Positive Technologies Application Inspector Enterprise Edition

Версия 3.6.0

Руководство администратора

POSITIVE TECHNOLOGIES

Дата редакции документа: 30.09.2020

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.

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 текста с условным обозначением	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 текста с условным обозначением	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 сайте ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", 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 программе 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 (администратор, аудитор, менеджер безопасности). 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.

В этом разделе

Роли пользователей (см. раздел 2.1)

Общий сценарий работы PT AI Enterprise Edition (см. раздел 2.2)

2.1. Роли пользователей

В PT AI Enterprise Edition для каждого пользователя предусмотрена своя роль (администратор, менеджер безопасности и аудитор). В соответствии с назначенной ролью пользователь получает набор полномочий.

Полномочия могут быть глобальными и проектными. Проект сканирования (далее также — проект) — это именованная задача, содержащая результаты анализа кода конкретного приложения в отдельном каталоге и во всех вложенных в него каталогах. Пользователи с глобальными полномочиями могут выполнять действия в рамках своей роли во всех проектах. Пользователи с проектными полномочиями — только в тех проектах, где они участвуют.

Администратор в PT AI Enterprise Edition обладает глобальными полномочиями, менеджер безопасности — глобальными и проектными, аудитор — только проектными.

Администратор назначается системным администратором. Для системного администратора не предусмотрена роль, и он не является участником проектов. Системный администратор занимается только сервисным обслуживанием PT AI Enterprise Edition (устанавливает модули и поддерживает их работу, встраивает PT AI Enterprise Edition в CI-процесс).

Администратор

Системный администратор назначает администратора для всех проектов в PT AI Enterprise Edition.

Администратор может:

- выписывать токены для агентов сканирования, легкого агента AI.Shell и плагинов CI/CD;
- настраивать систему в веб-интерфейсе;
- настраивать агенты сканирования;
- управлять правами доступа всех пользователей в системе;
- создавать и настраивать проекты сканирования;
- работать с результатами сканирования.

Менеджер безопасности

Администратор назначает глобального менеджера безопасности.

Глобальный менеджер безопасности может создавать новые проекты. В созданном проекте глобальный менеджер безопасности автоматически получает права проектного менеджера безопасности. Проектный менеджер, в свою очередь, может назначать в своем проекте других проектных менеджеров и аудиторов.

В зоне ответственности менеджера безопасности находится контроль соответствия разрабатываемого программного продукта стандартам политики безопасности, принятым на уровне проекта.

Менеджер безопасности настраивает проекты и запускает сканирования в интерфейсе PT AI Enterprise Viewer, работает с результатами сканирования, формирует отчеты о найденных уязвимостях.

Аудитор

Администраторы и менеджеры безопасности могут назначать аудиторов для каждого проекта.

Аудитор в пользовательском интерфейсе просматривает результаты сканирования проектов, формирует отчеты о найденных уязвимостях, изменяет статус уязвимостей (подтверждает или опровергает).

Также на роль аудитора может быть назначен разработчик программного продукта, который по коммиту запускает проверку проекта на агенте сборки.

2.2. Общий сценарий работы PT AI Enterprise Edition

В общем случае работа с PT AI Enterprise Edition состоит из следующих шагов:

1. Установка модулей системы. Системный администратор разворачивает модули PT AI Enterprise Edition и дополнительные компоненты, необходимые для работы модуля PT AI Enterprise Agent. В процессе установки модуля PT AI Enterprise Server системный администратор назначает роль администратора.
2. Настройка системных параметров. Администратор настраивает PT AI Enterprise Edition в веб-интерфейсе.
3. Конфигурация ролей. Администратор в веб-интерфейсе назначает других администраторов и глобальных менеджеров.
4. Создание проекта. Администратор или глобальный менеджер создают проект в интерфейсе PT AI Enterprise Viewer.
5. Внедрение PT AI Enterprise Edition в CI-процесс. Системный администратор настраивает механизм запуска проверки кода на наличие уязвимостей на агенте сборки.
6. Настройка проекта сканирования. Возможны два варианта настройки проекта:
   - В конфигурационном файле. Администратор или менеджер безопасности указывают параметры сканирования в конфигурационном файле.
   - В PT AI Enterprise Viewer. Администратор или менеджер безопасности настраивают параметры сканирования.
7. Запуск проверки проекта на наличие уязвимостей в PT AI Enterprise Viewer или на агенте сборки.
8. Если проверка проекта на наличие уязвимостей осуществляется на агенте сборки:
   - PT AI Enterprise Agent получает задачу на проверку кода от агента сборки (например, по коммиту разработчика).
   - PT AI Enterprise Agent проверяет код на наличие уязвимостей и возвращает результаты агенту сборки.
   - Результаты проверки отображаются в файле журнала в интерфейсе агента сборки.
   - В зависимости от настроек реагирования агента сборки на события, получаемые из файла журнала, сборка проекта останавливается, если политика безопасности в проекте нарушена, или сборка проекта продолжается, если политика безопасности в проекте соблюдена.

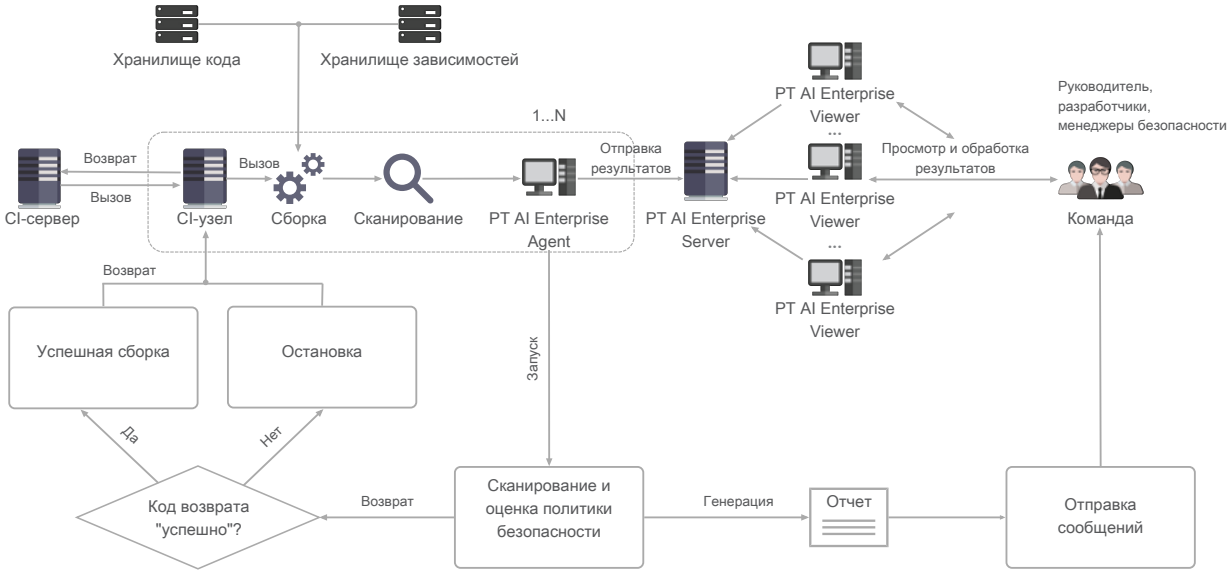

Рисунок 1. Использование PT AI Enterprise Edition в непрерывной интеграции

9. Работа с обнаруженными уязвимостями в PT AI Enterprise Viewer. Используя набор инструментов, представленный в интерфейсе, менеджер безопасности или аудитор проверяют и анализируют найденные уязвимости.
10. Исправление уязвимостей. Разработчик программного продукта исправляет уязвимости в своей среде разработки и отправляет код на повторное сканирование (делает коммит). Сканирование продолжается до тех пор, пока не будет соблюдена политика безопасности в проекте.
11. Подготовка отчета по результатам сканирования. Менеджер безопасности или аудитор формируют отчет о количестве и типах найденных уязвимостей и оценивают качество реализации политики безопасности в проекте.

3. Аппаратные и программные требования

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

- процессор Intel Core i7 с частотой 3,2 ГГц или аналоги;
- 8 ГБ оперативной памяти;
- 200 ГБ на жестком диске;
- сетевой адаптер 10 Мбит/с;
- монитор с разрешением 1366×768 пикселей;
- 64-разрядная версия Windows Server 2012 R2 и выше;
- средство автоматизации Windows PowerShell версии 5.0 и выше;
- браузер: Microsoft Edge, Mozilla Firefox 46 и выше, Google Chrome 50 и выше.

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

- процессор Intel Core i5 с частотой 2 ГГц или аналоги;
- 8 ГБ оперативной памяти;
- сетевой адаптер 10 Мбит/с;
- монитор с разрешением 1366×768 пикселей;
- браузер: Microsoft Edge, Mozilla Firefox 46 и выше, Google Chrome 50 и выше.

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

- процессор Intel Core i7 с частотой 3,2 ГГц или аналоги;
- 8 ГБ оперативной памяти;
- сетевой адаптер 10 Мбит/с;
- монитор с разрешением 1366×768 пикселей;
- браузер: Microsoft Edge, Mozilla Firefox 46 и выше, Google Chrome 50 и выше.

4. Лицензирование

Для защиты всех модулей PT AI Enterprise Edition от нелегального использования применяется сетевая программная лицензия Sentinel.

Сканирование в PT AI Enterprise Edition осуществляется только при наличии действующей лицензии. Срок действия лицензии для PT AI Enterprise Edition — 1 год. При завершении срока действия лицензии активное сканирование останавливается с кодом возврата 3. Вы можете полноценно работать с результатами сканирований, полученными ранее.

Лицензии PT AI Enterprise Edition различаются:

— количеством сканируемых проектов (10, 25, 50, 100 и без ограничения на количество проектов);

— набором включенных языков программирования для сканирования проектов.

Активация лицензии осуществляется администратором в веб-интерфейсе PT AI Enterprise Edition.

5. Схема развертывания PT AI Enterprise Edition

PT AI Enterprise Edition состоит из трех отдельно устанавливаемых модулей:

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

— PT AI Enterprise Agent — модуль для сканирования исходного кода. Представляет собой консольное приложение. PT AI Enterprise Agent проверяет исходный код на наличие уязвимостей и передает результаты сканирования модулю PT AI Enterprise Server.

— PT AI Enterprise Viewer — модуль, предоставляющий интерфейс для взаимодействия пользователя с PT AI Enterprise Edition. PT AI Enterprise Viewer позволяет настраивать и запускать сканирование, отображает результаты сканирования.

Модуль PT AI Enterprise Server обязательно должен быть установлен на отдельном компьютере с соответствующими аппаратными характеристиками (см. раздел 3). Модули PT AI Enterprise Viewer и PT AI Enterprise Agent рекомендуется также устанавливать на отдельных компьютерах. Модуль PT AI Enterprise Agent выполняет ресурсоемкий анализ кода. Из-за этого при установке модулей на одном компьютере может снизиться скорость работы с пользовательским интерфейсом.

Модуль PT AI Enterprise Server может поддерживать работу нескольких модулей PT AI Enterprise Viewer и PT AI Enterprise Agent. Увеличение числа установленных модулей PT AI Enterprise Agent позволяет одновременно сканировать несколько проектов и осуществлять их сборку на CI-агентах.

Если в компании предусмотрен процесс непрерывной интеграции, модуль PT AI Enterprise Agent должен быть установлен на том же компьютере, что и агент сборки. Также, если агенты сборки находятся под управлением ОС семейства Linux или предусмотрена работа с Docker-контейнерами, необходимо установить на них компонент AI.Shell (поставляется вместе с PT AI Enterprise Edition).

Развертывание PT AI Enterprise Edition выполняется с помощью мастера установки. Файл мастера установки необходимо разместить на каждом компьютере, где устанавливаются модули системы.

Для обеспечения безопасной передачи данных между модулями PT AI Enterprise Agent и PT AI Enterprise Server используется токен доступа, который необходимо сгенерировать в веб-интерфейсе.

> **Примечание.** В PT AI Enterprise Edition сохраняется возможность работы с SSL-сертификатами, используемыми в предыдущих версиях продукта.

После развертывания PT AI Enterprise Edition пользователи подключают модули PT AI Enterprise Viewer и PT AI Enterprise Agent к модулю PT AI Enterprise Server:

— При запуске PT AI Enterprise Viewer вводят адрес компьютера с установленным модулем PT AI Enterprise Server. Аутентификация пользователя в системе происходит через Active Directory. После ввода адреса отображается окно, в котором пользователь видит только те проекты, доступ к которым предоставил ему администратор или менеджер безопасности.

— Перед запуском PT AI Enterprise Agent в конфигурационном файле `aic.user.config` указывают токен доступа и адрес компьютера с установленным модулем PT AI Enterprise Server.

6. Установка продукта

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

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

В этом разделе

6.1. Установка модуля PT AI Enterprise Server

► Чтобы установить модуль PT AI Enterprise Server на компьютер:

1. Запустите установочный файл.
2. В окне с текстом Лицензионного соглашения ознакомьтесь с условиями Лицензионного соглашения.
3. Выберите **I accept the agreement**, если вы согласны со всеми пунктами Лицензионного соглашения.
4. Нажмите кнопку **Next**.
5. В окне **Select Destination Location** укажите папку для установки модуля.
6. Нажмите кнопку **Next**.

   Откроется окно общей конфигурации модуля PT AI Enterprise Server.
7. В окне укажите следующие параметры:
   - В поле **Domain** введите имя домена.
   - В поле **Message queue port** введите порт сервера очереди сообщений RabbitMQ.
   - В поле **Message queue user** введите имя пользователя сервера очереди сообщений RabbitMQ.

- В поле **Message queue password** введите пароль для подключения к серверу очереди сообщений RabbitMQ.
- В поле **Database port** введите порт сервера базы данных PostrgreSQL.
- В поле **Database name** введите имя базы данных PostrgreSQL.
- В поле **Database user** введите имя пользователя базы данных PostrgreSQL.
- В поле **Database password** введите пароль для подключения к базе данных PostrgreSQL.

8. Нажмите кнопку **Next**.

   Откроется окно конфигурации сервисов. PT AI Enterprise Edition назначает все порты для подключения к сервисам по умолчанию. Если назначенный по умолчанию порт занят, PT AI Enterprise Edition предупредит вас об этом и предложит задать другой порт вручную.

9. В окне укажите следующие параметры:

- В поле **Host** введите IP-адрес или DNS-имя компьютера с модулем PT AI Enterprise Server для доступа к сервисам.
- В поле **File sources path** — путь до папки, в которую будут загружаться файлы для сканирования, по умолчанию задан путь `C:\ProgramData\Application Inspector\Sources`.
- В поле **Update service working folder** — путь до папки для работы с обновлениями.
- В поле **FUS server host** — адрес сервера обновлений АО "Позитив Текнолоджиз".
- В поле **License server host** — адрес сервера лицензий.
- В поле **Gateway service https port** введите порт шлюза для сервисов, использующих протокол https.
- В поле **Gateway service http port** введите порт шлюза для сервисов, использующих протокол http.
- В поле **Auth service port** введите порт для подключения к сервису авторизации и аутентификации.
- В поле **Project service port** введите порт для подключения к сервису с данными проектов.
- В поле **File service port** введите порт для подключения к сервису работы с файлами.
- В поле **Settings service port** введите порт для подключения к сервису настроек.
- В поле **Agent auth gateway port** введите порт для подключения PT AI Enterprise Agent.
- В поле **Descriptions service port** введите порт для подключения к сервису описаний.
- В поле **Vault server port** введите порт для подключения к сервису защищенного хранения учетных данных Vault.
- В поле **Notify service port** введите порт для подключения к сервису нотификации.

- В поле **Issue tracker service port** введите порт для подключения к сервису отслеживания задач.
- В поле **Consul service port** введите порт для подключения к сервису Consul.
- В поле **Update service port** введите порт для подключения к сервису обновлений.
- В поле **UI service port** введите порт для подключения к веб-интерфейсу PT AI Enterprise Edition.
- В поле **Change history service port** введите порт для сервиса журнала истории событий.
- В поле **System management service port** введите порт для подключения к сервису управления системой.
- В поле **Scan scheduler port** введите порт для подключения к сервису управления очередью сканирования.

10. Нажмите кнопку **Next**.

    Откроется окно конфигурации сертификатов.

11. В поле **Location of SSL certificate** укажите расположение серверного сертификата.
12. В поле **SSL password** введите пароль для серверного сертификата.
13. Если в компании есть сервер выдачи и отзыва сертификатов, установите флажок **Verify client certificate for revocation**.
14. Нажмите кнопку **Next**.

    Откроется окно конфигурации администратора с глобальными полномочиями.

15. В поле **Administrators** введите имя пользователя (sAMAccountName), которому будет назначена роль администратора.

    Примечание. Вы можете назначать несколько администраторов, указывая их имена через ";".

16. Нажмите кнопку **Next**.
17. Убедитесь в правильном выборе параметров установки и нажмите кнопку **Install**.

    Начнется установка модуля на ваш компьютер. Дождитесь завершения установки.

    Примечание. Во время установки PT AI Enterprise Server также будет выполнена установка Microsoft .NET 4.7.2 Development Pack, если он не был установлен ранее. В этом случае для корректной работы может потребоваться перезагрузка операционной системы после установки.

18. Нажмите кнопку **Finish**.

Установка модуля PT AI Enterprise Server завершена.

6.2. Установка модуля PT AI Enterprise Viewer

► Чтобы установить модуль PT AI Enterprise Viewer на компьютер:

1. Запустите установочный файл.

   Откроется окно выбора языка установки.

2. Выберите язык установки и нажмите кнопку **ОК**.
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. Установите флажок **Создать значок на рабочем столе**, чтобы создать ярлык на рабочем столе.
9. Убедитесь в правильном выборе параметров установки и нажмите кнопку **Установить**.

   Начнется установка модуля на ваш компьютер. Дождитесь завершения установки.

   Примечание. Во время установки PT AI Enterprise Viewer также будет выполнена установка Microsoft .NET 4.7.2 Development Pack, если он не был установлен ранее. В этом случае для корректной работы может потребоваться перезагрузка операционной системы после установки.

10. Нажмите кнопку **Завершить**.

    Установка PT AI Enterprise Viewer завершена.

6.3. 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

Подготовка к развертыванию модуля PT AI Enterprise Agent (см. раздел 6.3.1)

Установка модуля PT AI Enterprise Agent (см. раздел 6.3.2)

Настройка модуля PT AI Enterprise Agent (см. раздел 6.3.3)

6.3.1. 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 Java: Apache Maven.
- Для загрузки зависимостей языка PHP: Composer.

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

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

6.3.2. 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. Нажмите кнопку **Далее**.
4. В окне с текстом Лицензионного соглашения ознакомьтесь с условиями Лицензионного соглашения.
5. Выберите **Я принимаю условия соглашения**, если вы согласны со всеми пунктами Лицензионного соглашения.
6. Нажмите кнопку **Далее**.

   Подготовка к установке программы будет продолжена.
7. Выберите папку для установки программы.
8. Нажмите кнопку **Далее**.
9. 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.

Примечание. Для создания токена доступа необходимо по завершении установки модуля PT AI Enterprise Server перейти в веб-интерфейс PT AI Enterprise Edition и выполнить инструкцию из раздела "Создание токена доступа" в Руководстве пользователя.

10. Нажмите кнопку **Далее**.
11. Если вместе с модулем PT AI Enterprise Agent не требуется установка службы управления агентами сканирования, в открывшемся окне снимите флажок **Work with scan scheduler**.

    Примечание. Если служба не установлена, то агент сканирования можно запускать только через консоль. Сканирование в интерфейсе PT AI Enterprise Viewer будет недоступно.
12. Убедитесь в правильном выборе параметров установки и нажмите кнопку **Установить**.

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

    Установка модуля PT AI Enterprise Agent завершена.

6.3.3. 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`.

Примечание. Если у вас установлена предыдущая версия PT AI Enterprise Edition, вы можете продолжать работать с клиентским сертификатом и настраивать подключение модуля PT AI Enterprise Agent по нему.

► 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, как показано на рисунке ниже.

```
<Agent.Properties.Settings>
  <setting name="AuthCertificatePassword" serializeAs="String">
    <value>Password</value> // Пароль от клиентского сертификата
  </setting>
  <setting name="AuthCertificatePath" serializeAs="String">
    <value>AI.Enterprise.Client.Development.pfx</value> // Путь до файла сертификата
  </setting>
  <setting name="SettingProviderUri" serializeAs="String">
    <value>https://ai-enterprise-server.domain.ru</value> // Адрес сервера
  </setting>
  <setting name="AccessToken" serializeAs="String">
    <value>Token</value> // Токен доступа
  </setting>
</Agent.Properties.Settings>
```

Рисунок 2. Настройка модуля PT AI Enterprise Agent

3. Сохраните файл.

Модуль PT AI Enterprise Agent настроен.

6.4. 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 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 6.4.1)

Установка AI.Shell из инсталлятора для Microsoft Windows (см. раздел 6.4.2)

Конфигурирование AI.Shell и запуск сканирования (см. раздел 6.4.3)

6.4.1. 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

ОС	Расширение пакета 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 содержимое в каталог `/usr/share/aisa`.
  2. Выполните команду установки:
     `sh/<Путь к каталогу с Ai.Shell>/scripts/install.sh`

     Примечание. Вы можете удалить AI.Shell командой `sh/<Путь к каталогу с Ai.Shell>/scripts/remove.sh`.

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

   Примечание. Для создания токена доступа необходимо по завершении установки модуля PT AI Enterprise Server перейти в веб-интерфейс PT AI Enterprise Edition и выполнить инструкцию из раздела "Создание токена доступа" в Руководстве пользователя.
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.

6.4.3. Конфигурирование AI.Shell и запуск сканирования

Вы можете 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.
2. Запустите сканирование командой:

`aisa --project-name "<Имя проекта сканирования>" --scan-target "<Путь к цели сканирования>"`, если вы настроили подключение AI.Shell к PT AI Enterprise Server на предыдущем шаге;

`aisa --set-settings –u <Адрес PT AI Enterprise Server> -t <Токен доступа> --project-name "<Имя проекта сканирования>" --scan-target "<Путь к цели сканирования>"`, если вы не настраивали подключение на предыдущем шаге.

Примечание. Для запуска сканирования с помощью AI.Shell используются те же параметры запуска, что и для PT AI Enterprise Agent, а также специфичные параметры (см. таблицу ниже).

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`

По завершении сканирования помимо стандартных кодов возврата могут отображаться коды, специфичные для AI.Shell:

— 27 — версия AI.Shell устарела, доступна новая версия для обновления;

— 28 — отсутствуют активные агенты сканирования;

— 29 — не указан токен доступа для AI.Shell.

7. Настройка сканирования

После установки всех модулей PT AI Enterprise Edition необходимо настроить параметры сканирования проекта и политику безопасности. Политика безопасности — это набор условий, необходимых для достижения требуемого уровня безопасности программного продукта. Нарушение политики безопасности задается в правиле. В процессе сборки проекта агент сборки проверяет соответствие результатов сканирования заданным в правиле условиям и прекращает сборку, если политика нарушена.

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

- Во время настройки агента сборки. Параметры сканирования вы указываете на шаге создания конфигурационного файла. Правило срабатывания политики безопасности вы указываете на шаге создания политик безопасности.
- До настройки агента сборки. Вы заранее создаете текстовые файлы с параметрами сканирования и правилом срабатывания политики безопасности. При настройке агента сборки вы указываете путь к созданным файлам. В этом случае настраивать параметры сканирования и политику безопасности в агенте сборки 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.

Настройка параметров сканирования на агенте сборки рассмотрена в разделе по интеграции PT AI Enterprise Edition в CI-процесс.

В этом разделе

7.1. 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.

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

7.2. 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	Набор правил (политика сработает, если хотя бы один скоуп актуален)
Scope	Rules	Список правил внутри скоупа (если все правила совпадают, скоуп актуален)
Rule	Field	Название поля 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 агента сборки.

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 до файла 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
          }
        ]
      }
    ]
  }
]
```

8. Интеграция PT AI Enterprise Edition в CI-процесс

PT AI Enterprise Edition может быть интегрован в CI-процесс на различных агентах сборки. Интеграция позволяет проверять код на наличие уязвимостей в процессе сборки проекта.

В этом разделе

8.1. Настройка агента сборки TeamCity

Настройка агента сборки TeamCity состоит из пяти шагов:

1. Настройка системы контроля версий (VCS).
2. Создание конфигурационного файла (необязательный шаг).
3. Сборка исходных кодов.
4. Создание политик безопасности (необязательный шаг).
5. Настройка запуска сканирования.

► Чтобы настроить агент сборки TeamCity:

1. Настройте VCS для выгрузки исходного кода в папку:
   - Откройте проект сборки на агенте TeamCity.
   - В меню настройки проекта сборки выберите **Version Control settings**.
   - Нажмите кнопку **Attach VCS Root**.
   - На открывшейся странице **Edit VCS Root** укажите тип VCS, в которой хранится исходный код, адрес репозитория и полный путь до локальной папки, в которую выгружается код из репозитория.

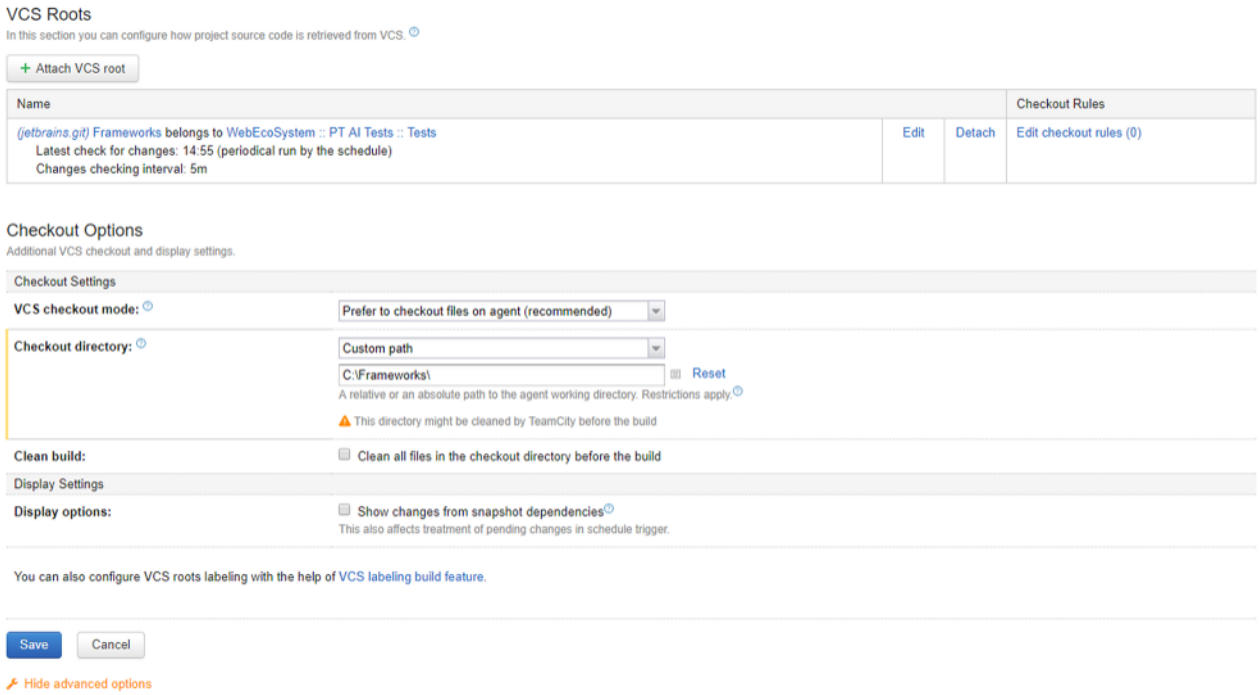

Рисунок 3. Настройка VCS

2. Нажмите кнопку **Save**.
3. Если вы хотите прописать конфигурационный файл на агенте сборки, добавьте шаг, который создает файл:
   - В меню настройки проекта выберите **Build Steps**.
   - Нажмите кнопку **Add build step**.
   - В раскрывающемся списке **Runner type** выберите **Create Text File**.
   - В поле **File Content** введите текст конфигурационного файла.
   - В поле **Destination file** укажите полный путь до папки на компьютере, куда будет сохранен конфигурационный файл.

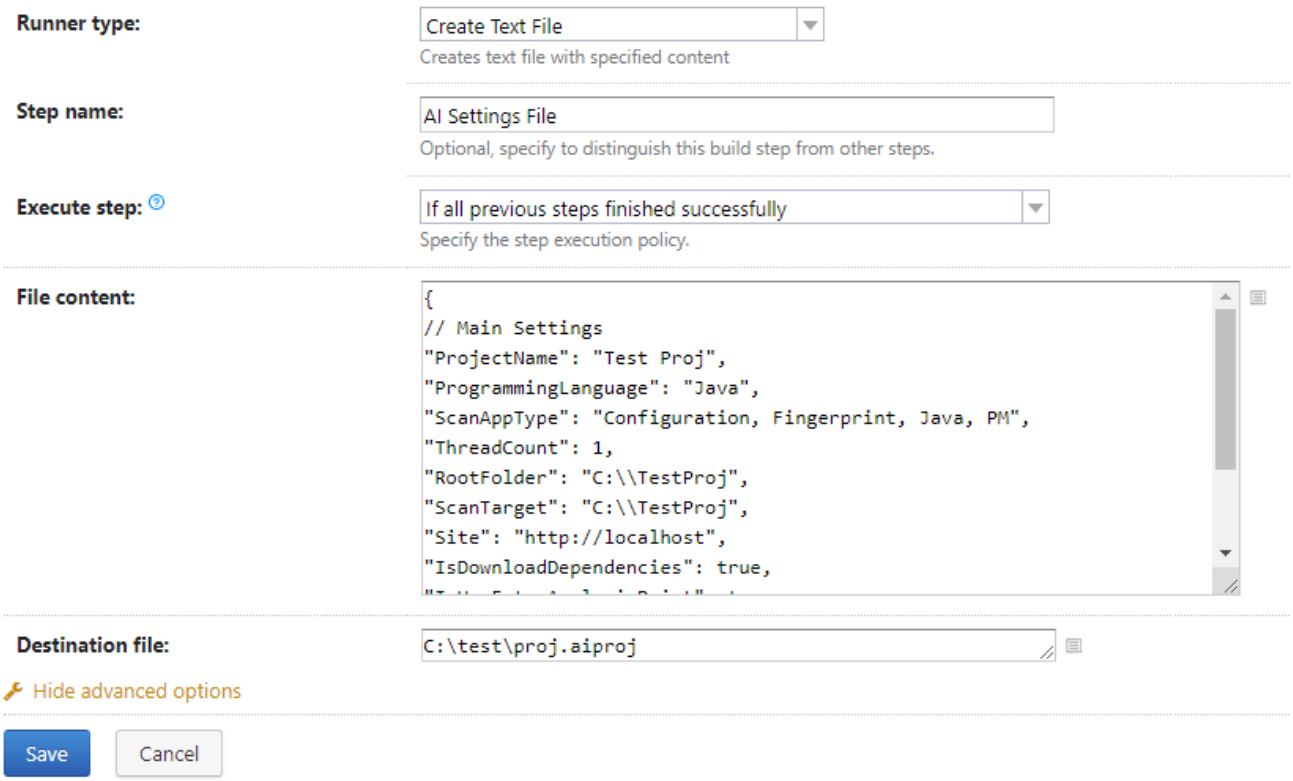

Рисунок 4. Создание конфигурационного файла

4. Нажмите кнопку **Save**.
5. Настройте шаг сборки исходных кодов:
   - Нажмите кнопку **Add build step**.
   - В раскрывающемся списке **Runner type** выберите **Command Line**.
   - В поле **Step name** введите имя шага сборки.
   - В поле **Execute step** укажите способ выполнения шага сборки **If all previous steps finished successfully**.
   - В поле **Working directory** укажите полный путь до корневой папки с приложением, содержащим исходный код.
   - В раскрывающемся списке **Run** выберите **Custom script**.
   - В поле **Custom script** введите команду `mvn clean package`.

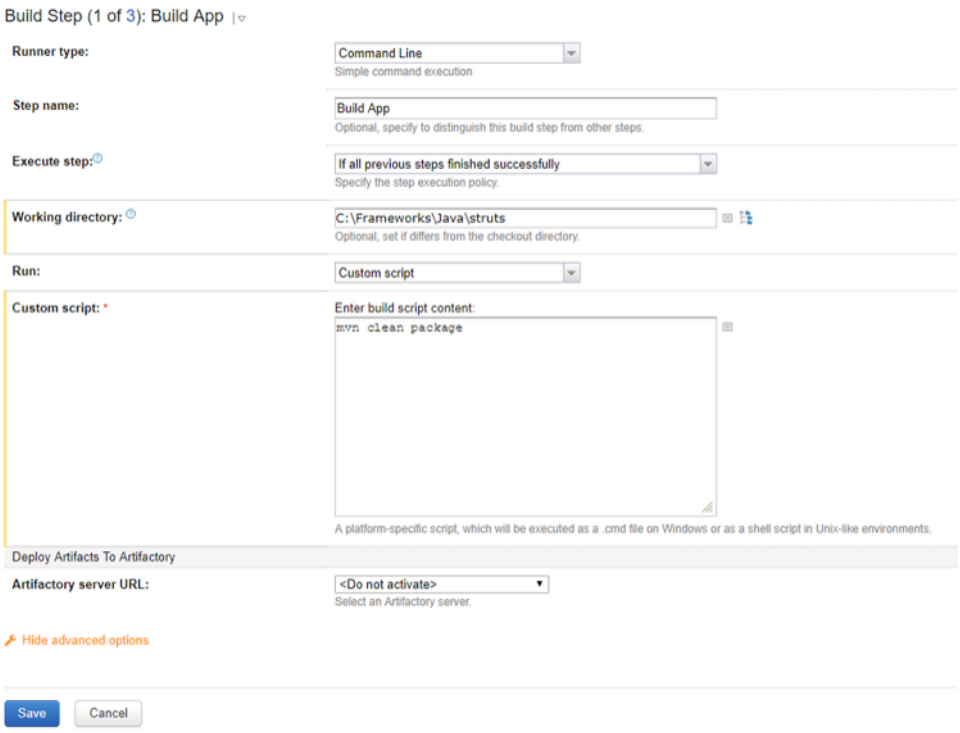

Рисунок 5. Настройка сборки исходных кодов

6. Нажмите кнопку **Save**.
7. Настройте шаг создания политик:
   - Нажмите кнопку **Add build step**.
   - В раскрывающемся списке **Runner type** выберите **Create Text File**.
   - В поле **Step name** введите имя шага сборки.
   - В поле **Execute step** укажите способ выполнения шага сборки **If all previous steps finished successfully**.
   - В поле **File Content** введите текст файла политики.
   - В поле **Destination file** укажите полный путь до папки на компьютере, куда будет сохранен файл с политикой.

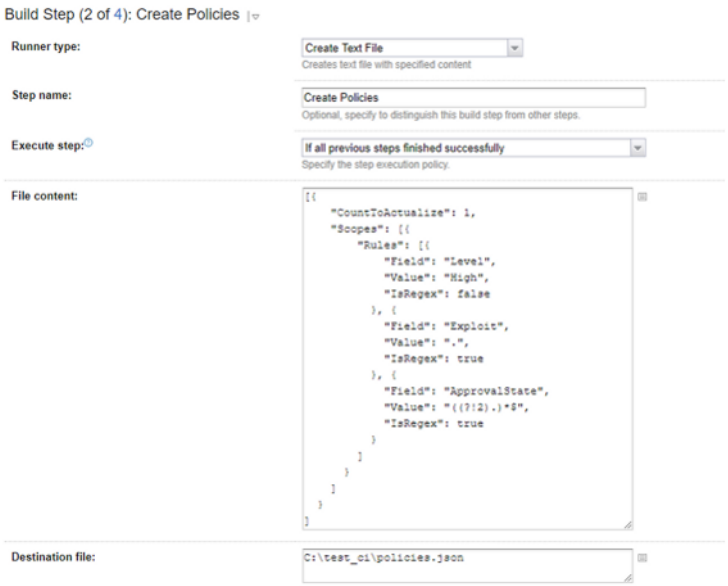

Рисунок 6. Настройка создания файла политик

8. Нажмите кнопку **Save**.
9. Настройте шаг запуска сканирования из консоли:
   - Нажмите кнопку **Add build step**.
   - В раскрывающемся списке **Runner type** выберите **Command Line**.
   - В поле **Step name** введите имя шага сборки.
   - В поле **Execute step** укажите способ выполнения шага сборки **If all previous steps finished successfully**.
   - В раскрывающемся списке **Run** выберите **Custom script**.
   - Если сканирование настроено в интерфейсе PT AI Enterprise Edition, в поле **Custom script** введите команду: `aic.exe --project-name "<имя проекта сканирования>" --scan-target "<путь к цели сканирования>" --policies-path "<путь к файлу с описанием политик>" --reports "<формат сохранения отчета: HTML, JSON, PDF, WAF>" --reports-folder "<путь к папке для сохранения отчетов>"`
   - Если сканирование настроено в конфигурационном файле, в поле **Custom script** введите команду: `aic.exe --project-settings-file "<путь к конфигурационному файлу>" --scan-target "<путь к цели сканирования>" --policies-path "<путь к файлу с описанием политик>" --reports "<формат сохранения отчета: HTML, JSON, PDF, WAF>" --reports-folder "<путь к папке для сохранения отчетов>"`

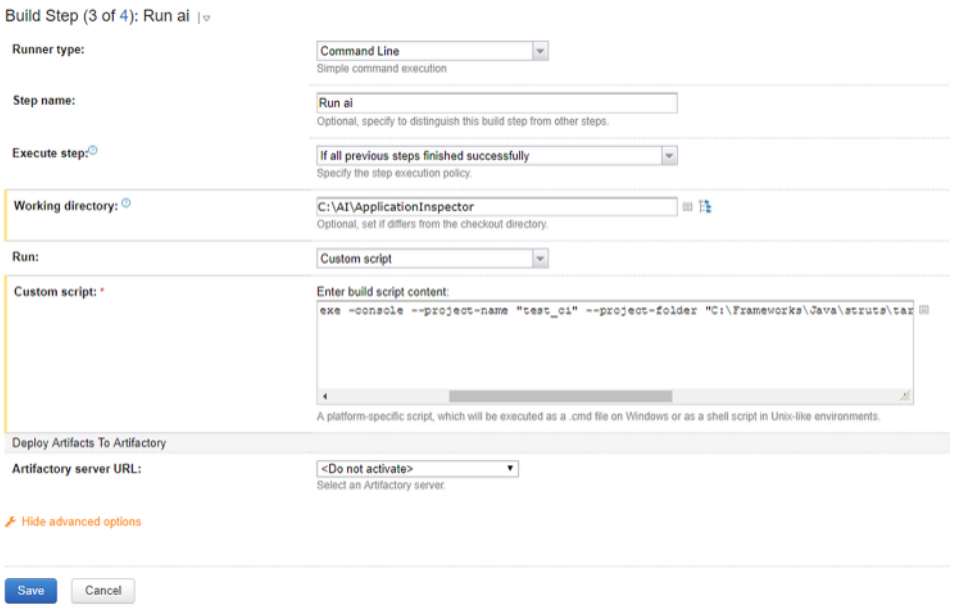

Рисунок 7. Настройка запуска сканирования из консоли

10. Нажмите кнопку **Save**.
11. Запустите сборку проекта.

    По завершении сканирования на странице сборки проекта отобразится код возврата и результат сборки. Список возможных кодов возврата приведен в Приложении (см. приложение B).

Рисунок 8. Результат выполнения сканирования

8.2. Настройка агента сборки Jenkins

В зависимости от количества сканируемых проектов возможны два способа настройки агента сборки Jenkins.

Если вам нужно проверить на наличие уязвимостей один проект, вы можете использовать базовую настройку Jenkins. При этом нужно настраивать агент сборки отдельно для каждого проекта.

Если вам нужно проверить несколько проектов одновременно, рекомендуется настраивать Jenkins с помощью плагина. Плагин позволяет не настраивать агент сборки отдельно для каждого проекта.

В этом разделе

Базовая настройка агента сборки Jenkins (см. раздел 8.2.1)

Настройка агента сборки Jenkins с помощью плагина (см. раздел 8.2.2)

8.2.1. Базовая настройка агента сборки Jenkins

> **Примечание.** Базовая настройка используется, если не установлена служба управления агентами сканирования.

Базовая настройка агента сборки Jenkins состоит из пяти шагов:

1. Настройка системы контроля версий (VCS).
2. Создание конфигурационного файла (необязательный шаг).
3. Сборка исходных кодов.
4. Создание политик безопасности (необязательный шаг).
5. Настройка запуска сканирования.

► Чтобы настроить агент сборки Jenkins:

1. Настройте VCS для выгрузки исходного кода в папку:
   - Откройте страницу конфигурации проекта на агенте Jenkins.
   - В блоке **General** установите флажок **GitHub project**.
   - В поле **Project URL** введите адрес репозитория, в котором хранится исходный код сканируемого приложения.
   - Нажмите кнопку **Advanced** в нижней части блока **General**.
   - Установите флажок **Use custom workspace**.
   - В поле **Directory** укажите полный путь до локальной папки, в которую выгружается код из репозитория.

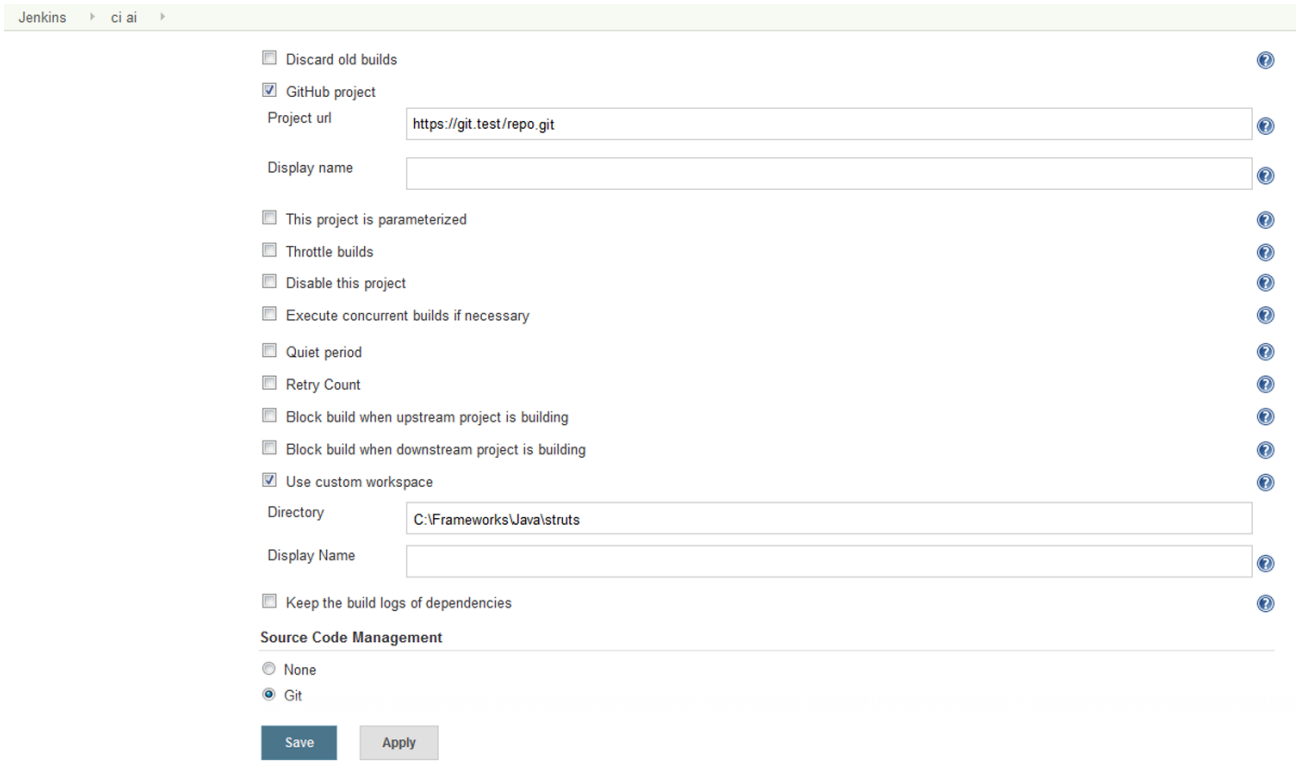

Рисунок 9. Настройка VCS

2. Если вы хотите прописать конфигурационный файл на агенте сборки, добавьте шаг, который создает файл:

   - В блоке **Build** нажмите кнопку **Add build step** и в раскрывшемся меню выберите пункт **Execute Windows batch command**.
   - В поле **Command** введите текст конфигурационного файла в соответствии с синтаксисом, принятым для написания BAT-файлов.

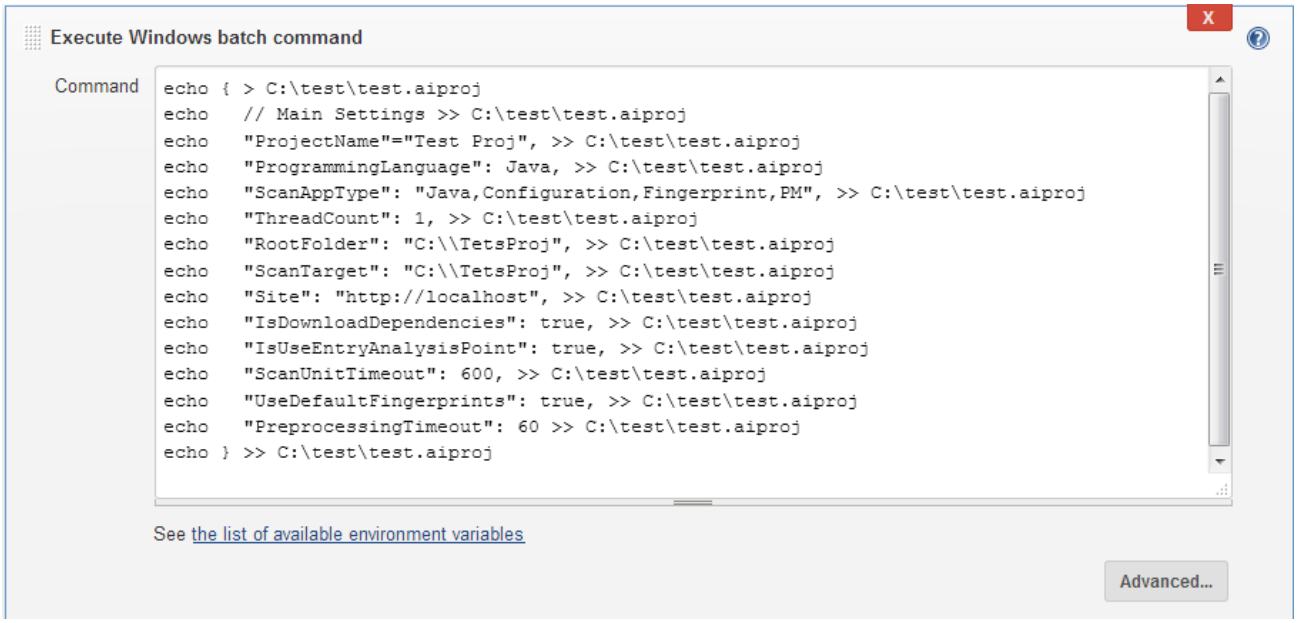

Рисунок 10. Создание конфигурационного файла

3. Настройте шаг сборки исходных кодов:
   - В блоке **Build** нажмите кнопку **Add build step** и в раскрывшемся меню выберите пункт **Invoke top-level Maven targets**.
   - В раскрывающемся списке **Maven Version** выберите **maven**.
   - В поле **Goals** введите `clean package`, как показано на рисунке ниже.

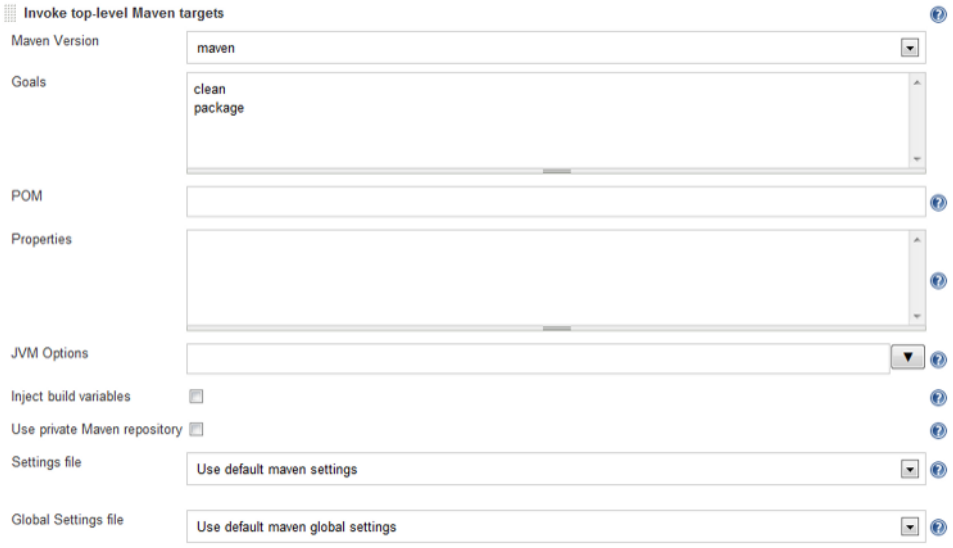

Рисунок 11. Настройка сборки исходных кодов

4. Настройте шаг создания политик:

- В блоке **Build** нажмите кнопку **Add build step** и в раскрывшемся меню выберите пункт **Execute Windows batch command**.
- В поле **Command** введите текст файла политики в соответствии с синтаксисом, принятым для написания BAT-файлов.

Рисунок 12. Настройка создания файла политик

5. Настройте шаг запуска сканирования из консоли:
   - В блоке **Build** нажмите кнопку **Add build step** и в раскрывшемся меню выберите пункт **Execute Windows batch command**.
   - Если сканирование настроено в интерфейсе PT AI Enterprise Edition, в поле **Command** введите команду: `aic.exe --project-name "<имя проекта сканирования>" --scan-target "<путь к цели сканирования>" --policies-path "<путь к файлу с описанием политик>" --reports "<формат сохранения отчета: HTML, JSON, PDF, WAF>" --reports-folder "<путь к папке для сохранения отчетов>"`
   - Если сканирование настроено в конфигурационном файле, в поле **Command** введите команду: `aic.exe --project-settings-file "<путь к конфигурационному файлу>" --scan-target "<путь к цели сканирования>" --policies-path "<путь к файлу с описанием политик>" --reports "<формат сохранения отчета: HTML, JSON, PDF, WAF>" --reports-folder "<путь к папке для сохранения отчетов>"`

Рисунок 13. Настройка запуска сканирования из консоли

6. Нажмите кнопку **Save**.
7. Запустите сборку проекта.

   По завершении сканирования на странице **Console Output** отобразится код возврата и результат сборки. Список возможных кодов возврата приведен в Приложении (см. приложение B).

```
Checking out Revision a08e800b023b8c5d28577fbe7f0275f106ac7e2b (refs/remotes/origin/master)
Commit message: "Master fix"
 > git.exe config core.sparsecheckout # timeout=10
 > git.exe checkout -f a08e800b023b8c5d28577fbe7f0275f106ac7e2b
 > git.exe rev-list a08e800b023b8c5d28577fbe7f0275f106ac7e2b # timeout=10
[struts2] $ cmd.exe /C "C:\soft\mvn\bin\mvn.cmd clean package && exit %%ERRORLEVEL%%"
[INFO] Scanning for projects...
[INFO]
[INFO] ------------------------------------------------------------------------
[INFO] Building StrutsExample Maven Webapp 1.0-SNAPSHOT
[INFO] ------------------------------------------------------------------------


C:\Frameworks\Java\struts>echo           }  1>>c:\test_ci\policies.json

C:\Frameworks\Java\struts>echo          ]  1>>c:\test_ci\policies.json

C:\Frameworks\Java\struts>echo       }  1>>c:\test_ci\policies.json

C:\Frameworks\Java\struts>echo     ]  1>>c:\test_ci\policies.json

C:\Frameworks\Java\struts>echo   }  1>>c:\test_ci\policies.json

C:\Frameworks\Java\struts>echo ]  1>>c:\test_ci\policies.json

C:\Frameworks\Java\struts>exit 0
[struts] $ cmd /c call C:\Users\user\AppData\Local\Temp\jenkins3895922381476295227.bat

C:\Frameworks\Java\struts>cd /d C:\AI\ApplicationInspector   && aic.exe -console --project-name "test_ci"
--project-folder "C:\Frameworks\Java\struts\target" --policies-path "C:\test_ci\policies.json" --reports "HTML,JSON,PDF"
--reports-folder "C:\test_ci\reports"
Work started
Project test_ci running
Invalid license token. Try reconnect.
Attempt 1 of 5.
Loading project test_ci
Project test_ci loaded
Run scan service
Inspection result d8307b88-4d9d-454d-ba23-898991a86331 from 09.02.2018 15:53:29 loaded
Scan completed
Report generation started at C:\test_ci\report.json
Report generation finished
Load politic from C:\test_ci\policies.json
1 loaded
Items to check 50

C:\AI\ApplicationInspector>exit 10
Build step 'Execute Windows batch command' marked build as failure
Finished: FAILURE
```

Рисунок 14. Результат выполнения сканирования

8.2.2. Настройка агента сборки Jenkins с помощью плагина

Настройка агента сборки Jenkins с помощью плагина состоит из следующих шагов:

1. Загрузка плагина в Jenkins.
2. Настройка подключения плагина к PT AI Enterprise Server.
3. Настройка проектной задачи. Проектная задача создается отдельно для каждого проекта.

Загрузка плагина в Jenkins

- Чтобы загрузить плагин в Jenkins:

  1. Скачайте плагин из репозитория по ссылке github.com/PositiveTechnologies/ptaiPlugins.
  2. Выполните сборку плагина с помощью Maven: `mvn clean install -DskipTests`.

     Примечание. Для сборки плагина необходимо предварительно установить и настроить JDK версии 8.
  3. Перейдите в веб-интерфейс Jenkins.
  4. В левой части главной страницы выберите раздел **Manage Jenkins**.
  5. На открывшейся странице выберите пункт **Manage Plugins**.
  6. Выберите вкладку **Advanced**.
  7. В блоке **Upload Plugin** нажмите кнопку **Choose File**.
  8. В открывшемся окне выберите файл `ptai-jenkins-plugin.hpi` в папке ptai-ee-tools-java\ptai-jenkins-plugin\target, созданный по завершении сборки, и нажмите кнопку **Open**.
  9. Нажмите кнопку **Upload**.

  Плагин PT AI EE plugin загружен и отображается на странице **Plugin Manager** на вкладке **Installed**. Вы можете перейти к настройке подключения плагина к PT AI Enterprise Server.

Настройка подключения плагина к PT AI Enterprise Server

- Чтобы настроить подключение плагина к PT AI Enterprise Server:

  1. В левой части главной страницы выберите раздел **Manage Jenkins**.
  2. На открывшейся странице выберите пункт **Configure System**.
  3. В списке параметров в блоке **PT AI vulnerability analysis** нажмите кнопку **Add PT AI global configuration**, чтобы добавить новое подключение к PT AI Enterprise Server.

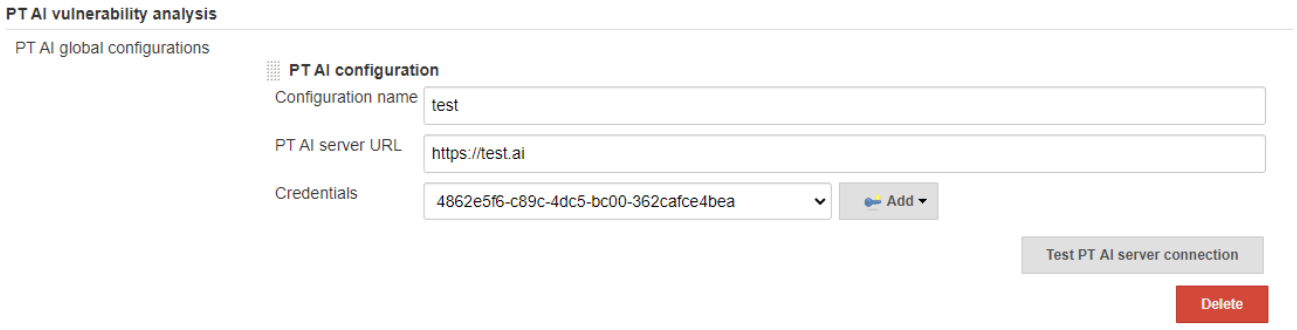

Рисунок 15. Настройка подключения плагина к PT AI Enterprise Server

4. В поле **Configuration name** введите имя подключения, которое будет отображаться в веб-интерфейсе Jenkins.
5. В поле **PT AI server URL** введите адрес PT AI Enterprise Server.
6. Нажмите кнопку **Add** рядом с полем **Credentials** и в раскрывшемся меню выберите пункт **Jenkins**.

   Откроется окно **Jenkins Credentials Provider: Jenkins**.

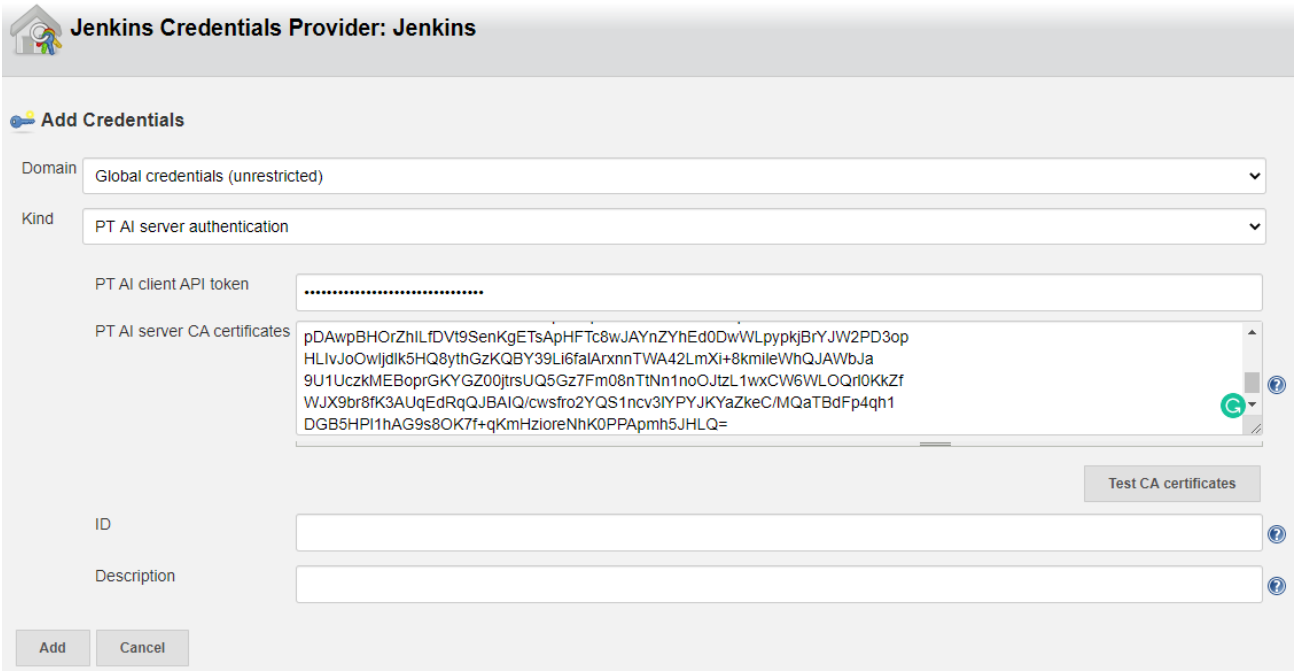

Рисунок 16. Добавление сертификатов

7. В раскрывающемся списке **Kind** выберите **PT AI server authentication**.
8. В поле **PT AI client API token** введите токен доступа для плагинов CI/CD.

   Примечание. Для создания токена доступа необходимо перейти в веб-интерфейс PT AI Enterprise Edition и выполнить инструкцию из раздела "Создание токена доступа" в Руководстве пользователя.
9. В поле **PT AI server CA certificates** укажите серверный сертификат.
10. По кнопке **Test CA certificates** проверьте серверный сертификат.
11. Нажмите кнопку **Save**.

Подключение плагина к PT AI Enterprise Server настроено. Вы можете перейти к настройке проектной задачи.

Настройка проектной задачи

► Чтобы настроить проектную задачу:

1. В левой части главной страницы выберите раздел **New Item**.
2. На открывшейся странице выберите пункт **Freestyle project** и укажите в поле название проекта.
3. Нажмите кнопку **OK**.
4. На открывшейся странице в блоке **Source Code Management** в поле **Repository URL** введите адрес репозитория, в котором хранится исходный код сканируемого приложения.
5. В блоке **Build** в меню кнопки **Add build step** выберите плагин **PT AI vulnerability analysis**.
6. В раскрывающемся списке **Scan settings type** выберите:
   - **PT AI Viewer UI-defined settings**, если сканирование настроено в PT AI Enterprise Viewer.
   - **JSON-defined settings**, если вы хотите прописать конфигурационный файл и файл политики безопасности на агенте сборки.
7. Если вы выбрали **PT AI Viewer UI-defined settings**, в поле **Project name** введите имя проекта, созданного и настроенного в PT AI Enterprise Viewer.

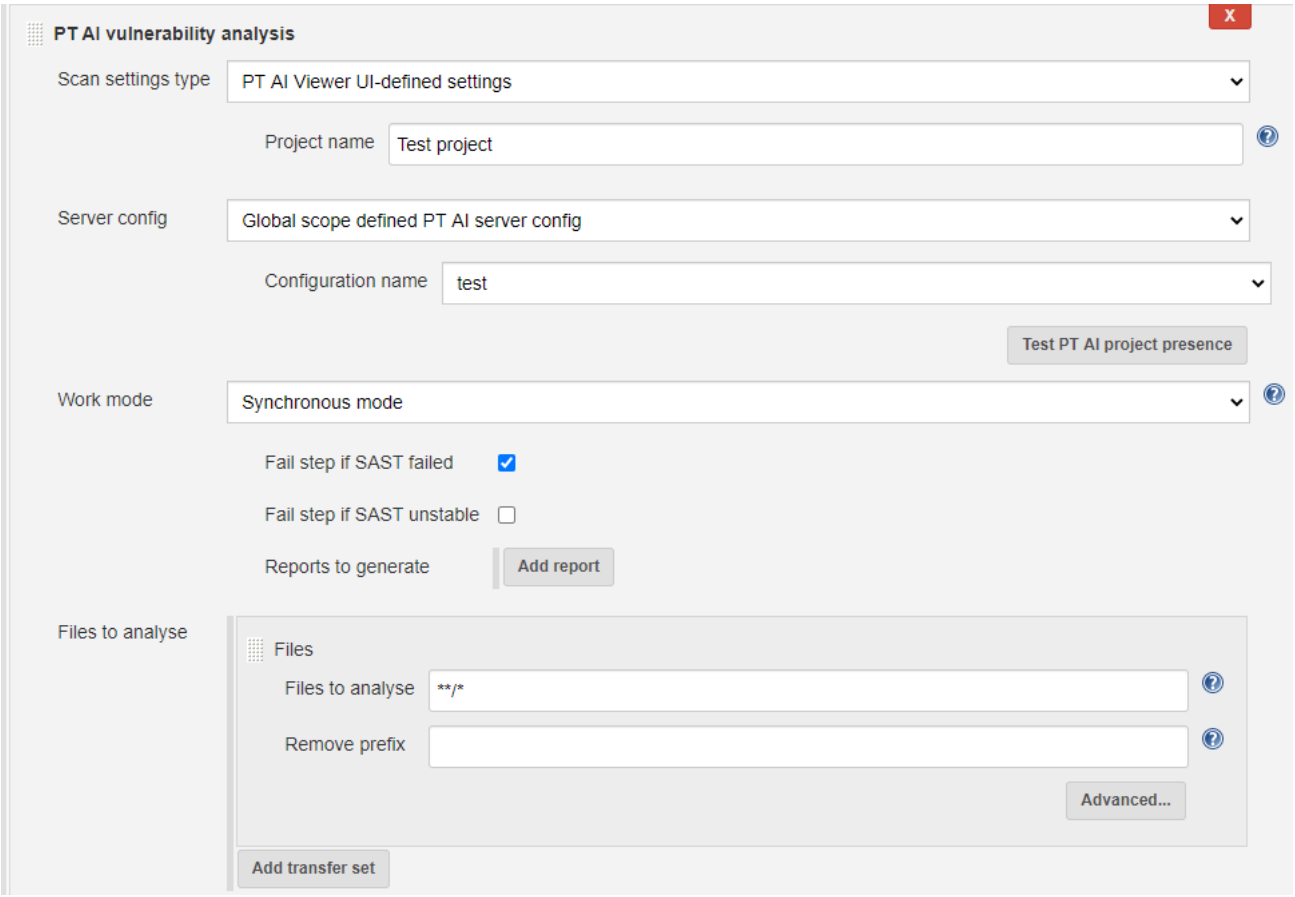

Рисунок 17. Настройка проектной задачи, если сканирование настроено в PT AI Enterprise Viewer

8. Если вы выбрали **JSON-defined settings**, в полях **Scan settings** и **Policy** введите текст конфигурационного файла и файла политики (опционально) в формате JSON.

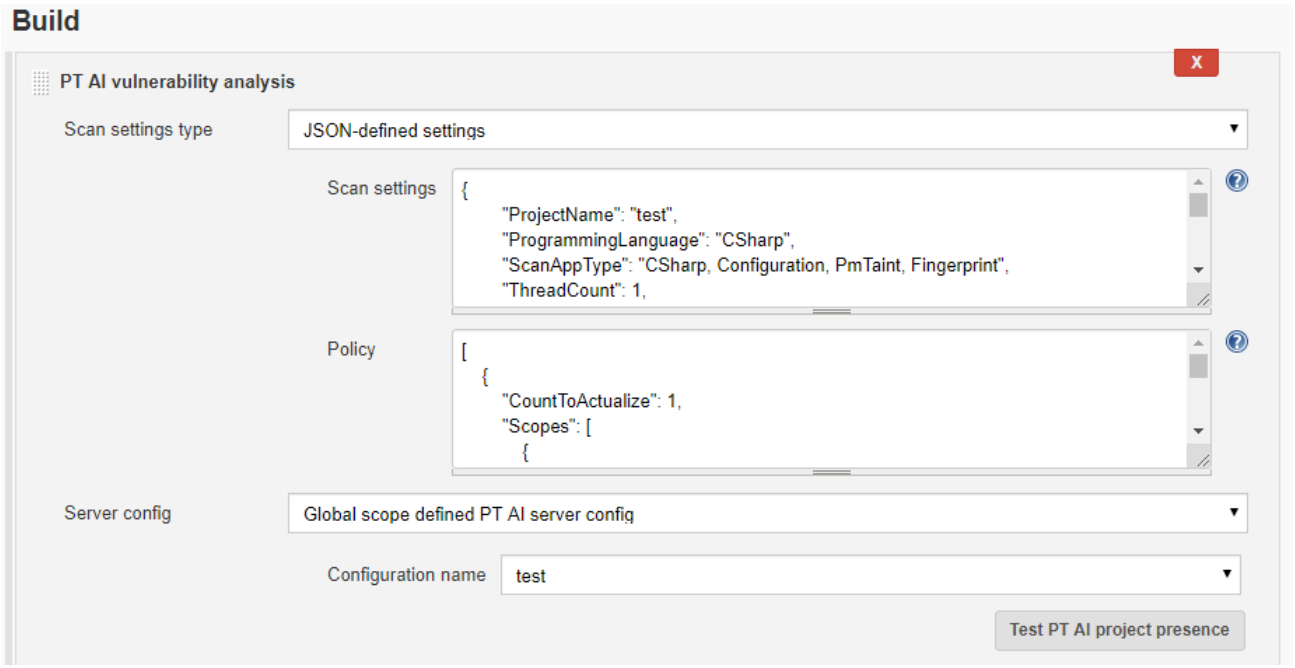

Рисунок 18. Настройка проектной задачи, если сканирование настроено на агенте сборки

9. В раскрывающемся списке **Server config** выберите:
   - **Global scope defined PT AI server config** для использования глобальных параметров плагина, заданных на шаге настройки подключения плагина к PT AI Enterprise Server.
   - **Task scope defined PT AI server config** для использования параметров плагина, заданных для конкретного проекта. Например, если вы хотите настроить подключение проекта к другому PT AI Enterprise Server.
10. Если вы выбрали **Global scope defined PT AI server config**, в поле **Configuration name** выберите имя PT AI Enterprise Server, заданное при настройке подключения плагина к PT AI Enterprise Server.
11. Если вы выбрали **Task scope defined PT AI server config**, настройте параметры подключения плагина для конкретного проекта аналогично параметрам подключения плагина к PT AI Enterprise Server.
12. В раскрывающемся списке **Work mode** выберите:
    - **Asynchronous mode** для сканирования в асинхронном режиме. В этом случае Jenkins запустит проверку кода на наличие уязвимостей и продолжит сборку, не дожидаясь завершения проверки.
    - **Synchronous mode** для сканирования в синхронном режиме. В этом случае Jenkins запустит проверку кода на наличие уязвимостей и будет ожидать завершения проверки.
13. Если вы выбрали **Synchronous mode**:
    - Установите флажок **Fail step if SAST failed**, чтобы Jenkins останавливал сборку при несоответствии сканируемого приложения заданной политике безопасности.

- Установите флажок **Fail step if SAST unstable**, чтобы Jenkins останавливал сборку при возникновении ошибок, не связанных с результатами проверки кода на наличие уязвимостей (например, ошибки в конфигурации, отсутствующая или недействительная лицензия).

14. В поле **Files to analyze** задайте возможность включения и (или) исключения определенных файлов из сканирования по маске.
15. Нажмите кнопку **Save**.
16. Запустите сборку проекта.

По завершении сборки запустится проверка кода на наличие уязвимостей через плагин. Результаты проверки будут сохранены в отчете проекта в разделе **Workspace**.

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 support.ptsecurity.com или по телефону. Запросы на портале — основной способ обращений за технической поддержкой.

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

В этом разделе

9.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать запросы на техническую поддержку.

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

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", 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. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по телефону +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языках.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданному запросу.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте запрос на портале support.ptsecurity.com. Запрос на портале, созданный и обновляемый по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

9.3. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся запросам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

9.4. Как служба технической поддержки работает с запросами

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

В этом разделе

Предоставление информации для технической поддержки (см. раздел 9.4.1)

Типы запросов (см. раздел 9.4.2)

Время реакции и приоритизация запросов (см. раздел 9.4.3)

Выполнение работ по запросу (см. раздел 9.4.4)

9.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" нужно предоставить:

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

"Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

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

9.4.2. Типы запросов

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

Вопросы по установке, повторной установке и предстартовой настройке продукта

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

Вопросы по администрированию и настройке продукта

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

Восстановление работоспособности продукта

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

Обновление продукта

"Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

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

9.4.3. Время реакции и приоритизация запросов

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

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

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

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

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

9.4.4. Выполнение работ по запросу

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

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

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

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

Приложение А. Пример конфигурационного файла

Ниже приведен пример конфигурационного файла, в котором задаются параметры сканирования. Вы можете прописать конфигурационный файл при настройке агента сборки или в отдельном текстовом файле.

```
{
 // Настройка основных параметров
 "ProjectName": "Test_Proj", // Имя проекта
 "ProgrammingLanguage": "Csharp", // Язык приложения: Java, Php, Csharp, VB,
ObjectiveC, CPlusPlus, Sql, Swift, Python, JavaScript, Kotlin, Go
 "ScanAppType": "CSharp , Configuration, Fingerprint, PmTaint ", // Модули поиска
уязвимостей:  Php, Java, CSharp, Configuration, Fingerprint, PmTaint , Blackbox,
JavaScript


 "ThreadCount": 1, // Количество потоков
 "Site": "http://localhost", // Адрес сайта
 "IsDownloadDependencies": true, // Загрузить зависимости


 "IsUsePublicAnalysisMethod": false, // Искать от доступных public и protected
методов
 "IsUseEntryAnalysisPoint": true, // Искать от точек входа


 "ScanUnitTimeout": 600, // Максимальное время сканирования файла в секундах
 "PreprocessingTimeout": 60, // Тайм-аут препроцессинга в минутах
 "CustomParameters": null, // Дополнительные параметры запуска


 "SkipFileFormats": ["*.gif"], // Форматы файлов, исключенные из сканирования
 "SkipFilesFolders": ["\\.git\\", "\\.gitignore", "\\.gitmodules", "\
\.gitattributes", "\\$tf\\", "\\$BuildProcessTemplate\\", "\\.tfignore"], // Фильтр
дерева


 // Поиск уязвимостей
 "DisabledPatterns": ["145", "146", "148", "149"], // Поиск по шаблонам, отключенные
шаблоны
 "DisabledTypes": [], // Проверки исходного кода, отключенные проверки исходного кода
 "ConsiderPreviousScan": true, // Учитывать предыдущее сканирование
 "UseIssueTrackerIntegration": true, // Использовать интеграцию с Jira


 // Параметры языка Java
```

```
 "IsUnpackUserPackages": false, // Распаковывать пользовательские пакеты
 "JavaParameters": null, // Параметры запуска JDK
 "JavaVersion": 0, // Версия JDK, 0 соответствует версии 1.8, 1 соответствует версии
1.11

 // Параметры языка C#
 "ProjectType": "Solution", // Типа проекта: Solution, WebSite
 "SolutionFile": "path_to_solution.sln", // Путь к файлу решения/проекта
 "WebSiteFolder": "path_to_website", // Папка сайта

 // Параметры языка JavaScript
 "JavaScriptProjectFile": "path_to_file", // Путь к файлу скрипта
 "JavaScriptProjectFolder": "path_to_dir", // Путь к корневой папке проекта
javascript

 // Параметры PMTaint
 "UseTaintAnalysis": false, // Использовать taint-анализ
 "UsePmAnalysis": true, // Использовать только pm-анализ
 "DisableInterpretCores": false, // Игнорировать ядра интерпретации (C#, Java, PHP)
при анализе

 // Параметры базы знаний YARA
 "UseDefaultFingerprints": true, // Использовать базу уязвимых компонентов PT AI
 "UseCustomYaraRules": false, // Использовать пользовательские правила YARA

 // Настройка параметров черного ящика
 "BlackBoxScanLevel": "None", // Режим поиска: Fast, Normal, Full
 "CustomHeaders": [["", ""]], // Дополнительные 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-путь к форме
   "regexp_of_success": null // Шаблон проверки
  }
 },
 "ProxySettings": {
  "IsEnabled": false, // Активировать параметры прокси-сервера
  "Host": null, // IP-адрес
  "Port": null, // Порт
  "Type": 0, // Тип прокси: 0 = HTTP, 1 = HTTPNOCONNECT, 2 = SOCKS4, 3 = SOCKS5
  "Username": null, // Логин
  "Password": null // Пароль
 },


// Настройка автоматической проверки уязвимостей
 "RunAutocheckAfterScan": false, // Запустить автопроверку после сканирования
 "AutocheckSite": "http://localhost", // Адрес сайта для автопроверки, если адрес не
указан, используется значение параметра "Site"
 "AutocheckCustomHeaders": [["", ""]], // Дополнительные заголовки
 "AutocheckAuthentication": {
  "auth_item": {
   "domain": null, // Адрес проверки
   "credentials": {
    "cookie": null, // Значение cookie
    "cookies": null,
```

```
    "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, // поле "Адрес проверки"
   "form_url": null, // поле "Адрес формы"
   "form_xpath": ".//form",  // XPath-путь к форме
   "regexp_of_success": null // Шаблон проверки
  }
 },
 "AutocheckProxySettings": {
  "IsEnabled": false, // Активировать параметры прокси-сервера
  "Host": null, // IP-адрес
  "Port": null, // Порт
  "Type": 0, // Тип прокси: 0 = HTTP, 1 = HTTPNOCONNECT, 2 = SOCKS4, 3 = SOCKS5
  "Username": null, // Логин
  "Password": null // Пароль
 },


 "SendEmailWithReportsAfterScan": true, // Отправлять отчет на почту по завершении
сканирования
 "CompressReport": false, // Сжимать отчет перед отправкой


 // Настройка отправки почты
 "EmailSettings": {
  "SmtpServerAddress": "mail.ptsecurity.ru", // Адрес SMTP-сервера
```

```
  "UserName": "testagent_wes@ptsecurity.com", // Имя пользователя
  "Password": "P@ssw0rd", // Пароль
  "EmailRecipients": "User@ptsecurity.ru", // Адрес получателя отчета, вы можете
указывать несколько адресов через ";"
  "EnableSsl": true, // Включить SSL
  "Subject": "Email Title", // Тема сообщения
  "ConsiderCertificateError": true, // Учитывать ошибки сертификата
  "SenderEmail": "testagent_wes@ptsecurity.com" // Отправитель
 },


  // Настройка отчета
 "ReportParameters": {
  "SaveAsPath": null,  // Папка для сохранения отчетов
  "UseFilters": false,  // Использовать фильтры
  "CreatePdfPrintVersion": false,   // Создавать версию для печати
  "IncludeDiscardedVulnerabilities": false, // Добавить в отчет опровергнутые
уязвимости
  "IncludeSuppressedVulnerabilities": false, // Добавить в отчет исключенные
уязвимости
  "IncludeSuspectedVulnerabilities": true, // Добавить в отчет подозрения на
уязвимость
  "IncludeGlossary": false, // Добавить в отчет справочник об уязвимостях
  "IncludeDFD": false // Добавить диаграмму потока данных
 }
}
```

Приложение Б. 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, PDF, JSON, WAF. Вы можете указывать несколько форматов через запятую
`--report-type`	Нет	Тип отчета, создаваемого по окончании сканирования. Может принимать одно из следующих значений: PlainReport, AutoCheck, Nist, Oud4, Owasp, Owaspm, Pcidss, Sans. Если тип не задан, то генерируется отчет PlainReport
`--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
`--settings-export-file`	Нет	Выгрузка параметров проекта в файл по указанному пути в формате JSON

Параметр	Используется в легком агенте AI.Shell	Описание
`--scan-off`	Да	Создание проекта по конфигурационному файлу без запуска задачи сканирования. Используется вместе с параметром `--project-settings-file`

Приложение B. Коды возврата

По завершении сканирования на агенте сборки 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 настройке параметров проекта
6	Во время сканирования найдены ошибки
7	Ошибка отправки отчета на почту
8	Некорректный путь к конфигурационному файлу
9	Некорректный путь к папке отчетов
10	Сработала политика безопасности (сборка не удовлетворяет заданной политике безопасности)
11	Некорректные параметры настройки отчетов
12	Не найден клиентский сертификат
13	Сканирование было удалено
14	Ошибка аутентификации при настройке автоматической проверки уязвимостей
15	Некорректные параметры настройки 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 сканирования
19	Модуль сканирования не найден
20	Ошибка загрузки исходных файлов с сервера PT AI Enterprise Server
21	Тайм-аут оповещения PT AI Enterprise Server о нормальной работе PT AI Enterprise Agent
22	Ошибка в процессе обновления

Код	Описание
23	Неверный пароль от сертификата
24	Не найден серверный сертификат
26	Запущена служба планировщика. 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
60	Совмещенные коды 6 и 10. Сработала политика безопасности, и в ходе сканирования найдены некритичные ошибки
100	Сканирование отменено (Ctrl+C)
1000	Неопознанная ошибка

О компании

"Позитив Текнолоджиз" уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявить, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга "Эксперт-400".

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com