Positive Technologies Application Inspector Enterprise Edition

Версия 4.1.0

Руководство администратора

POSITIVE TECHNOLOGIES

Дата редакции документа: 22.07.2022

Содержание

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по развертыванию, настройке и администрированию Positive Technologies Application Inspector Enterprise Edition (далее также — PT AI Enterprise Edition). Руководство не содержит инструкций по использованию основных функций продукта.

Руководство адресовано специалистам, выполняющим установку, первоначальную настройку и администрирование PT AI Enterprise Edition.

Комплект документации PT AI Enterprise Edition включает в себя следующие документы:

— Этот документ.

— Руководство пользователя — содержит подробную информацию о сценариях работы с продуктом, о настройке функций продукта для решения конкретных задач.

— Руководство по интеграции PT AI Enterprise Edition в сборочный процесс — содержит рекомендации по внедрению анализа кода в сборочный процесс различных CI-систем.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о PT AI Enterprise Edition (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам

Пример	Описание
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT AI Enterprise Edition

Вы можете найти дополнительную информацию о PT AI Enterprise Edition на портале технической поддержки.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 9).

2. О PT AI Enterprise Edition

PT AI Enterprise Edition — распределенная система, которая позволяет автоматизировать поиск уязвимостей и признаков недокументированных возможностей (далее — НДВ) в рамках жизненного цикла безопасной разработки и аудита информационной безопасности. В основе работы PT AI Enterprise Edition лежат методы, объединяющие достоинства статического, динамического и интерактивного подходов к анализу.

PT AI Enterprise Edition может быть встроен в процесс непрерывной интеграции (англ. continuous integration, CI) на агентах сборки TeamCity, Jenkins и других, что позволяет проверять код на наличие уязвимостей в процессе сборки разрабатываемого продукта.

В PT AI Enterprise Edition реализована ролевая модель доступа. Пользователи могут быть наделены полномочиями администратора, менеджера безопасности (глобального и проектного), аудитора. Каждый пользователь имеет соответствующий своей роли уровень доступа к данным и взаимодействует с продуктом с учетом специфики роли.

С помощью PT AI Enterprise Edition разработчики могут писать безопасный код, своевременно устраняя в нем уязвимости, а менеджеры безопасности могут контролировать процесс безопасной разработки.

Использование PT AI Enterprise Edition позволяет повысить качество и сократить сроки разработки и тестирования программного обеспечения, снизить трудоемкость поиска уязвимостей, характерную для ручного анализа.

Преимуществами PT AI Enterprise Edition являются:

- ролевая модель доступа;
- высокая эффективность поиска уязвимостей при низком уровне ложных срабатываний;
- отсутствие необходимости в развертывании приложения;
- наглядная демонстрация уязвимостей;
- сокращение времени проверки кода за счет инкрементального сканирования, учитывающего предыдущие результаты;
- исключение выбранных пользователем уязвимостей из результатов сканирования с помощью добавления комментариев в исходный код.

Ключевыми возможностями PT AI Enterprise Edition являются:

- Анализ кода на ранних стадиях разработки.
- Автоматическая генерация HTTP-запроса (эксплойта). Эксплойт позволяет проверить найденную уязвимость на развернутом приложении.
- Гибкая интеграция с межсетевым экраном прикладного уровня через формирование правил, препятствующих возможности эксплуатации обнаруженных уязвимостей (virtual patching).
- Сканирование запущенного веб-приложения методом черного ящика на тестовом стенде. Сканер анализирует динамические скрипты, формы, параметры, заголовки и прочие входные точки, через которые данные попадают внутрь системы и оказывают на нее негативное воздействие.
- Поддержка пользовательских шаблонов поиска и пользовательских правил, предназначенных для выявления конструкций со специфичной бизнес-логикой или с признаками НДВ.
- Определение оптимального места для исправления уязвимости в коде.
- Сбор статистических данных о результатах сканирования и найденных уязвимостях.
- Создание задач в Atlassian Jira на исправление уязвимостей, найденных при сканировании.

3. Аппаратные и программные требования

Минимальные аппаратные и программные требования для компьютера с модулем PT AI Enterprise Server:

- x86-совместимый 8-ядерный процессор с тактовой частотой 2,4 ГГц;
- 16 ГБ оперативной памяти;
- 200 ГБ на жестком диске;
- сетевой адаптер 10 Мбит/с;
- операционная система: Debian версий 10, 11, CentOS версии 8, Ubuntu версий18.04 LTS, 20.04 LTS, 21.04, 21.10;
- доступные порты 80, 443, 1947, 5672, 5432, 6432, 8200, 8501 для взаимодействия сервисов PT AI Enterprise Server по протоколам HTTP, HTTPS, WebSocket, TCP, AMQP.

Минимальные аппаратные и программные требования для компьютера с модулем PT AI Enterprise Agent:

- x86-совместимый 8-ядерный процессор с тактовой частотой 2,4 ГГц;
- 16 ГБ оперативной памяти;
- 50 ГБ на жестком диске;
- сетевой адаптер 10 Мбит/с;
- операционная система: 64-разрядная версия Windows 10.

Минимальные аппаратные и программные требования для компьютера с модулем AI.Shell:

- процессор Intel Core i5 с частотой 2 ГГц или аналоги;
- 512 МБ оперативной памяти;
- сетевой адаптер 10 Мбит/с;
- операционная система: 64-разрядная версия Windows 10, Debian версий 10, 11, CentOS версии 8, Ubuntu версий18.04 LTS, 20.04 LTS, 21.04, 21.10.

4. Схема развертывания PT AI Enterprise Edition

PT AI Enterprise Edition состоит из трех отдельно устанавливаемых модулей:

— PT AI Enterprise Server. Предоставляет другим модулям и веб-интерфейсу доступ к данным в PT AI Enterprise Edition, управляет этими данными. В состав инсталлятора PT AI Enterprise Server входит группа сервисов, управляющих работой системы, сервис для работы с сервером очереди сообщений RabbitMQ и база данных PostgreSQL.

— PT AI Enterprise Agent. Проверяет исходный код на наличие уязвимостей и передает результаты сканирования модулю PT AI Enterprise Server. Представляет собой консольное приложение.

— Легкий кроссплатформенный агент AI.Shell. Используется для интеграции с CI-системами и в Docker-контейнере. Подробнее см. в Руководстве по интеграции PT AI Enterprise Edition в сборочный процесс.

Процесс развертывания PT AI Enterprise Edition состоит из нескольких этапов:

1. Установка PT AI Enterprise Server на отдельном компьютере с соответствующими характеристиками (см. раздел 3).
2. Настройка системных параметров в веб-интерфейсе, в том числе создание токена доступа для подключения PT AI Enterprise Agent к PT AI Enterprise Server.
3. Установка PT AI Enterprise Agent и его подключение к PT AI Enterprise Server по токену доступа. Рекомендуется разворачивать PT AI Enterprise Agent на отдельном компьютере, чтобы ресурсоемкий анализ кода, выполняемый PT AI Enterprise Agent, не влиял на производительность PT AI Enterprise Server. PT AI Enterprise Server поддерживает работу нескольких модулей PT AI Enterprise Agent. Увеличение числа установленных модулей PT AI Enterprise Agent позволяет одновременно сканировать несколько проектов.
4. Установка AI.Shell, если предусмотрена интеграция с CI-системами.
5. Настройка конфигурационного файла и файла с правилом срабатывания политики безопасности для запуска сканирования с помощью AI.Shell.

5. Лицензирование

Для защиты всех модулей PT AI Enterprise Edition от нелегального использования нужна действующая лицензия.

Сканирование в PT AI Enterprise Edition осуществляется только при наличии лицензии. По завершении срока действия лицензии активное сканирование останавливается, создание новых проектов, настройка существующих проектов и перезапуск завершенных сканирований становятся недоступными. Вы можете полноценно работать с результатами сканирований, полученными ранее.

Лицензии PT AI Enterprise Edition различаются набором включенных языков программирования и количеством агентов сканирования. Если язык приложения не поддерживается вашей лицензией или превышено количество допустимых агентов сканирования, в интерфейсе отображается соответствующее сообщение.

Активация лицензии осуществляется администратором в веб-интерфейсе программы.

6. Установка продукта

В общем случае установка PT AI Enterprise Edition состоит из следующих этапов:

1. Установка модуля PT AI Enterprise Server.
2. Развертывание модуля PT AI Enterprise Agent:
   - предварительная установка и настройка программ, необходимых для работы модуля;
   - установка модуля;
   - настройка модуля.
3. Установка легкого агента AI.Shell.

В этом разделе

6.1. Установка модуля PT AI Enterprise Server

Установка PT AI Enterprise Server производится на ОС семейства Linux.

Внимание! Для работы PT AI Enterprise Server в операционной системе должен быть установлен компонент Docker CE версии 20 или выше.

► Чтобы установить PT AI Enterprise Server:

1. Запустите скрипт установки:
   ```
   sudo sh install.<Номер версии PT AI Enterprise Server>.sh
   ```
   При запуске скрипта сформируется файл журнала `/var/log/ptai/install/ptai-install-<Дата и время>.log`, который содержит информационные сообщения от системы, предупреждения и ошибки.

   Примечание. Сервисы, запущенные в Docker-контейнере, обращаются к узлу, на котором развернут PT AI Enterprise Server, по его имени (hostname). Если у вас не настроен DNS-сервер для разрешения имен узлов в IP-адреса, вы можете установить соответствие имени узла и IP-адреса с помощью ключа –a, `--advertise-addr` или переменной окружения `ADVERTISE_ADDR`.
2. Если требуется, запустите скрипт установки с указанием IP-адреса:
   ```
   sudo sh install.<Номер версии PT AI Enterprise Server>.sh -- -a <IP-адрес>
   ```
3. Введите `y` для принятия условий лицензионного соглашения.
4. Введите `y` для подтверждения установки PT AI Enterprise Server.

   Начнется установка PT AI Enterprise Server.

Примечание. По завершении установки вы можете проверить установленные Docker-контейнеры командой `docker ps -a`. Для мониторинга работы Docker-контейнеров рекомендуется использовать команду `docker stats` или утилиту ctop.

PT AI Enterprise Server установлен. Дистрибутив хранится в каталоге `/opt/ptai`.

Для управления работой PT AI Enterprise Server из консоли используется скрипт `ptaictl`. С помощью скрипта `ptaictl` вы можете:

- останавливать работу PT AI Enterprise Server командой `sudo /opt/ptai/latest/bin/ptaictl stop`;
- возобновлять работу PT AI Enterprise Server командой `sudo /opt/ptai/latest/bin/ptaictl start`;
- удалять PT AI Enterprise Server командой `sudo /opt/ptai/latest/bin/ptaictl uninstall`;
- выполнять замену серверного сертификата и ключа командой `sudo /opt/ptai/latest/bin/ptaictl cert`.

Для журналирования в файл результатов выполнения команд `stop`, `start` и `uninstall` используется ключ `-l` или `--log`. Например, `sudo /opt/ptai/latest/bin/ptaictl start -l /tmp/log.txt`.

Для команды `cert` используются ключи:

- `-c` или `--cert`

  Путь к файлу с сертификатом в формате PEM.

- `-k` или `--key`

  Путь к файлу с закрытым ключом в формате PEM, ключ не должен быть зашифрован.

- `--norestart`

  Не выполнять перезапуск Docker-контейнеров.

По умолчанию скрипт `ptaictl` запускается в тихом режиме, без вывода на экран информации от сервисных команд (кроме данных об ошибках). Для отображения подробной информации вы можете указать флаг `VERBOSE` с любым непустым значением. Например, `sudo VERBOSE=1 /opt/ptai/latest/bin/ptaictl stop`

6.2. Развертывание модуля PT AI Enterprise Agent

Этот раздел содержит инструкции по подготовке к развертыванию, установке и настройке модуля PT AI Enterprise Agent.

В этом разделе

6.2.1. Подготовка к развертыванию модуля PT AI Enterprise Agent

Для корректной работы модуля PT AI Enterprise Agent необходимо предварительно установить и настроить следующие программы:

— Для сборки проектов C#: Microsoft .NET 4.7.2 Development Pack. Загрузка и установка Microsoft .NET 4.7.2 Development Pack выполняются во время установки модуля PT AI Enterprise Agent, если он не был установлен ранее. В этом случае для корректной работы может потребоваться перезагрузка операционной системы после установки.

— Для загрузки зависимостей языка PHP: Composer.

Примечание. Для сканирования Xamarin-проектов необходимо установить Microsoft .NET Framework 3.5.1.

Примечание. Для сканирования проектов на языках C/C++ и ObjectiveC необходимо установить пакеты Windows Kits версии не ниже 10.0.17134.0 и Visual Studio MSVC SDK версии не ниже 14.28.29333.

Также в параметрах контроля учетных записей (UAC) ОС Windows рекомендуется отключить запрос разрешений на установку ПО.

6.2.2. Установка модуля PT AI Enterprise Agent

► Чтобы установить модуль PT AI Enterprise Agent на компьютер:

1. Запустите установочный файл.

   Откроется окно выбора языка установки.

2. Выберите язык установки и нажмите кнопку **ОК**.

   Откроется окно мастера установки.

3. В окне с текстом лицензионного соглашения ознакомьтесь с условиями лицензионного соглашения.

4. Выберите **Я принимаю условия соглашения**, если вы согласны со всеми пунктами лицензионного соглашения.

5. Нажмите кнопку **Далее**.

   Подготовка к установке программы будет продолжена.

6. Выберите папку для установки программы.

7. Нажмите кнопку **Далее**.

8. В открывшемся окне настройте подключение модуля PT AI Enterprise Agent к модулю PT AI Enterprise Server по токену доступа:

   - введите адрес компьютера с модулем PT AI Enterprise Server;
   - введите токен доступа.

9. Нажмите кнопку **Далее**.
10. Если после установки модуля PT AI Enterprise Agent не требуется автоматический запуск службы управления агентами сканирования (AI.CLi.Sheduler), в открывшемся окне снимите флажок **Work with scan scheduler**.

    Примечание. Если служба не запущена, то агент сканирования можно запускать только через консоль. Сканирование в веб-интерфейсе будет недоступно.
11. Нажмите кнопку **Далее**.
12. Убедитесь в правильном выборе параметров установки и нажмите кнопку **Установить**.

    Начнется установка модуля на ваш компьютер. Дождитесь завершения установки.
13. Нажмите кнопку **Завершить**.

    Установка модуля PT AI Enterprise Agent завершена.

6.2.3. Настройка модуля PT AI Enterprise Agent

В процессе установки модуля PT AI Enterprise Agent вы настраиваете его подключение к модулю PT AI Enterprise Server по токену доступа. Если после установки адрес PT AI Enterprise Server или токен изменились, вы можете настроить модуль PT AI Enterprise Agent, указав соответствующие изменения в конфигурационном файле `aic.user.config`.

- Чтобы настроить модуль PT AI Enterprise Agent:

  1. Откройте файл `aic.user.config` в папке с установленным модулем PT AI Enterprise Agent.
  2. Добавьте или измените строки в файле:

     ```
     <AI.ScanAgent.Properties.Settings>
     <setting name="SettingProviderUri" serializeAs="String">
     <value><Имя узла или IP-адрес PT AI Enterprise Server></value>
     </setting>
     <setting name="AccessToken" serializeAs="String">
     <value><Токен доступа></value>
     </setting>
     </AI.ScanAgent.Properties.Settings>
     ```
  3. Сохраните файл.
  4. Перезапустите службу AI.CLi.Sheduler.

  Модуль PT AI Enterprise Agent настроен.

6.3. Установка легкого агента AI.Shell

Модуль PT AI Enterprise Agent поддерживает работу только с ОС семейства Windows. Если в компании предусмотрена интеграция в CI-процесс на агентах сборки (далее также — CI-агентах) под управлением ОС семейства Linux или вы работаете с Docker-контейнерами,

вам необходимо установить на CI-агенты компонент AI.Shell. AI.Shell — это легкий кроссплатформенный агент, который отправляет задачу сканирования модулю PT AI Enterprise Server, а PT AI Enterprise Server ставит задачу в очередь на выполнение доступному PT AI Enterprise Agent.

В этом разделе

Установка AI.Shell из пакета (см. раздел 6.3.1)

Установка AI.Shell из инсталлятора для Microsoft Windows (см. раздел 6.3.2)

Конфигурирование AI.Shell и запуск сканирования (см. раздел 6.3.3)

6.3.1. Установка AI.Shell из пакета

В зависимости от ОС, AI.Shell имеет несколько вариантов поставки.

Таблица 2. Пакеты установки AI.Shell

ОС	Расширение пакета установки
Microsoft Windows (x64)	Стандартный инсталлятор для Microsoft Windows (содержит все файлы приложения, необходимые для работы) или готовый к использованию пакет для Windows Docker, не требующий установки
Alpine (x64) последней версии или LTS	.tar.gz
CentOS (x64) последней версии или LTS	.rpm
Ubuntu (x64) последней версии или LTS	.deb
Debian (x64) последней версии или LTS	.deb
Другие Linux-системы	.tar.gz

Установка AI.Shell из пакетов с расширениями .deb и .rpm

Примечание. Если в ОС не установлена библиотека libssl, которая необходима для безопасной передачи данных через интернет и является частью реализации протоколов шифрования SSL и TLS, ее нужно предварительно установить.

- Чтобы установить AI.Shell из пакетов с расширениями .deb и .rpm,

  выполните команду установки:

  `apt-get install <Имя пакета>` или `dpkg -i <Имя пакета>` — для .deb-пакетов;

  `rpm -i <Имя пакета>` — для .rpm-пакетов.

Установка AI.Shell из .tar.gz-архива

- Чтобы установить AI.Shell из .tar.gz-архива:

  1. Скачайте предоставленный архив и распакуйте его в каталог `/usr/share/aisa`.
  2. Выполните команду установки:
     ```
     sh /usr/share/aisa/scripts/install.sh
     ```
     Примечание. Вы можете удалить AI.Shell командой `sh /usr/share/aisa/scripts/remove.sh`.

6.3.2. Установка AI.Shell из инсталлятора для Microsoft Windows

- Чтобы установить AI.Shell на компьютер:

  1. Запустите установочный файл.

     Откроется окно выбора языка установки.
  2. Выберите язык установки и нажмите кнопку **ОК**.

     Откроется окно мастера установки.
  3. В окне с текстом лицензионного соглашения ознакомьтесь с условиями лицензионного соглашения.
  4. Выберите **Я принимаю условия соглашения**, если вы согласны со всеми пунктами лицензионного соглашения.
  5. Нажмите кнопку **Далее**.
  6. Выберите папку для установки программы.
  7. Нажмите кнопку **Далее**.
  8. В открывшемся окне настройте подключение AI.Shell к модулю PT AI Enterprise Server по токену доступа:
     - введите FQDN или IP-адрес PT AI Enterprise Server;
     - введите токен доступа.
  9. Нажмите кнопку **Далее**.
  10. Убедитесь в правильном выборе параметров установки и нажмите кнопку **Установить**.

      Начнется установка программы на ваш компьютер. Дождитесь завершения установки программы.
  11. Нажмите кнопку **Завершить**.

      Установка AI.Shell завершена.

6.3.3. Конфигурирование AI.Shell и запуск сканирования

Вы можете создавать проект и запускать сканирование с помощью AI.Shell из командной строки или на CI-агенте.

- Чтобы запустить задачу сканирования с помощью AI.Shell:

  1. Настройте подключение AI.Shell к модулю PT AI Enterprise Server командой:

     ```
     aisa --set-settings -u <Адрес PT AI Enterprise Server> -t <Токен доступа>
     ```

     Примечание. Если запуск сканирования производится на CI-агенте, вы можете не настраивать подключение к PT AI Enterprise Server отдельной командой, а указывать параметры подключения непосредственно при запуске сканирования: `aisa -u <Адрес PT AI Enterprise Server> -t <Токен доступа> --project-name "<Имя проекта сканирования>" --scan-target "<Путь к объекту сканирования>`.

  2. Если вы хотите запустить сканирование проекта и одновременно настроить его параметры, выполните команду:

     ```
     aisa --project-settings-file "<Путь к конфигурационному файлу>" --scan-target "<Путь к объекту сканирования>"
     ```

  3. Если вы хотите запустить сканирование ранее созданного проекта с текущими параметрами, выполните команду:

     ```
     aisa --project-name "<Имя проекта сканирования>" --scan-target "<Путь к объекту сканирования>"
     ```

     Примечание. Для запуска сканирования с помощью AI.Shell используются те же параметры, что и для PT AI Enterprise Agent, а также специфичные параметры. Список всех параметров запуска сканирования приведен в приложении (см. приложение А).

Таблица 3. Параметры запуска сканирования для AI.Shell

Параметр	Описание	Примечание
`-u`	Адрес сервера PT AI Enterprise Server	Параметры учитываются только в паре. Если параметры заданы, то сначала происходит валидация этих параметров, а затем сканирование
`-t`	Токен доступа	
`--no-wait`	Отключение подписки на события задачи сканирования	Если параметр задан, то после отправки сканирования в очередь работа AI.Shell завершится, если не задан — AI.Shell примет от PT AI Enterprise Server все статусы задачи сканирования и прогресс сканирования до момента завершения задачи. Только после этого работа AI.Shell завершится. **Примечание.** Если задан параметр `--no-wait`, выпуск отчетов невозможен, даже если заданы параметры создания отчетов `--reports-folder` и `--reports`

Параметр	Описание	Примечание
`--create-project`	Создание проекта, если он не был создан ранее	Используется с параметрами `--project-name` и `--scan-target`
`--status`	Подписка на получение информации о сканировании, запущенном с параметром `--no-wait`	Используется с параметрами `--project-id` и `--scan-result-id`. При добавлении параметра `--no-wait` приходит однократное сообщение о статусе сканирования
`--log-level`	Уровень журналирования	Возможные аргументы (расположены в порядке уменьшения количества выводимой информации): — trace; — debug; — info; — warning; — error; — critical; — none
`--policy-settings-file`	Обновление политик безопасности без запуска сканирования	При использовании с параметрами `--project-name` и `--scan-off` сканирование не запускается, обновляются только политики безопасности

7. Обновление PT AI Enterprise Edition

Вы можете выполнять обновление PT AI Enterprise Edition до версии 4.1.0 с версий 3.6.6 и 4.0.0.

Архитектура PT AI Enterprise Edition версии 3.6.6 существенно отличается от архитектуры PT AI Enterprise Edition версии 4.1.0, поэтому автоматическое обновление продукта в этом случае невозможно. Перенос данных выполняется вручную в два этапа: экспорта и импорта. Для обновления с версии 4.0.0 достаточно удалить предыдущую версию и установить новую.

В этом разделе

7.1. Обновление PT AI Enterprise Edition с версии 4.0.0 до версии 4.1.0

- Чтобы обновить PT AI Enterprise Edition с версии 4.0.0 до версии 4.1.0:

  1. Удалите PT AI Enterprise Edition версии 4.0.0:
     ```
     sudo /opt/ptai/latest/bin/ptaictl uninstall
     ```
  2. Установите PT AI Enterprise Edition версии 4.1.0:
     ```
     sudo sh <Номер версии PT AI Enterprise Server>.sh
     ```

  PT AI Enterprise Edition обновлен.

Все проекты, результаты сканирований и ранее настроенные параметры сохраняются в текущей версии.

7.2. Обновление PT AI Enterprise Edition с версии 3.6.6 до версии 4.1.0

> **Примечание.** Перед началом обновления PT AI Enterprise Edition убедитесь в наличии достаточного объема свободного дискового пространства (см. раздел 3).

Обновление выполняется в два этапа. На этапе экспорта с помощью CLI-утилиты migrator.exe создается файл с резервной копией данных. В файл в незашифрованном виде помещаются следующие данные:

- дамп базы данных PT AI Enterprise Edition в PostgreSQL;
- конфигурация PT AI Enterprise Edition;
- секретные данные проектов (например, пароли для доступа к репозиторию с исходным кодом проекта);

— параметры журналирования событий на syslog-сервере или сервере Elasticsearch (после обновления необходимо включить журналирование заново на странице **Администрирование**);

— исходный код проектов (опционально).

На этапе импорта выполняется установка PT AI Enterprise Edition версии 4.1.0 с указанием файла резервной копии данных, созданного на этапе экспорта.

Важно отметить, что при экспорте данных не осуществляется перенос почтовых профилей и параметров прокси-сервера, настроенных в предыдущей версии. Экспорт и импорт возможны только для PT AI Enterprise Edition версии 3.6.6. Если вы используете более раннюю версию, необходимо сначала обновить ее до версии 3.6.6.

Экспорт данных

Экспорт данных выполняется с помощью утилиты migrator.exe. Перед началом экспорта утилита останавливает все сервисы PT AI Enterprise Edition, используя стандартные механизмы Windows. Возможна ситуация, когда ОС вернет ошибку. В таком случае необходимо перезагрузить ОС, а затем повторить процедуру экспорта.

► Чтобы выполнить экспорт данных из PT AI Enterprise Edition версии 3.6.6:

1. Остановите все активные задачи сканирования и агенты сканирования.
2. Запустите утилиту migrator.exe с командой `export` и укажите локальную папку, в которую будет сохранен файл с резервной копией данных (ключ `-o`).

   Примечание. Если у вас установлен английский язык интерфейса, то при указании русских символов в пути экспорта может возникать ошибка. Для ее устранения выберите русский язык в качестве языка интерфейса.
3. Если требуется, дополните экспортируемые данные исходным кодом проектов (флаг `-e`).

   Например:

   ```
   migrator.exe export -e -o C:\<Папка с резервной копией>
   ```

   Примечание. Утилита автоматически определяет размещение файла конфигурации PT AI Enterprise Edition. В файле указаны параметры для доступа к нужным службам. При необходимости вы можете указать его расположение с помощью ключа `-c`. Например: `migrator.exe export -e -o C:\<Папка с резервной копией> -c C:\<Путь к конфигурационному файлу>`.

   Примечание. Для отображения информации о доступных флагах и ключах вы можете использовать команду `--help`.

Данные экспортированы, файл с резервной копией располагается по указанному пути.

Импорт данных

Импорт данных из PT AI Enterprise Edition версии 3.6.6 осуществляется в процессе установки версии 4.1.0. Если версия 4.1.0 была установлена ранее, то мастер установки отобразит ошибку и предложит прервать установку или продолжить без переноса данных.

- Чтобы выполнить импорт данных в PT AI Enterprise Edition версии 4.1.0:

  Запустите скрипт установки PT AI Enterprise Server с ключом `–b`, `--backup` или переменной окружения `BACKUP_FILE`.

  Например:

  ```
  sudo sh install.<Номер версии PT AI Enterprise Server>.sh -- -b /<Абсолютный путь к файлу с резервной копией данных>
  ```

  Примечание. Установка выполняется в несколько этапов, ключ `–b` передается распаковщику, отрабатывающему на первом этапе. Чтобы передать ключ дальше, необходимо использовать разделитель `--`. В противном случае может отображаться ошибка "Unrecognized flag".

  Данные импортированы.

Поскольку в PT AI Enterprise Edition версии 4.1.0 не поддерживается аутентификация с использованием доменных учетных записей Active Directory, при переносе данных с версии 3.6.6 на версию 4.1.0 создается LDAP-провайдер с параметрами подключения пользователей. После установки PT AI Enterprise Edition необходимо убедиться в корректности параметров LDAP-провайдера и обеспечить доступ к LDAP-серверу.

8. Настройка сканирования

После установки модулей PT AI Enterprise Edition вы можете настроить параметры сканирования проекта и политику безопасности. Политика безопасности — это набор условий, необходимых для достижения требуемого уровня безопасности программного продукта. Если в проекте настроена проверка политики безопасности, то в процессе сборки проекта CI-агент проверяет соответствие результатов сканирования условиям срабатывания политики безопасности и прекращает сборку при нарушении политики.

Вы можете настроить параметры сканирования проекта и политику безопасности следующими способами:

- Во время настройки CI-агента. Параметры сканирования вы указываете на шаге создания конфигурационного файла. Правило срабатывания политики безопасности вы указываете на шаге создания политик безопасности.
- До настройки CI-агента. Вы заранее создаете текстовые файлы с параметрами сканирования и правилом срабатывания политики безопасности. При настройке CI-агента вы указываете путь к созданным файлам. В этом случае настраивать параметры сканирования и политику безопасности в CI-агенте не требуется.
- В интерфейсе PT AI Enterprise Edition. Настройка проекта сканирования и политики безопасности в интерфейсе PT AI Enterprise Edition рассмотрена в Руководстве пользователя.

В этом разделе содержатся инструкции по созданию конфигурационного файла с параметрами сканирования и файла с правилом срабатывания политики безопасности.

В этом разделе

8.1. Настройка параметров сканирования в конфигурационном файле

► Чтобы настроить параметры сканирования в конфигурационном файле:

1. Создайте конфигурационный файл в формате JSON в текстовом редакторе.
2. Пропишите в конфигурационном файле параметры сканирования.

   Примечание. Пример конфигурационного файла приведен в приложении (см. приложение B).
3. Сохраните конфигурационный файл.

8.2. Настройка политики безопасности

Вы можете настраивать политику безопасности в конфигурационном файле или в интерфейсе PT AI Enterprise Edition. Подробную информацию о настройке политики безопасности в интерфейсе см. в Руководстве пользователя.

- Чтобы создать правило срабатывания политики безопасности:

  1. Создайте файл в формате JSON в текстовом редакторе.
  2. Напишите правило в файле в соответствии с форматом записи, представленным в таблице ниже.
  3. Сохраните файл.

Таблица 4. Формат записи правила срабатывания политики безопасности

Название раздела	Название строки	Описание строки
Policy	ID	Произвольное строковое обозначение (необязательное, уникальное)
	CountToActualize	Минимально необходимое количество срабатываний политики на найденных уязвимостях (если 0 или не задано, то достаточно одного срабатывания)
	Scopes	Наборы правил (политика сработает, если хотя бы один набор актуален)
Scope	Rules	Список правил внутри одного набора (если все правила совпадают, набор актуален)
Rule	Field	Имя атрибута уязвимости
	Value	Значение поля, требуемое для срабатывания правила (регистронезависимо, если не задан IsRegex)
	IsRegex	Флаг сравнения по регулярному выражению

В таблице ниже представлены описания основных значений строки Field. Вы можете получить полный список значений из JSON-отчета, который создается по окончании сканирования. Параметры отчета `--reports` и `--reports-folder` задаются при настройке CI-агента.

Таблица 5. Основные значения строки Field

Значение	Тип данных	Описание
ApprovalState	Число	Статус подтверждения уязвимости. Может принимать значения: 0 — без статуса, 1 — подтвержде-

Значение	Тип данных	Описание
		на, 2 — опровергнута, 3 — не существует, 4 — подтверждена автоматически
EntryPointFile	Строка	Путь до файла с точкой входа
EntryPointValue	Строка	Значение функции или метода — точки входа в карточке уязвимости
IsSecondOrder	Логическое значение	Наличие флага IsSecondOrder для уязвимости: false или true
IsSuspected	Логическое значение	Подозрение на уязвимость: false или true
IsSuppressed	Логическое значение	Скрытые уязвимости: false или true. По умолчанию скрытые уязвимости учитываются в политике безопасности
VulnerabilityLevel	Строка	Уровень опасности уязвимости: high, medium, low, potential
SearchAlgorithm	Число	Алгоритм поиска уязвимостей. Может принимать значения: 0 — от точек входа (FromEntryPoint); 1 — от доступных public и protected методов (FromPublicProtected); 2 — Taint; 999 — неизвестен
VulnerabilityTitle	Строка	Название типа уязвимости
VulnerableFile	Строка	Путь к файлу с точкой выхода
VulnerableValue	Строка	Значение функции или метода — точки выхода в карточке уязвимости
Exploit	Строка	Запрос для проверки уязвимости
VulnerableFunction	Строка	Уязвимая функция
Payload	Строка	Параметры вектора атаки
IsNew	Логическое значение	Флаг для новой найденной уязвимости: false или true

Ниже приведен пример правила для поиска уязвимостей высокого уровня опасности, исключая "Опровергнутые" и "Подозрения на уязвимость".

```
[
  {
    "CountToActualize": 1,
    "Scopes": [
```

```
      {
        "Rules": [
          {
            "Field": "VulnerabilityLevel", // field name
            "Value": "High", // field value, case insensitive
            "IsRegex": false // whether to use regular expressions
          },
          {
            "Field": "IsSuspected",
            "Value": "false",
            "IsRegex": false
          },
          {
            "Field": "ApprovalState",
            "Value": "[^2]",
            "IsRegex": true
          }
        ]
      }
    ]
  }
]
```

9. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

9.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

9.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

9.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

Предоставление информации для технической поддержки (см. раздел 9.3.1)

Типы запросов (см. раздел 9.3.2)

Время реакции и приоритизация запросов (см. раздел 9.3.3)

Выполнение работ по запросу (см. раздел 9.3.4)

9.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

9.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

9.3.3. Время реакции и приоритизация запросов

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

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

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 6).

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

Таблица 6. Время реакции на запрос и время его обработки

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

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

9.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

- о диагностике проблемы и ее результатах;
- о поиске решения или возможности обойти причины возникновения проблемы;
- о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

- предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;
- проблема классифицирована как неподдерживаемая.

Приложение А. Параметры запуска сканирования из консоли

Вы можете запускать сканирование в PT AI Enterprise Edition из консоли. Ниже приведен список параметров запуска.

Таблица 7. Список параметров запуска

Параметр	Используется в легком агенте AI.Shell	Описание
`--project-name`	Да	Регистронезависимое имя проекта сканирования
`--full-scan`	Да	Принудительный запуск полного сканирования
`--policies-path`	Да	Путь к файлу с описанием политик
`--project-settings-file`	Да	Путь к конфигурационному файлу
`--reports-folder`	Да	Путь к папке для сохранения отчетов
`--reports`	Да	Формат сохранения отчета: HTML, JSON, PDF, XML, WAF. Вы можете указывать несколько форматов через запятую. Для выпуска пользовательского отчета вы можете указать значение `custom`
`--report-type`	Да	Тип отчета, создаваемого по окончании сканирования. Может принимать одно из следующих значений: PlainReport, AutoCheck, Nist, Oud4, Owasp, Owaspm, Pcidss, Sans. Если вы создаете пользовательский отчет (для параметра `--reports` указано значение `custom`), то нужно указать имя этого отчета
`--sync`	Нет	Синхронный запуск нескольких экземпляров исполняемого файла aic.exe. При синхронном запуске aic.exe PT AI Enterprise Agent выполняет сканирования по очереди
`--scan-target`	Да	Путь к папке или файлу приложения для сканирования. Если путь не задан, PT AI Enterprise Agent сканирует текущую папку
`--restore-sources`	Нет	Параметр, позволяющий скачивать приложение для сканирования с PT AI Enterprise Server в папку с путем `--scan-target`. При этом все содержимое папки удаляется и заменяется данными с PT AI Enterprise Server

Параметр	Используется в легком агенте AI.Shell	Описание
`--settings-export-file`	Нет	Выгрузка параметров проекта в файл по указанному пути в формате JSON
`--help`	Да	Отображение всех доступных параметров запуска
`--scan-off`	Да	Создание проекта по конфигурационному файлу без запуска задачи сканирования. Используется вместе с параметром `--project-settings-file`

Приложение Б. Коды возврата

По завершении сканирования отображается код возврата. Ниже приведен список возможных кодов возврата.

Таблица 8. Список кодов возврата

Код	Описание
0	Успешное сканирование
-1	Программа уже запущена
-2	Ошибка запуска дочернего процесса
2	Не найдена папка для сканирования
3	Проблема с лицензией
4	Не найден проект для сканирования
5	Ошибки в параметрах проекта
6	Некритические ошибки в файлах журнала
7	Ошибка отправки отчета на электронную почту
8	Некорректный путь к конфигурационному файлу
9	Некорректный путь к папке отчетов
10	Сработала политика безопасности (сборка не удовлетворяет заданной политике безопасности)
11	Некорректная настройка параметров отчетов
13	Сканирование было удалено
14	Ошибка аутентификации при настройке автоматической проверки уязвимостей
15	Некорректные параметры прокси-сервера (если использовалась автоматическая проверка уязвимостей)
16	Некорректный адрес сайта для сканирования (если использовалась автоматическая проверка уязвимостей)
17	Ошибка в политике безопасности
18	Критическая ошибка модуля PT AI Enterprise Agent
19	Не найден модуль PT AI Enterprise Agent
20	Ошибка загрузки исходных файлов с PT AI Enterprise Server
21	Тайм-аут оповещения PT AI Enterprise Server о нормальной работе PT AI Enterprise Agent
22	Ошибка в процессе обновления
24	Не найден серверный сертификат

Код	Описание
25	Недействительный URI PT AI Enterprise Server. Ошибка отображается только при сканировании с помощью AI.Shell
26	Запущена служба AI.Cli.Sheduler. Запуск агента сканирования через консоль невозможен
27	Версия AI.Shell устарела, доступна новая версия для обновления
28	Отсутствуют активные агенты сканирования
29	Отсутствует токен доступа для AI.Shell
30	Неверный путь к файлу с описанием политики безопасности
31	Сканирование проекта уже запущено
32	Ошибка подключения к PT AI Enterprise Server (например, AI.Shell новой версии установлен на PT AI Enterprise Server старой версии)
33	Ошибка обновления исходных файлов проекта
60	Совмещенные коды 6 и 10. Сработала политика безопасности, и в ходе сканирования найдены некритические ошибки
100	Сканирование отменено
1000	Неопознанная ошибка

Приложение B. Пример конфигурационного файла

Ниже приведен пример конфигурационного файла, в котором задаются параметры сканирования. Вы можете настроить конфигурацию при настройке CI-агента или в отдельном текстовом файле.

```
{
  // Настройка основных параметров
  "ProjectName": "Test_Proj", // Имя проекта
  "ProgrammingLanguage": "Php", // Язык приложения: Java, Php, Csharp, VB,
ObjectiveC, CPlusPlus, TSql, PlSql, Swift, Python, JavaScript, Kotlin, Go
  "ScanAppType": "Configuration, Fingerprint, PHP, PmTaint, BlackBox", // Модули
поиска уязвимостей: Php, Java, CSharp, JavaScript, Configuration, DependencyCheck,
PmTaint, BlackBox
  "IsUsePublicAnalysisMethod": false, // Искать от доступных public и protected
методов
  "IsDownloadDependencies": true, // Загрузить зависимости
  "CustomParameters": null, // Параметры запуска

  // Параметры языка Java
  "JavaParameters": null, // Параметры запуска Java Virtual Machine
  "IsUnpackUserPackages": false, // Распаковка пользовательских JAR-файлов
  "JavaVersion": 0, // Версия JDK, 0 соответствует версии 1.8, 1 соответствует
версии 1.11
  "PreprocessingTimeout": 60, // Тайм-аут препроцессинга в минутах
  "UserPackagePrefixes": null, // Префиксы пользовательских пакетов

  // Параметры языков C# и VB.NET
  "ProjectType": 0, // Тип проекта: Solution, WebSite
  "SolutionFile": null, // Путь к файлу решения или проекта

  // Параметры PMTaint
  "UseTaintAnalysis": true, // Включить анализ потока данных
  "UsePmAnalysis": true, // Включить поиск по шаблонам

  // Проверять соответствие политике безопасности
  "UseSecurityPolicies": false,

  // Параметры пользовательских правил анализа
  "UseCustomYaraRules": false, // Включить правила анализа YARA
  "UseSastRules": false, // Включить правила анализа SAST

  // Параметры черного ящика
  "Site": "http://localhost", // Адрес сайта
  "Level": 2, // Режим поиска: Fast, Normal, Full
```

```
  "ScanScope": 0, // Область сканирования: Folder, Domain, Path
  "CustomHeaders": [["", ""]], // Дополнительные HTTP-заголовки
  "Authentication": {
    "auth_item": {
      "domain": null, // Адрес проверки
      "credentials": {
        "cookie": null, // Значение cookie
        "type": 2, // Тип аутентификации: 0 = Form, 1 = HTTP, 2 = None, 3 = Cookie
        "login": {
          "name": null, // Ключ логина
          "value": null, // Значения логина
          "regexp": null,
          "is_regexp": false
        },
        "password": {
          "name": null, // Ключ пароля
          "value": null, // Значения пароля
          "regexp": null, // Например: "p[aA]ss(word)?"
          "is_regexp": false
        }
      },
      "test_url": null, // Адрес проверки
      "form_url": null, // Адрес формы
      "form_xpath": ".//form", // XPath формы
      "regexp_of_success": null // Искомая строка
    }
  },
  "ProxySettings": {
    "IsEnabled": false, // Активировать параметры прокси-сервера
    "Host": null, // Адрес
    "Port": null, // Порт
    "Type": 0, // Тип прокси: 0 или HTTP, 1 или HTTPNOCONNECT, 2 или SOCKS4, 3 или
SOCKS5
    "Username": null, // Логин
    "Password": null // Пароль
  },


  // Настройка автоматической проверки уязвимостей
  "RunAutocheckAfterScan": true, // Запускать автоматическую проверку уязвимостей
после сканирования
  "AutocheckCustomHeaders": [ [ "", "" ] ], // Дополнительные HTTP-заголовки
  "AutocheckAuthentication": {
    "auth_item": {
```

```
      "domain": null, // Адрес проверки
      "credentials": {
        "cookie": null,
        "type": 2, Тип аутентификации: 0 = Form, 1 = HTTP, 2 = None, 3 = Cookie
        "login": {
          "name": null, // Ключ логина
          "value": null, // Значение логина
          "regexp": null,
          "is_regexp": false
        },
        "password": {
          "name": null, // Ключ пароля
          "value": null, // Значение пароля
          "regexp": null, // Например: "p[aA]ss(word)?"
          "is_regexp": false
        }
      },
      "test_url": null, // Адрес проверки
      "form_url": null, // Адрес формы
      "form_xpath": ".//form", // XPath формы
      "regexp_of_success": null // Искомая строка
    }
  },
  "AutocheckProxySettings": {
    "IsEnabled": false, // Активировать параметры прокси-сервера
    "Host": null, // Адрес
    "Port": null, // Порт
    "Type": 0, // Тип прокси: 0 или HTTP, 1 или HTTPNOCONNECT, 2 или SOCKS4, 3 или
SOCKS5
    "Username": null, // Логин
    "Password": null // Пароль
  }
}
```

POSITIVE TECHNOLOGIES

О нас

Positive Technologies — ведущий разработчик решений для кибербезопасности. Наши технологии и сервисы используют более 2300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Уже 20 лет наша основная задача — предотвращать хакерские атаки 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).