном устройстве.

3. Выберите модуль «Завершение процессов».
4. Нажмите ⚙.
5. Нажмите **Выбрать действие** и в раскрывшемся меню выберите **Завершить все процессы, используя имя**.
6. Введите имя процесса в формате `{"proc_name": "<Имя процесса>"}`.
7. Нажмите **Выполнить действие**.

9.5.3. 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 7. 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

Блокировка локальных учетных записей

Вы можете вручную заблокировать и разблокировать локальную учетную запись в операционной системе. Длительность блокировки определяется соответствующим параметром для действия «Заблокировать учетную запись (объект) по логину» в конфигурации политики.

- Чтобы заблокировать учетную запись:
  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, в операционной системе которого вы хотите заблокировать учетную запись.
  3. Выберите модуль «Блокировка учетных записей».

4. Нажмите ⚙.
5. Напротив учетной записи в списке нажмите **Заблокировать**.

Учетная запись заблокирована.

- Чтобы досрочно разблокировать учетную запись,

  нажмите **Разблокировать**.

Завершение сеансов локальных учетных записей

Вы можете вручную завершить сеанс локальной учетной запись в операционной системе.

Примечание. Завершить сеанс учетной записи root в Linux невозможно.

- Чтобы завершить сеанс учетной записи:

1. В главном меню выберите раздел **Агенты**.
2. Нажмите на название агента, в операционной системе которого вы хотите завершить сеанс учетной записи.
3. Выберите модуль «Блокировка учетных записей».
4. Нажмите ⚙.
5. Напротив учетной записи в списке нажмите **Завершить сеанс**.

Вы также можете завершить все активные сеансы по кнопке **Завершить активные сеансы**.

9.5.4. 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 EDR не требуется: обмен данных с ним не будет блокироваться.

- Чтобы изолировать узел, на котором установлен агент:

1. В главном меню выберите раздел **Агенты**.
2. Нажмите на название агента.
3. Выберите модуль «Изоляция узлов».

4. Нажмите ⚙.
5. Выберите способ изоляции узла.
6. Настройте время, через которое изоляция узла будет снята автоматически.
7. Нажмите **Изолировать**.

   Примечание. Вы можете обновить статус изоляции узла по кнопке ↻.

Узел изолирован.

- Чтобы досрочно снять частичную изоляцию узла,

  нажмите **Снять изоляцию**.

  Примечание. Для досрочного снятия полной изоляции узла вам нужно включить сетевые адаптеры на устройстве вручную.

9.5.5. Блокировка по IP-адресу

Модуль «Блокировка по IP-адресу» блокирует все сетевые соединения по IP-адресу. Адрес может быть заблокирован на уровне политики, агента или на обоих уровнях. Блокировка полезна, если вы обнаружили подозрительное соединение и хотите его прервать. Если IP-адрес заблокирован на уровне политики, вы можете дополнительно заблокировать его на агенте. В таком случае соединения узла с этим адресом не будут разблокированы даже после изменения конфигурации модуля в политике. Заблокировать IP-адрес сервера MaxPatrol EDR невозможно.

- Чтобы заблокировать IP-адрес на агенте:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите заблокировать IP-адрес.
  3. Выберите модуль «Блокировка по IP-адресу».
  4. Нажмите ⚙.
  5. Введите IP-адрес в формате IPv4, IPv6 или подсеть в нотации CIDR.
  6. Нажмите **Заблокировать**.

  IP-адрес заблокирован на агенте.

- Чтобы разблокировать IP-адрес на агенте,

  напротив IP-адреса в списке нажмите **Разблокировать**.

  Примечание. Соединения с этим IP-адресом не восстановятся, если он заблокирован на уровне политики.

9.5.6. Перенаправление DNS-запросов (sinkholing)

Далее приведена информация о модуле «Перенаправление DNS-запросов (sinkholing)» и инструкции по работе с ним.

В этом разделе

О модуле «Перенаправление DNS-запросов (sinkholing)» (см. раздел 9.5.6.1)

Настройка модуля «Перенаправление DNS-запросов (sinkholing)» (см. раздел 9.5.6.2)

Перенаправление DNS-запросов вручную (см. раздел 9.5.6.3)

9.5.6.1. О модуле «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 8. 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

9.5.6.2. Настройка модуля «Перенаправление DNS-запросов (sinkholing)»

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

  1. В главном меню выберите **EDR** → **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**.

9.5.6.3. Перенаправление DNS-запросов вручную

Если вы заметили на узле подозрительный или вредоносный трафик с какого-либо домена, вы можете перенаправить все DNS-запросы с этого домена на специальный адрес, заданный в конфигурации модуля (см. раздел 9.5.6.2) в политике.

- Чтобы перенаправить DNS-запросы с домена:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите перенаправлять DNS-запросы.
  3. Выберите модуль «Перенаправление DNS-запросов (sinkholing)».
  4. Нажмите ⚙.
  5. Введите один или несколько доменов, трафик с которых нужно перенаправлять.
  6. Нажмите **Добавить**.

  DNS-запросы с домена перенаправлены.

- Чтобы отменить перенаправление DNS-запросов,

  напротив домена в списке нажмите **Удалить**.

  Примечание. Отменить перенаправление DNS-запросов с доменов, которые заданы в политике, можно только в политике.

9.5.7. Карантин

Далее приведена информация о модуле «Карантин» и инструкции по работе с ним.

В этом разделе

О модуле «Карантин» (см. раздел 9.5.7.1)

Изоляция файла вручную (см. раздел 9.5.7.2)

Восстановление файла из карантина (см. раздел 9.5.7.3)

Удаление файла из карантина (см. раздел 9.5.7.4)

Скачивание файла из карантина (см. раздел 9.5.7.5)

9.5.7.1. О модуле «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 9. 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)

Параметр или блок параметров	Описание
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

9.5.7.2. Изоляция файла вручную

Вы можете поместить копию подозрительного файла в карантин на время его проверки. После этого в целях безопасности рекомендуется удалить сам файл (см. раздел 9.5.1).

- Чтобы поместить копию файла в карантин:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите поместить файл в карантин.
  3. Выберите модуль «Карантин».
  4. Нажмите .
  5. Введите путь к файлу.
  6. Нажмите **Изолировать файл**.

9.5.7.3. Восстановление файла из карантина

Если вы убедились, что файл безопасный, вы можете вручную восстановить его из карантина.

- Чтобы вручную восстановить файл из карантина:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите восстановить файл из карантина.
  3. Выберите модуль «Карантин».
  4. Нажмите .
  5. Напротив файла в списке нажмите .

  Примечание. Если в конфигурации политики после помещения файла в карантин был изменен пароль для архива, то файл восстановлен не будет. В таком случае для восстановления файла необходимо вернуть старый пароль.

9.5.7.4. Удаление файла из карантина

Если файл признан вредоносным, он будет окончательно удален из карантина по ротации. Вы также можете окончательно удалить его вручную.

- Чтобы окончательно удалить файл:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите окончательно удалить файл.
  3. Выберите модуль «Карантин».
  4. Нажмите ⚙.
  5. Напротив файла в списке нажмите 🗑.

Вы также можете удалить все файлы из карантина по кнопке **Удалить все** или несколько выбранных по кнопке **Удалить выбранные**.

9.5.7.5. Скачивание файла из карантина

Если файл признан вредоносным, вы можете скачать его из карантина и передать на исследование экспертам. Скачанный файл будет помещен в архив с паролем, который задается в конфигурации (см. раздел 9.5.7.1).

- Чтобы скачать файл из карантина:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите скачать файл из карантина.
  3. Выберите модуль «Карантин».
  4. Нажмите ⚙.
  5. Напротив файла в списке нажмите ⬇.

Вы также можете скачать архив со всеми файлами в карантине. Для этого вам нужно выделить файлы в списке и нажать кнопку **Скачать архив**.

9.5.8. Запуск командной оболочки

Модуль «Запуск командной оболочки» позволяет выполнять команды в PowerShell или Bash на конечном устройстве из веб-интерфейса MaxPatrol EDR. 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 10. 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

Выполнение команд в оболочке

- Чтобы выполнить команду в оболочке:
  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите выполнить команду.
  3. Выберите модуль «Запуск командной оболочки».
  4. Нажмите ⚙.
  5. Нажмите **Запустить**.
  6. Введите команду и нажмите клавишу Enter.

Скачивание журнала выполненных команд

- Чтобы скачать журнал выполненных команд:
  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Запуск командной оболочки».
  3. Выберите модуль «Запуск командной оболочки».
  4. Нажмите ⚙.
  5. Выберите вкладку **Журнал**.
  6. Выберите одну или несколько записей в журнале.
  7. Нажмите ⬇.

9.5.9. Интерпретатор языка Lua

Модуль «Интерпретатор языка Lua» предоставляет возможность для выполнения произвольного кода на языке Lua на агенте.

- Чтобы выполнить произвольный код на языке Lua:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите выполнить код.
  3. Выберите модуль «Интерпретатор языка Lua».
  4. Нажмите  .
  5. Введите код.
  6. Нажмите **Выполнить**.

9.6. Модули интеграции

В этом разделе приведена информация о модулях интеграции.

В этом разделе

Проверка файлов в PT Sandbox (см. раздел 9.6.1)

Сканирование в режиме аудита (MaxPatrol VM) (см. раздел 9.6.2)

Отправка событий на syslog-сервер (см. раздел 9.6.3)

Отправка файлов (см. раздел 9.6.4)

9.6.1. Проверка файлов в PT Sandbox

Далее приведена информация о модуле «Проверка файлов в PT Sandbox» и инструкции по работе с ним.

В этом разделе

О модуле «Проверка файлов в PT Sandbox» (см. раздел 9.6.1.1)

Настройка модуля «Проверка файлов в PT Sandbox» (см. раздел 9.6.1.2)

Отправка файлов на проверку в PT Sandbox вручную (см. раздел 9.6.1.3)

Получение данных о проверенных файлах (см. раздел 9.6.1.4)

9.6.1.1. О модуле «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.

Для проверки файлов с конечных устройств в PT Sandbox должны быть доступны образы win10-1803-x64 (для файлов из Windows) и redos-murom-x64 (для файлов из Linux).

Таблица 11. Параметры модуля «Проверка файлов в PT Sandbox»

Параметр или блок параметров	Описание
Ключ API	Ключ для доступа к публичному API PT Sandbox. Для генерации ключа API вам нужно выполнить команду `sudo ptmsctl api auth create <Название ключа API>` в консольной утилите PT Sandbox
Глубина распаковки архивов	Максимальное количество вложенных друг в друга архивов, которые будут распаковываться при проверке. Увеличение глубины распаковки архивов снижает скорость проверки. Если распаковывать архивы не требуется, вы можете ввести `0`, тогда архивы будут проверяться как обычные файлы
Продолжительность наблюдения за файлом	Максимальное время наблюдения за файлом в ОС в секундах
Максимальный размер файла	Максимальный размер файла, который вы можете отправить на проверку в PT Sandbox
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
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

9.6.1.2. Настройка модуля «Проверка файлов в PT Sandbox»

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

  1. В главном меню выберите **EDR** → **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 ключ для доступа к публичному API PT Sandbox.

   Примечание. Для генерации ключа API вам нужно выполнить команду `sudo ptmsctl api auth create <Название ключа API>` в консольной утилите PT Sandbox. Подробная инструкция по генерации ключа API приведена в разделе «Генерация токена доступа» в Справочном руководстве по публичному API из комплекта поставки PT Sandbox.

6. Если требуется, задайте дополнительные параметры модуля.
7. Если требуется, выберите действия, которые будут выполняться при регистрации событий ИБ (см. раздел 10).
8. Нажмите **Сохранить**.

9.6.1.3. Отправка файлов на проверку в PT Sandbox вручную

- Чтобы отправить файл с конечного устройства на проверку в PT Sandbox:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, установленного на конечном устройстве.
  3. Выберите модуль «Проверка файлов в PT Sandbox».
  4. Нажмите ⚙.
  5. Введите путь к файлу.
  6. Если требуется, отключите поведенческий анализ файла.

     Без поведенческого анализа проверка пройдет быстрее.

  7. Нажмите **Проверить файл**.

9.6.1.4. Получение данных о проверенных файлах

Информация о файлах, отправленных на проверку с агента в PT Sandbox, содержится в таблице `files` в базе данных агента. Информация обо всех проверенных файлах со всех агентов с такой же политикой содержится в таблице `feeds` в базах данных и агента, и сервера MaxPatrol EDR. Вы можете получить данные о проверенных файлах с помощью SQL-запроса к базе данных агента или сервера.

- Чтобы получить информацию о проверенных в PT Sandbox файлах:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Проверка файлов в PT Sandbox».
  3. Выберите модуль «Проверка файлов в PT Sandbox».

4. Нажмите ⚙.
5. Если требуется, измените SQL-запрос.
6. Выберите базу данных, из которой вы хотите получить данные.
7. Нажмите **Выполнить запрос**.

9.6.2. Сканирование в режиме аудита (MaxPatrol VM)

Далее приведена информация о модуле «Сканирование в режиме аудита (MaxPatrol VM)» и инструкции по работе с ним.

В этом разделе

О модуле «Сканирование в режиме аудита (MaxPatrol VM)» (см. раздел 9.6.2.1)

Настройка модуля «Сканирование в режиме аудита (MaxPatrol VM)» (см. раздел 9.6.2.2)

Ручной запуск сканирования (см. раздел 9.6.2.3)

Отключение запуска сканирования по расписанию (см. раздел 9.6.2.4)

Просмотр результатов сканирования (см. раздел 9.6.2.5)

9.6.2.1. О модуле «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 EDR 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 12. 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

Параметр или блок параметров	Описание
	версию ниже используемой, то в результатах будут неполные данные. Если выше — результаты сканирования обработаны не будут. **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
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

9.6.2.2. Настройка модуля «Сканирование в режиме аудита (MaxPatrol VM)»

Вы можете настроить запуск сканирования в режиме аудита по расписанию или при регистрации события ИБ, а также запускать его вручную (см. раздел 9.6.2.3). 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 EDR 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 **EDR** → **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, задайте дополнительные параметры модуля.
  7. Если требуется, выберите действия, которые будут выполняться при регистрации событий ИБ (см. раздел 10).
  8. Нажмите **Сохранить**.

9.6.2.3. Ручной запуск сканирования

Запуск сканирования на одном агенте

Вы можете вручную запустить сканирование в режиме аудита на агенте. Если на агенте уже выполняется сканирование, то оно не будет запущено повторно.

- Чтобы запустить сканирование:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите запустить сканирование.
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Нажмите **Запустить сканирование**.

  Сканирование запущено. Вы можете остановить сканирование по кнопке **Остановить сканирование**.

Скачать журнал работы модуля вы можете по кнопке **Скачать журнал модуля**.

Запуск сканирования на всех агентах группы

Вы можете вручную запустить сканирование в режиме аудита сразу на всех агентах группы. Сканирование на агенте из группы не будет запущено, если с ним нет связи или на нем уже выполняется сканирование.

- Чтобы запустить сканирование на всех агентах группы:

  1. В главном меню выберите раздел **Группы агентов**.
  2. Нажмите на название группы, на агентах которой вы хотите запустить сканирование.
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Нажмите **Запустить сканирование**.

9.6.2.4. Отключение запуска сканирования по расписанию

Вы можете отключить запуск сканирования по расписанию. В этом случае сканирование будет запускаться только вручную — или при регистрации того или иного события ИБ, если это было настроено в политике.

Отключения запуска по расписанию на одном агенте

- Чтобы отключить запуск сканирования по расписанию:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором вы хотите отключить запуск сканирования по расписанию.
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Нажмите **Отключить запуск по расписанию**.

  Запуск сканирования по расписанию отключен. Вы можете повторно включить запуск по расписанию по кнопке **Включить запуск по расписанию**.

Отключения запуска по расписанию на всех агентах группы

- Чтобы отключить запуск сканирования по расписанию для группы агентов:

  1. В главном меню выберите раздел **Группы агентов**.
  2. Нажмите на название группы, для агентов которой вы хотите отключить запуск сканирования по расписанию.

     Откроется карточка группы агентов.
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Нажмите **Отключить запуск по расписанию**.

  Запуск сканирования по расписанию отключен. Вы можете повторно включить запуск по расписанию по кнопке **Включить запуск по расписанию**.

9.6.2.5. Просмотр результатов сканирования

Просмотр результатов сканирования на одном агенте

- Чтобы просмотреть результаты сканирования:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, на котором установлен модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».
  4. Нажмите ⚙.
  5. Выберите раздел **Сканирования**.

     Отобразятся результаты сканирования узла.

Просмотр результатов сканирования на всех агентах группы

- Чтобы просмотреть результаты сканирования:

  1. В главном меню выберите раздел **Группы агентов**.
  2. Нажмите на название группы, на которую назначена политика с модулем «Сканирование в режиме аудита (MaxPatrol VM)».
  3. Выберите модуль «Сканирование в режиме аудита (MaxPatrol VM)».

4. Нажмите ⚙.
5. Выберите раздел **Сканирования**.

   Отобразятся результаты последнего сканирования всех узлов группы.

9.6.3. Отправка событий на syslog-сервер

Модуль «Отправка событий на syslog-сервер» отправляет системные события и записи о событиях ИБ на syslog-сервер, адрес которого задается в конфигурации. Для автоматической отправки событий ИБ на syslog-сервер в политике должно настроено действие «Отправить событие на syslog-сервер» (см. раздел 10). Вы также можете вручную отправлять события из карточки модуля на агенте.

Внимание! Системные события отправляются только в нормализованном виде, поэтому на всех агентах должен быть установлен и включен модуль «Нормализатор». Системные события, для которых нет правил нормализации, не будут отправлены на syslog-сервер.

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 13. 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

Отправка файла вручную

- Чтобы отправить файл:

  1. В главном меню выберите раздел **Агенты**.
  2. Нажмите на название агента, файл с которого вы хотите отправить во внешнюю систему.
  3. Выберите модуль «Отправка файлов».
  4. Нажмите ⚙.

5. Введите путь к файлу.
6. Нажмите **Отправить файл**.

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

Назначение действий на событие модуля (см. раздел 10.1)

Массовое назначение действия на события модуля (см. раздел 10.2)

10.1. Назначение действий на событие модуля

► Чтобы назначить действия на событие модуля:

1. В главном меню выберите **EDR** → **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 .

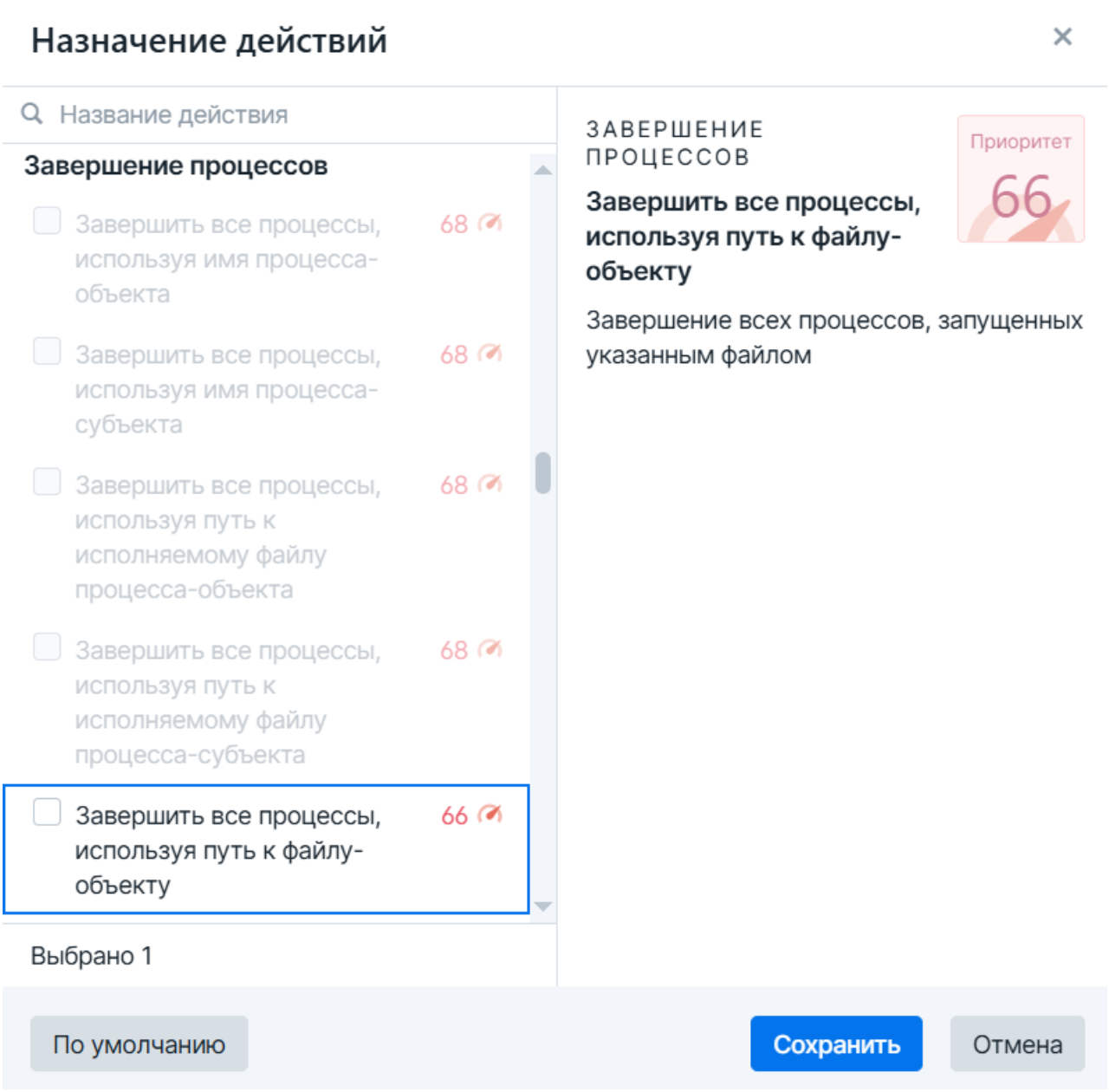

Рисунок 4. Назначение действий

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

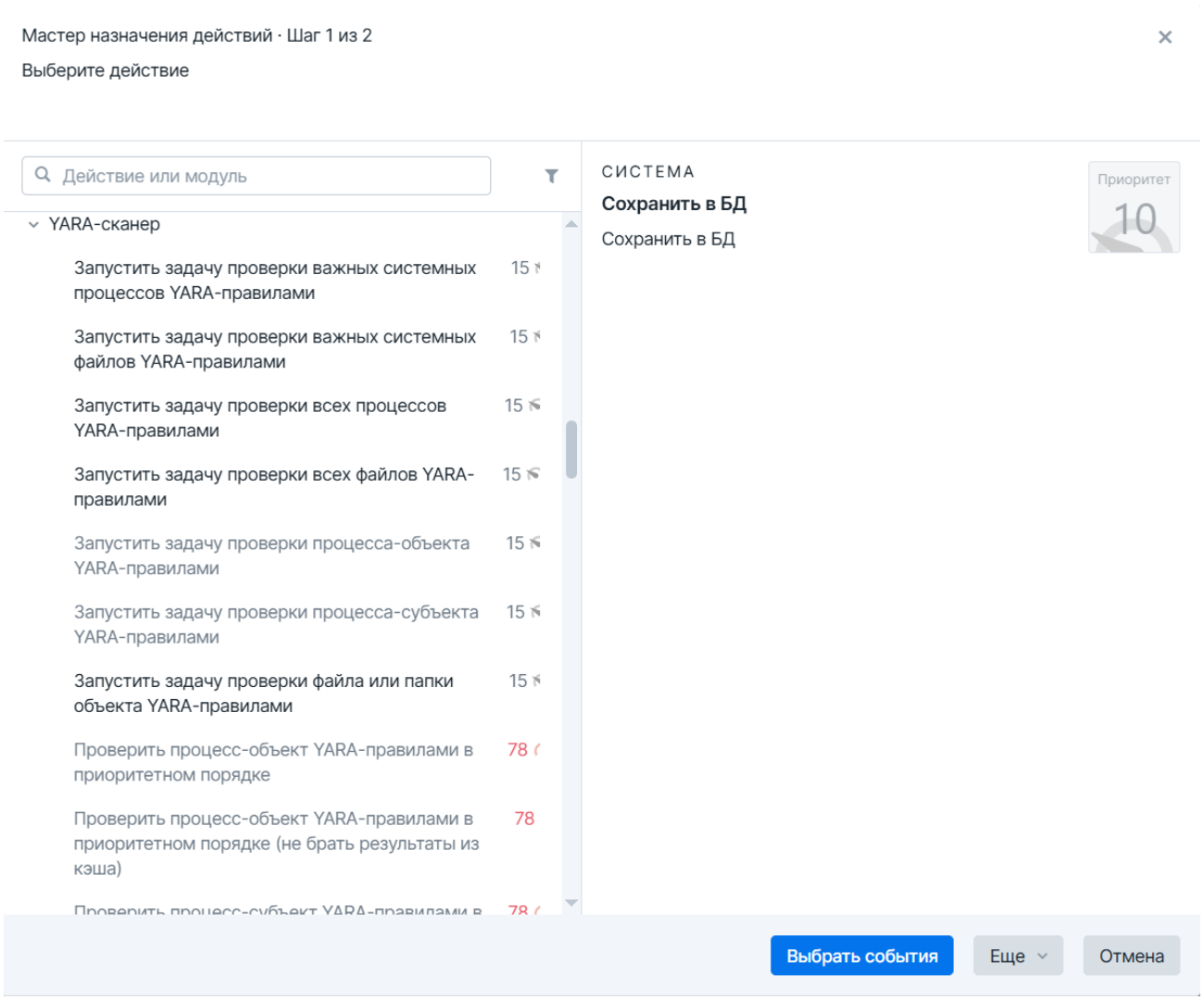

Рисунок 5. Выбор действия

  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 кнопку **Еще** и в раскрывшемся меню выбрав пункт **Назначить на все доступные события**.

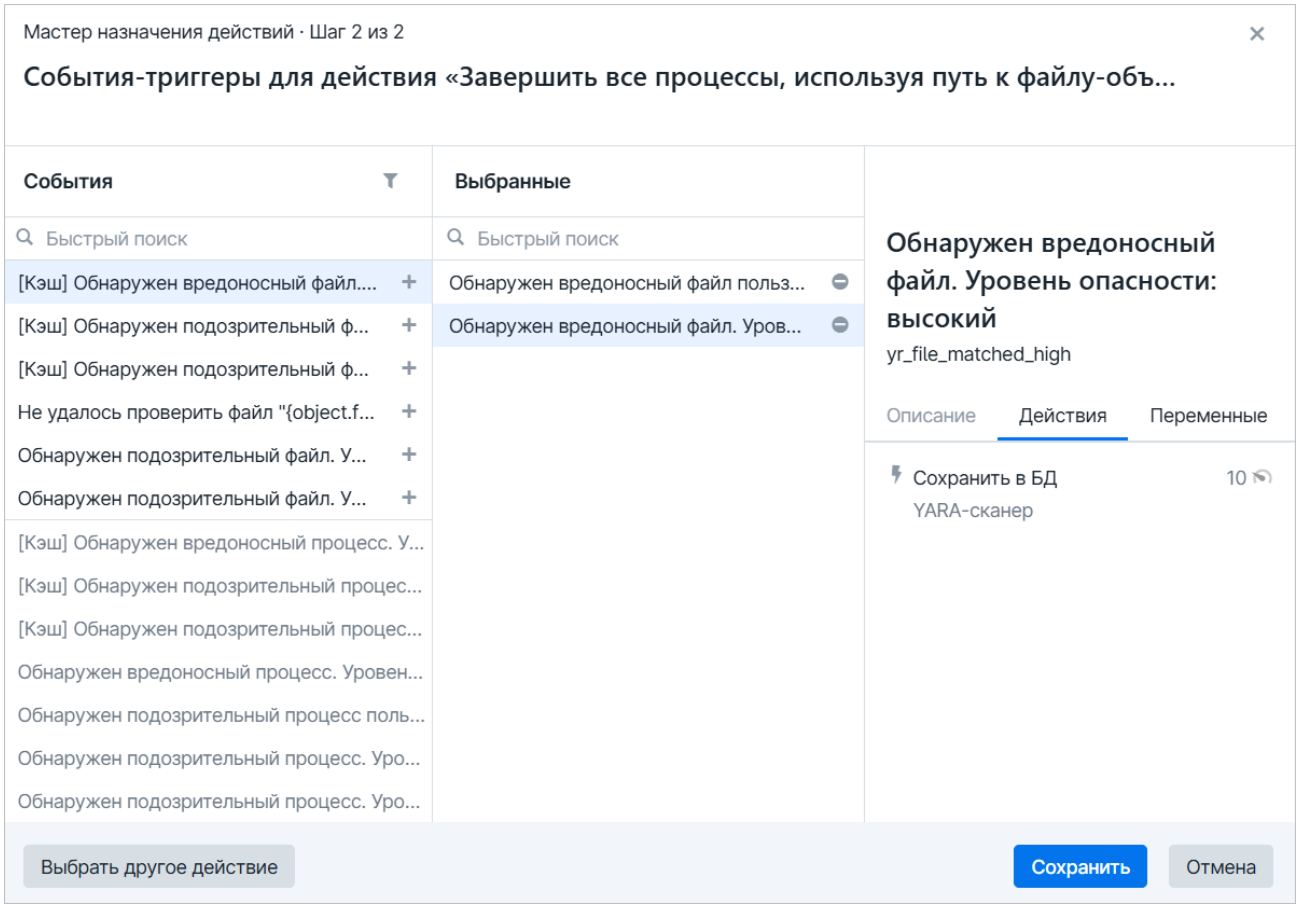

Рисунок 6. Выбор событий

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 **EDR** → **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 EDR 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 14. 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. Наши технологии используют около 3000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.