

# Техническая архитектура и безопасность

YasnoCore LLM 1.0.0 | ООО «ЯСНОКОР» | редакция 19.10.2026

| Компонент             | Граница                                                                                     |
|-----------------------|---------------------------------------------------------------------------------------------|
| Собственное ядро      | 11 модулей Python, версия 1.0.0, без обязательных pip-зависимостей                          |
| Gateway               | 127.0.0.1:8090; контроль формата/лимитов и аудит                                            |
| Inference             | Отдельный локальный процесс 127.0.0.1:8080; модель и нативный сервер лицензируются отдельно |
| CLI                   | Подготовка наборов, метрики, опись, smoke-test и запуск обучения                            |
| Дополнительный портал | Apache/PHP/MariaDB, HTTPS, аутентификация и роли подготовки корпуса                         |

Путь запроса: локальное клиентское приложение → YasnoCore LLM gateway → локальный inference-бэкенд → ответ клиенту. При такой конфигурации пользовательский текст не отправляется в облачный AI-сервис. Автоматического обращения к облачному API в собственном ядре нет.

Два домена llm.yasnocore.ru и llm.yasnosoft.ru используют один DocumentRoot и одну конфигурацию кабинета. Новый домен не создаёт вторую базу данных. Сессии браузера привязаны к имени хоста; при переходе между доменами может понадобиться отдельный вход.

## Защита исполнения

Проверенная ОС - Astra Linux SE 1.8.2 «Воронеж», режим 1. Служба работает от отдельной непривилегированной записи. Код принадлежит root; запись разрешена в выделенные служебные каталоги. Профиль защиты, ЗПС и МКЦ не отключаются. Нативный inference должен соответствовать правилам доверенной подписи Astra.

# Сторонние компоненты и ограничения

YasnoCore LLM 1.0.0 | ООО «ЯСНОКОР» | редакция 19.10.2026

| Компонент              | Роль / поставка                                                                    |
|------------------------|------------------------------------------------------------------------------------|
| CPython 3.11           | Интерпретатор; отдельно, PSF License                                               |
| llama.cpp              | Внешний inference-сервер; отдельно, MIT                                            |
| Веса модели            | Настраиваются отдельно; лицензия точного checkpoint проверяется до распространения |
| PyTorch / NumPy        | Опциональный CPU smoke-test; пакеты Astra отдельно                                 |
| Transformers / PEFT    | Опциональное полное обучение; не входят в подтверждённый CPU-профиль               |
| Apache / PHP / MariaDB | Среда отдельного кабинета; не обязательны для Python-ядра                          |

В проверенном окружении бэкэнд имеет рабочий alias Qwen3.8-27B. Alias - конфигурационное имя сервера; оно не является доказательством происхождения, версии upstream или лицензионных прав на checkpoint. Веса и лабораторные модели в архив не входят; их права не присваиваются ЯСНОКОР.

Наборы НТРК, частные тексты, чувашско-русские корпуса и адаптеры рабочих исследований не публикуются в документации и не передаются с проверочным экземпляром. Для использования каждого источника нужно отдельное документированное основание.

Внутренние API не имеют внешней пользовательской аутентификации. Защита строится на loopback и изоляции сервера; для внешних пользователей нужен отдельный защищённый шлюз. Эти документы не подтверждают формальную оценку защиты, работу с ненулевыми метками/МРД, качество на десяти языках либо уже выданный сертификат Ready for Astra.