

SASTAV AI (artificial Intelligence)

Описание функциональных характеристик,
информация для установки,
эксплуатации ПО

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ.....	3
2 ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК.....	4
3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ.....	7
4 УСЛОВИЯ ЭКСПЛУАТАЦИИ И ОГРАНИЧЕНИЯ.....	8
5 ТРЕБОВАНИЯ К СИСТЕМЕ.....	9
6 ИНФОРМАЦИЯ ДЛЯ УСТАНОВКИ ПО.....	10
7 ИНФОРМАЦИЯ ДЛЯ ЭКСПЛУАТАЦИИ ПО.....	12
8 КОМАНДЫ УПРАВЛЕНИЯ И ЖУРНАЛЫ.....	13
9 ЗАВЕРШЕНИЕ И ОСТАНОВКА ПО.....	14
10 ПОДДЕРЖКА И ОБРАБОТКА ОШИБОК.....	15

1 ОБЩИЕ СВЕДЕНИЯ

Настоящий документ содержит описание функциональных характеристик AI SASTAV и общую информацию, необходимую для установки и эксплуатации программного обеспечения. Документ предназначен для публичного ознакомления и для специалистов, планирующих внедрение продукта.

Продукт	AI SASTAV
Правообладатель	ООО «Пайнап»
Версия	0.8.1
Дата релиза	08.08.2026
Редакция документа	14.09.2026
Формат поставки	Контейнеризированное серверное программное обеспечение с веб-интерфейсом и машинными форматами выдачи результатов.

AI SASTAV выполняет статический анализ исходного кода с сочетанием структурной модели, детерминированных методов и искусственного интеллекта. Продукт предназначен для выявления уязвимостей, дефектов безопасности и нарушений бизнес-логики, риск которых определяется контекстом приложения, распределением ролей, связями объектов и допустимой последовательностью операций.

AI SASTAV может эксплуатироваться самостоятельно и подключаться к SASTAV. Описанный в настоящем документе пользовательский сценарий использует веб-интерфейс с обозначением SASTAV и ядро сканирования AI SASTAV. При таком способе работы управление проектами и заданиями выполняется через этот веб-интерфейс.

Получение программного обеспечения

Установочный комплект и условия лицензирования предоставляет правообладатель. Комплект включает образ в формате tar, compose-файл, конфигурацию и скрипт установки; лицензия выдается после установки по сформированному коду.

<https://sastav.ru>

Техническая поддержка: Заргаров Александр Денисович; +7 (916) 397-19-15; azargarov@iitdgroup.ru.

2 ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК

AI SASTAV выполняет статический анализ исходного кода с сочетанием структурной модели, детерминированных методов и искусственного интеллекта. Продукт предназначен для выявления уязвимостей, дефектов безопасности и нарушений бизнес-логики, риск которых определяется контекстом приложения, распределением ролей, связями объектов и допустимой последовательностью операций.

ИИ-компонент может быть подключен через внешний провайдер либо развернут локально. Выбор модели не изменяет прикладной процесс: AI SASTAV формирует структурированные артефакты, проверяет ответ собственным валидатором и выдает нормализованный результат.

Решаемые задачи

Класс задачи	Примеры
Контроль доступа	IDOR, Broken Access Control, Missing Authorization, обход проверки владельца или роли.
Изоляция данных	Нарушение границы арендатора, смешение данных клиентов, несогласованная фильтрация по организации.
Бизнес-логика	Недопустимый переход состояния, повторная операция, обход лимита или обязательного согласования.
Архитектура и доверие	Непроверенная граница сервиса, доверие пользовательскому признаку, опасная связь компонентов, Insecure Design.
Внутренние политики	Нарушение проектных ограничений и требований безопасности, формализованных для конкретного приложения.

Все перечисленные далее функции реализованы в версии 0.8.1. Интеграционный обмен с SASTAV является опциональным; собственный анализ, хранение результата и аудит доступны без такой интеграции.

Программное обеспечение «AI SASTAV»

ОСНОВНЫЕ ФУНКЦИИ F-01–F-09

ID	Функция	Вход	Выход
F-01	Создание проектов и версий анализа	Наименование проекта, версия кода, параметры анализа.	Проект и идентификатор версии анализируемого кода.
F-02	Загрузка / импорт исходного кода	Архив исходного кода либо подключение к репозиторию.	Принятый снимок кода с составом файлов и идентификатором импорта.
F-03	Индексация и построение структурной модели кода	Снимок исходного кода и конфигурация языка.	AST, индекс сущностей, связи, графы вызовов и потоков данных.
F-04	Настройка профилей анализа и аналитических контуров	Профиль, выбранные анализаторы и параметры запуска.	Сохраненная конфигурация активного аналитического контура.
F-05	Настройка риск-политик	Правило или политика в формате Markdown, критерии и ограничения.	Версионированная риск-политика, применяемая к проекту.
F-06	Семантическая оценка кандидатов с применением ИИ	Кандидаты, структурированные артефакты кода и риск-политика.	Структурированная оценка сценария, участники, признаки и обоснование.
F-07	Валидация результатов	Ответ ИИ-компонента и ссылки на сущности структурной модели.	Подтвержденный либо отклоненный результат с диагностикой проверки.
F-08	Дедупликация и нормализация	Проверенные результаты разных правил и аналитических контуров.	Канонический набор результатов без повторов, в единой схеме.
F-09	Присвоение риска, статуса и тегов	Результат, риск-политика и действия пользователя.	Риск, статус, служебные метки и история их изменения.

Программное обеспечение «AI SASTAV»

ОСНОВНЫЕ ФУНКЦИИ F-10–F-17

ID	Функция	Вход	Выход
F-10	Доказательства, трасса и контекст	Канонический результат и структурная модель проекта.	Файлы, строки, межфайловая трасса, связанный контекст и объяснение.
F-11	Экспорт и интеграционный обмен	Отобранные результаты и параметры экспорта.	Отчет SARIF/JSON либо передача через интеграционный интерфейс.
F-12	Кэширование результатов	Повторно используемые структурные артефакты и результаты этапов.	Кэшированные объекты и ключи, сокращающие повторную обработку.
F-13	Журнал аудита	Действия пользователей и системные события анализа.	Собственный журнал AI SASTAV; при интеграции — также общий журнал SASTAV.
F-14	Создание, настройка и удаление проекта	Параметры проекта и команда пользователя в пределах его роли.	Измененное состояние проекта и запись о действии в журнале аудита.
F-15	Запуск/отмена задания, очередь и статус	Версия проекта, профиль, политика и команда запуска/отмены.	Задание, позиция/состояние очереди, ход выполнения и итоговый статус.
F-16	Фильтры и навигация по коду	Риск, статус, категория, компонент и выбранный результат.	Отфильтрованный список и переход к связанным файлам, строкам и сущностям.
F-17	Комментарии и фиксация решения по результату	Комментарий, новый статус и решение уполномоченного пользователя.	Сохраненное решение, комментарий и запись в журнале аудита.

Программное обеспечение «AI SASTAV»

3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Тип	Состав
Вход продукта	Исходный код и конфигурации; параметры проекта; профиль анализа; риск-политика в Markdown; исключения; при необходимости — реквизиты интеграции.
Промежуточные данные	AST, индекс сущностей и связей, графы вызовов и потоков, кандидаты, структурированный контекст ИИ, кэш и технические события.
Данные для ИИ	Производные структурированные артефакты: AST, связи, контекст, метаданные и применяемое правило. Исходный код в исходном виде внешней модели не передается.
Выход продукта	Результаты с категорией, риском и статусом; файлы и строки; трасса; объяснение и доказательства; отчет SARIF/JSON; интеграционная передача при настройке.
Аудит	Собственный журнал AI SASTAV; при интеграции события дополнительно передаются в общий журнал SASTAV.

Порядок формирования результата

1. Кандидат формируется детерминированным правилом, структурной моделью кода, риск-политикой либо их сочетанием.
2. Из проекта отбирается релевантный контекст и преобразуется в структурированные артефакты, достаточные для проверки сценария.
3. ИИ-контур выполняет семантическую оценку и возвращает структурированные признаки, участников сценария и обоснование.
4. Собственный локальный валидатор проверяет формат, ссылки на код и согласованность доказательств.
5. Результат нормализуется, объединяется с дублирующими срабатываниями и получает категорию, риск, статус и теги.
6. Результат сохраняется в мастер-системе и может быть выгружен в локальный файл SARIF/JSON.
7. Специалист подтверждает, отклоняет или уточняет результат; решение фиксируется в собственном журнале аудита AI SASTAV.

4 УСЛОВИЯ ЭКСПЛУАТАЦИИ И ОГРАНИЧЕНИЯ

AI SASTAV не гарантирует обнаружение всех уязвимостей и не заменяет тестирование, экспертное ревью и управление рисками.

Качество зависит от полноты исходного кода и контекста, точности риск-политики, поддерживаемости языка и выбранной модели.

Результат ИИ может содержать ошибочную оценку и перед блокирующим решением подлежит проверке специалистом.

При недоступности настроенного ИИ-провайдера семантический этап не выполняется; детерминированные этапы и ранее сохраненные результаты остаются доступны.

Самостоятельность продукта и подключение к SASTAV

AI SASTAV самостоятельно принимает задания, хранит проекты и конфигурации, строит структурную модель, выполняет анализ и валидацию, формирует результаты, обеспечивает экспорт и ведет собственный журнал аудита. Эти функции доступны без установки SASTAV.

При подключении к SASTAV AI SASTAV продолжает работать как самостоятельный аналитический компонент: получает задания и контекст через интеграционный интерфейс, передает результаты и дополнительно публикует события в общем журнале SASTAV. Отключение интеграции не лишает продукт собственной функции анализа и аудита.

AI SASTAV может эксплуатироваться самостоятельно и подключаться к SASTAV. Описанный в настоящем документе пользовательский сценарий использует веб-интерфейс с обозначением SASTAV и ядро сканирования AI SASTAV. При таком способе работы управление проектами и заданиями выполняется через этот веб-интерфейс.

Обработка данных ИИ-компонентом

AI SASTAV обрабатывает ответ модели локальным собственным валидатором. Запросы к модели не сохраняются и не используются для обучения; результаты сохраняются в мастер-системе и могут быть выгружены в локальные файлы. Собственный журнал сохраняется также при подключении к SASTAV; в интегрированном режиме события дополнительно поступают в общий журнал.

5 ТРЕБОВАНИЯ К СИСТЕМЕ

Параметр	Требование
Серверная ОС	Российская Unix-подобная серверная ОС для архитектуры x86-64, обеспечивающая работу Linux-контейнеров Docker и Docker Compose.
Процессор	Не менее 8 ядер.
Оперативная память	Не менее 24 ГБ.
Диск	Не менее 80 ГБ для развертывания и рабочих данных.
Контейнерная среда	Docker; в технологическом составе версии 0.8.1 указан Docker 20.10.16. Для команд данного руководства необходим доступный плагин Docker Compose с вызовом docker compose.
Клиент	Современный веб-браузер и сетевой доступ к адресу развернутого веб-интерфейса.
Права	Установку выполняет администратор целевого сервера с правом sudo и доступом к Docker. Работа в веб-интерфейсе выполняется под назначенной учетной записью.
HTTP	80/tcp для доступа к веб-интерфейсу по HTTP.
HTTPS	443/tcp, если HTTPS настроен при установке.
ИИ-контур	Доступ к настроенному внешнему API-провайдеру либо локальной модели. При отсутствии такого доступа семантический этап не выполняется.

Ресурсы увеличивают по объему исходного кода и требуемой параллельности. Совместимость конкретного выпуска ОС и компонентов контейнерной среды проверяют до начала установки.

6 ИНФОРМАЦИЯ ДЛЯ УСТАНОВКИ ПО

Получите у правообладателя комплект для согласованной версии и его контрольные суммы. Сравните SHA-256 установочных файлов с ведомостью поставки. Для файла ai-sast.tar используется команда `sha256sum ai-sast.tar`; результат сравнивают с контрольной суммой именно этого файла.

6.1 Подготовка и запуск мастера установки

Скачайте комплект поставки, распакуйте его в отдельный рабочий каталог и откройте терминал в каталоге, содержащем `setup_aisast.sh`. Сохраните структуру комплектных файлов: образ, compose-файл, конфигурация и скрипты должны оставаться доступны мастеру установки.

Предоставьте скрипту право выполнения и запустите его с правами администратора:

```
chmod +x setup_aisast.sh
sudo ./setup_aisast.sh
```

Мастер запрашивает параметры установки. Последовательно ответьте на его вопросы, выберите каталог установки и сохраните этот путь. Дождитесь окончания работы мастера. При сообщении об ошибке сохраните его текст и обратитесь к техническому специалисту; не продолжайте запуск до устранения причины.

Перейдите в каталог, который был выбран в мастере. В следующей команде `INSTALL_DIR` обозначает именно этот каталог. Вместо текста в угловых скобках укажите его фактический абсолютный путь:

```
INSTALL_DIR="<абсолютный путь каталога установки>"
cd -- "$INSTALL_DIR"
./start_sastav.sh
```

При первом запуске ожидается запрос лицензии и код установки. Скопируйте выведенный код и передайте вендору для получения лицензии. Этот запрос является этапом первичной активации.

6.2 Получение и импорт лицензии

Получите лицензию, соответствующую коду установленного экземпляра. Из каталога установки выполните:

```
sudo ./import_license.sh
```

Вставьте полученную лицензию в ответ на запрос скрипта. Ознакомьтесь с лицензионным соглашением; при принятии его условий введите Y. После завершения импорта повторно запустите продукт:

```
./start_sastav.sh
```

Используйте адрес веб-интерфейса и учетные данные, выведенные скриптом. Сохраните их для дальнейшей эксплуатации. Для самостоятельно установленного экземпляра используются именно данные этой установки.

6.3 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

После входа в веб-интерфейс перейдите к добавлению ядра сканирования. Создайте ядро со следующими параметрами и сохраните запись:

Поле	Значение
Название	Произвольное понятное название ядра.
Адрес	http://ai-sast:8585
Количество строк	100000
Количество потоков	1

Затем добавьте команду пользователей с произвольным названием. В дальнейшем выберите эту команду в настройках репозитория. Термин «команда» в этом шаге означает группу пользователей, а не команду терминала.

Проверьте доступность ядра и наличие нужного набора правил перед запуском анализа. В контрольном примере используется набор IDOR. Если требуемый набор отсутствует, получите его и порядок настройки у технического специалиста.

Для использования ИИ-компонента настройте доступ к выбранному внешнему провайдеру либо локальной модели в соответствии с конфигурацией поставки. Реквизиты провайдера должны быть доступны установленному экземпляру. Проверка готовности включает вход в веб-интерфейс и выполнение анализа подготовленного исходного кода.

7 ИНФОРМАЦИЯ ДЛЯ ЭКСПЛУАТАЦИИ ПО

7.1 Загрузка и вход

Откройте в браузере адрес установленного веб-интерфейса. Введите выданные администратором логин и пароль и нажмите «Войти в систему». После успешного входа открывается рабочая область с доступными проектами.

7.2 Проект и исходный код

В форме «Создание проекта» задайте название; описание необязательно. Нажмите «Создать проект» либо «Создать и перейти в проект». В проекте добавьте репозиторий: укажите название, набор правил, команду пользователей и тип лицензии. При необходимости выберите ядро сканирования AI SASTAV.

В блоке «Загрузка кода» выберите загрузку файлом либо подключение к репозиторию. Сохраните настройки. При загрузке файлом исходный архив прикладывается к запуску сканирования. Набор правил выбирают по задачам анализа; в качестве примера может использоваться IDOR.

7.3 Запуск и выполнение

Откройте добавление сканирования, выберите набор правил и укажите ветку анализируемого кода. Поле коммита и комментарий к запуску могут быть необязательными. Для файлового режима приложите архив и нажмите «Начать сканирование». Программа создает задание и отображает его состояние; во время начальной загрузки возможны статус «В процессе» и стадия «Скачивание».

Дождитесь окончания обработки, откройте результаты задания и карточку интересующего дефекта. Изучите правило, риск, статус, связанный код, местоположение и объяснение. Доступные фильтры позволяют отбирать результаты, а комментарии и смена статуса — фиксировать решение специалиста. При необходимости задание отменяется пользователем с соответствующими полномочиями.

7.4 Экспорт и завершение

Откройте «Скачать отчет», выберите SARIF либо JSON и нажмите «Скачать». Ожидаемый результат — отчет в выбранном формате. Сохраните необходимые файлы и выполните выход из учетной записи. Серверные компоненты продолжают работать после завершения пользовательской сессии.

8 КОМАНДЫ УПРАВЛЕНИЯ И ЖУРНАЛЫ

Состояние контейнеров

```
docker ps -a
```

Команда выводит контейнеры, используемые образы, состояние и имена. Найдите контейнеры данной установки с образами `hub.sastav.ru/*`. В столбце STATUS для работающего сервиса ожидается Up. Состояния Exited и Restarting требуют диагностики. Статус Up подтверждает запуск контейнера; функциональную готовность проверяют входом и контрольным анализом.

Журналы и параметры команды

Возьмите точное имя нужного контейнера из столбца NAMES. В следующих командах вместо <имя контейнера> укажите это имя:

```
docker logs "<имя контейнера>"
docker logs --tail 200 "<имя контейнера>"
docker logs --follow "<имя контейнера>"
```

Без параметров выводятся доступные сообщения журнала. Параметр `--tail 200` ограничивает вывод последними 200 строками. Параметр `--follow` показывает новые сообщения по мере поступления; Ctrl+C завершает просмотр, сохраняя работу контейнера.

Проверка контейнерной среды

```
docker --version
docker compose version
```

Команды выводят версии Docker и Docker Compose. Если `docker compose` не распознается, администратор должен установить совместимый плагин Compose до применения команд остановки из этого руководства. При отказе в доступе к Docker используйте учетную запись с выданными административными правами.

9 ЗАВЕРШЕНИЕ И ОСТАНОВКА ПО

Завершение пользовательской работы

Сохраните необходимые отчеты, завершите работу с результатами и выполните выход из учетной записи через меню пользователя. Выход из веб-интерфейса завершает пользовательскую сессию; серверные компоненты продолжают работать. Для прерывания задания используйте действие отмены задания в пределах полномочий своей роли.

Остановка серверных компонентов

Администратор открывает терминал в каталоге установленного комплекта. До остановки следует убедиться, что необходимые результаты сохранены и текущие задания могут быть прекращены. Выполните:

```
docker compose down  
docker ps -a
```

Первая команда останавливает и удаляет контейнеры и сети, которыми управляет данный Compose-проект. Вторая позволяет проверить состояние. Для возобновления эксплуатации из каталога установки выполните `./start_sastav.sh`.

Удаление установленного комплекта

После остановки администратор проверяет фактический путь каталога установки и удаляет только этот каталог средствами ОС. Остановка через `docker compose down` и удаление каталога сами по себе не означают удаления всех Docker-образов, именованных томов и внешних хранилищ. Их состав и принадлежность данному экземпляру проверяют отдельно; удаляют только ресурсы, которые больше не используются другими установками.

Обновление

Перед обновлением изучите примечания к новой версии и выполните предусмотренные миграции. Встроенное резервное копирование в редакции 0.8.1 не применяется; при необходимости оператор сохраняет конфигурацию и данные средствами своей инфраструктуры. После обновления повторите вход и контрольный анализ.

10 ПОДДЕРЖКА И ОБРАБОТКА ОШИБОК

При обращении в поддержку сообщите версию продукта, время возникновения ошибки, выполняемую операцию и ее результат. Для ошибки анализа дополнительно укажите идентификатор задания; для проблемы запуска — состояние контейнера и диагностические сообщения.

Ситуация	Проверка
Нет доступа к веб-интерфейсу	Адрес, HTTP/HTTPS, порт, сетевой маршрут, состояние контейнеров.
Не завершена активация	Код установки, соответствие лицензии, результат <code>import_license.sh</code> .
Не начинается анализ	Наличие настроенного ядра, набора правил, лицензии и исходного кода.
Ошибка семантического этапа	Доступность выбранного ИИ-компонента и его настройки.
Ошибка экспорта	Наличие результатов и выбранный формат SARIF или JSON.

Технический специалист: Заргаров Александр Денисович; +7 (916) 397-19-15; azargarov@iitdgroup.ru.

Часы приема обращений согласовываются с техническим контактом. Получение установочного комплекта, лицензии и обновлений выполняется в соответствии с условиями предоставления программного обеспечения правообладателем.