

Справка для службы безопасности и ИТ

INTEBRIX Optimization Platform 1.0.0: форма поставки и режимы развёртывания, размещение данных, разграничение доступа, журнал аудита, совместимость с Astra Linux SE 1.8.2 и РЕД ОС 8.0.2, обновления, требования к инфраструктуре и границы ответственности

Справка описывает форму поставки INTEBRIX Optimization Platform 1.0.0, размещение данных, разграничение доступа, журнал аудита, подтверждённую совместимость с российскими операционными системами и границы ответственности поставщика. Правообладатель — ООО «ИНТЕБРИКС», ИНН 9707059284, ОГРН 1267700207895, аккредитованная ИТ-компания (реестр Минцифры России № 107180). Источники — эксплуатационная документация из состава поставки и протокол установочных испытаний от 18.08.2026.

1. Форма поставки и режимы развёртывания

Платформа — серверное приложение с веб-интерфейсом. Штатный способ развёртывания — контейнерный: Docker Compose, пять сервисов.

Сервис	Состав	Публикация порта на хосте
frontend	nginx 1.27: статика приложения (React 19), прокси <i>/api/</i> и <i>/ws/</i> , заголовки безопасности и политика CSP	80/tcp — внешний
api	FastAPI под Gunicorn (4 процесса) и Uvicorn, Python 3.12	5001/tcp — внешний
worker	Celery, решатели HiGHS и CBC; параллелизм 2 задачи	не публикуется
postgres	PostgreSQL 16	127.0.0.1:5433 — петлевой интерфейс
redis	Valkey 8 (Redis-совместимый) — кэш и брокер очереди	127.0.0.1:6380 — петлевой интерфейс

Режим задаётся параметром **deploy_mode: cloud** — размещение у правообладателя, **on_prem** — контур заказчика с доступом в сеть, **air_gapped** — изолированный контур. Значения пишутся через подчёркивание, написание через дефис приложением отвергается на старте.

Путей поставки два. Подключённый контур — исходный дистрибутив, образы собираются на машине заказчика. Закрытый контур — архив *intebrix-airgap-<версия>.tar.gz*: сохранённые образы (*images.tar*), файл состава сервисов, конфигурация nginx, эксплуатационные сценарии, образец параметров с предустановленным *DEPLOY_MODE=air_gapped*, контрольные суммы *SHA256SUMS*. Публичный реестр образов не используется ни в одном режиме.

Целостность комплекта подтверждается контрольными суммами SHA-256: перечень входит в архив, сумма самого архива сообщается заказчику отдельным каналом связи. Кэш переведён на Valkey (BSD-3) из-за лицензионных ограничений Redis 7/8; возврат к образам Redis в поставке запрещён.

2. Размещение данных

В режимах *on_prem* и *air_gapped* данные остаются в контуре заказчика, в томах Docker на узле установки. Расчётная функциональность полностью работает без доступа в интернет: обязательные компоненты входят в состав образов.

Что хранится: наборы исходных данных, модели, наборы ограничений и результаты; журнал расчётов с эхо входных данных — для воспроизведения расчёта; учётные записи (пароли — хеш *bcrypt*, политика: не короче 12 символов, проверка на пять последних); журнал аудита (адрес электронной почты, IP-адрес, действие, объект, время); реквизиты подключений к внешним источникам — в зашифрованном виде. Ключи API и ключи активации показываются один раз при выпуске, повторный просмотр невозможен. Резервная копия содержит дамп PostgreSQL, журналы за 30 суток и манифест; в неё попадают персональные данные, поэтому для хранения вне контура предусмотрено шифрование GPG.

Обращения к внешним сервисам необязательны и отключаются конфигурацией:

Сервис	Назначение	Отключение и поведение после него
OSRM	матрица расстояний и времён	<i>INTEBRIX_OSRM_ENABLED=false</i> либо адрес внутреннего экземпляра; расстояния считаются геодезически
YandexGPT	текстовые пояснения к результату	<i>LLM_PROVIDER=none</i> ; расчёт не затрагивается
Приёмник ошибок	сбор ошибок исполнения	пустой <i>SENTRY_DSN</i> ; инициализация только при <i>DEPLOY_MODE=cloud</i> , иначе запись в локальный файл
Telegram	уведомления о расчётах	пустой токен бота
Поставщик OIDC	единый вход	пустой <i>OIDC_ISSUER_URL</i> — работает встроенная аутентификация; допускается внутренний Keycloak
Тайлы карт	подложка карты	параметр сборки интерфейса и политика CSP; в закрытом контуре подложка не отображается, узлы, связи и расчёты работают полностью

Значения по умолчанию для OSRM и поставщика тайлов указывают на внешние публичные сервисы и при развёртывании в контуре заказчика подлежат переопределению — это отдельный пункт контрольного перечня после установки.

3. Разграничение доступа

Аутентификация. Пара токенов JWT (HS256): доступа — 60 минут, обновления — 30 суток с ротацией и хранением идентификатора выданного токена, повторное использование отозванного отклоняется. Поддерживаются двухфакторная проверка по одноразовым паролям TOTP (RFC 6238), блокировка учётной записи после серии неудачных попыток, автоматический выход при бездействии (30 минут), единый вход по OIDC, ключи программного доступа для машинных клиентов. Публичной регистрации нет: учётная запись создаётся администратором либо по выданному ключу активации.

Организация — граница видимости. Пользователь принадлежит ровно одной организации. Модели, наборы данных, история расчётов, журнал аудита, ключи API и интеграции доступны только внутри своей организации. Изоляция построена на трёх независимых уровнях: контекст арендатора берётся из записи пользователя в базе, а не из утверждения в токене (подмена значения в токене доступа не даёт);

все обращения к данным проходят через типовые функции с условием по идентификатору организации; на таблицах арендаторов включены политики защиты строк PostgreSQL. Второй уровень контролируется статическим анализатором в конвейере сборки: выборка из таблицы арендатора без фильтра по организации останавливает сборку.

Роль	Права
viewer	просмотр моделей и результатов
analyst	просмотр, создание и изменение моделей, запуск расчётов
manager	права аналитика, удаление моделей, управление составом команды, просмотр журнала аудита и статистики потребления
admin	все права, включая управление пользователями и ролями, ключи API, настройки организации, лицензию, очистку журнала аудита, выгрузку и удаление организации

Иерархия накопительная: *viewer* < *analyst* < *manager* < *admin*. Проверка выполняется на уровне обработчика — по конкретному полномочию либо по минимальному уровню роли.

При нехватке прав сервер в производственном режиме отвечает **403** без указания недостающего полномочия и роли; полное сообщение попадает в журнал сервера (событие *rbac.deny*), отказ фиксируется в журнале аудита. Диагностику ведёт администратор по журналу: подробный текст отказа раскрывал бы внутреннюю модель прав и подсказывал, какое полномочие требуется получить.

Обращение к чужому объекту возвращает 404, а не 403. Ответ 403 подтвердил бы существование объекта с таким идентификатором и позволил бы перебором собирать сведения о данных другой организации, не имея к ним доступа. Ответ 404 делает несуществующий и недоступный объект неразличимыми по коду ответа. Корректность изоляции покрыта сквозным тестом попыток доступа из одной организации к объектам другой.

Дополнительно: доступ к каждому расчётному ядру проверяется отдельно по составу лицензии; интерактивная документация API (*/docs*, */redoc*, */openapi.json*) по умолчанию отключена и в приложении, и в nginx, включается на время аудита; действуют ограничения частоты — 100 запросов в минуту в целом и 10 в минуту на запуск расчётов.

4. Журнал аудита

Записывается каждое действие, изменяющее состояние: идентификатор и адрес электронной почты пользователя, тип действия, тип и идентификатор объекта, дополнительные сведения, IP-адрес, отметка времени. Отдельно ведётся файловый журнал обращений *logs/audit.jsonl* — кто, что, сетевой адрес, путь, код ответа, длительность, режим только добавления. Начиная с версии 1.0.0 каталоги журналов вынесены в отдельные тома и переживают пересоздание контейнеров.

Неизменяемость обеспечена триггером уровня СУБД: разрешена только вставка, прямые попытки изменить или удалить записи через СУБД завершаются ошибкой.

Просмотр — роли *manager* и *admin* (раздел «Администрирование → Журнал», фильтр по типу действия). **Очистка по сроку хранения** возможна только штатной операцией и только для роли *admin* при четырёх условиях: срок хранения от 30 до 3650 суток, подтверждение вводом идентификатора организации, код двухфакторной проверки (если она включена у администратора) и выгрузка удаляемых записей в файл снимка в той же транзакции. Факт очистки сам фиксируется в журнале. Рекомендуемый срок хранения — не менее 12 месяцев, окончательное значение закрепляется регламентом эксплуатирующей организации. Обезличивание персональных данных пользователя выполняется отдельной операцией с подтверждением: записи истории расчётов сохраняются, но теряют привязку к автору.

5. Совместимость с российскими операционными системами

Испытания проведены 18.08.2026 на арендованных виртуальных серверах в России; проверены оба пути поставки.

Параметр	Стенд № 1	Стенд № 2
Операционная система	Astra Linux Special Edition 1.8.2 «Орёл»	РЕД ОС 8.0.2 MINIMAL
Ядро, архитектура	6.1.124-1-generic, x86_64	6.12.56-1.red80, x86_64
Путь поставки	подключённый контур: сборка образов на машине заказчика	закрытый контур: развёртывание из комплекта поставки без доступа в интернет
Docker	25.0.5.astra2	29.5.3
Docker Compose	2.20.2.astra2	5.3.1
Результат	развёрнуты пять служб, все прошли проверку состояния	развёрнуты пять служб, все прошли проверку состояния

Средства контейнеризации входят в штатные репозитории обеих систем, подключение сторонних источников не требуется. Установка в закрытом контуре выполнена одной командой, заняла 1 минуту 35 секунд, код возврата установщика 0, обращений в сеть Интернет не выполнялось; целостность комплекта подтверждена сверкой контрольной суммы SHA-256 на передающей и принимающей стороне. Штатный набор автоматических проверок дал на обеих системах совпадающий результат — 555 пройдено, 44 пропущено по условиям выполнения, 9 не пройдено, состав не пройденных совпадает полностью: восемь работают на данных заказчика, намеренно не включённых в поставку, девятая разобрана в протоколе (значение целевой функции совпало на всех платформах, состав плана на обеих российских системах совпал побайтово).

Два замечания протокола. На Astra Linux требуется пакет *docker-compose-v2*: пакет с именем *docker-compose* содержит версию 1.29.2, непригодную для работы. Сборка образов на машине заказчика зависит от доступности внешних репозиториях базовых пакетов, поэтому для российских заказчиков штатным следует считать развёртывание из комплекта закрытого контура.

6. Обновления и поддержка

В облачном режиме обновление применяет правообладатель в согласованное технологическое окно. В контуре заказчика и в изолированном контуре порядок задаёт штатный сценарий: резервная копия (точка отката) → получение новых образов из сети либо из переданного архива → остановка сервисов приложения и расчётного исполнителя при работающей СУБД → миграции схемы → пересоздание сервисов на новых образах → контрольная проверка живости. При отрицательном результате любого шага выполняется **автоматический откат** к копии, снятой перед обновлением; ход обновления протоколируется с отметками времени в UTC.

В закрытый контур обновление поставляется тем же комплектом, передаётся согласованным каналом (носитель, однонаправленный шлюз, выделенный канал) и проверяется по контрольным суммам перед установкой. Исправления безопасности, в том числе в сторонних компонентах, выпускаются внеочередным порядком с приоритетом; о мажорных и несовместимых изменениях уведомление направляется не позднее чем за 30 календарных дней до выпуска.

Поддержка: support@intebrix.ru и форма обратной связи, рабочие дни 10:00–19:00 по московскому времени, язык обращения и ответа русский. Сроки реакции: критический уровень — не более 4 рабочих часов, высокий — не более 8, обычный — не более 2 рабочих дней. На каждый подтверждённый дефект создаётся регрессионный тест, включаемый в постоянный набор. Показатель доступности не менее 99,5% в календарный месяц относится к облачному режиму размещения.

7. Требования к инфраструктуре

Параметр	Минимально	Рекомендуется
Процессор	4 ядра x86-64	8 и более ядер x86-64
Оперативная память	8 ГБ	16 ГБ и более
Дисковое пространство	50 ГБ SSD	200 ГБ и более SSD
Сеть	100 Мбит/с	1 Гбит/с

Системное ПО: Linux с ядром 5.x и выше, Docker Engine 24.0 и выше, Docker Compose 2.20 и выше, базовые *curl*, *openssl*, *tar*, *gpg* — при шифровании копий. Целевая архитектура промышленной эксплуатации — amd64. Отдельная установка Python, PostgreSQL, Valkey и nginx на хост не требуется.

Периметр: рекомендуется разрешить на хосте только 22, 80 и 443. СУБД и кэш привязаны к петлевому интерфейсу и наружу не публикуются, доступ к базе — через SSH-туннель. Контейнер веб-интерфейса слушает HTTP, TLS терминируется внешним обратным прокси заказчика; обязательна передача заголовка *X-Real-IP* (иначе ограничение частоты применяется ко всем пользователям совместно) и увеличенный таймаут чтения для длительных расчётов. Рабочее место: актуальные браузеры на движке Chromium (включая «Яндекс Браузер») и Mozilla Firefox, включённые JavaScript и cookie, WebSocket для отображения хода расчёта.

Контрольный перечень после установки включает стойкие значения ключей подписи и права 600 на файл параметров, производственный режим с отключённым отладочным выводом, изменённый пароль СУБД, закрытые снаружи порты СУБД и кэша, включённый TLS, настроенное резервное копирование с проверкой восстановления на тестовом узле, а для закрытого контура — режим *air_gapped* и отключённые внешние сервисы.

8. Что мы не делаем

- **Сертификата ФСТЭК России у платформы нет.** Ни один документ поставки такого сертификата не заявляет, аттестация по требованиям защиты информации не проводилась. Испытания 18.08.2026 — установочные испытания совместимости с российскими ОС, а не сертификационные. Актуальный статус сертификации и включения в реестр российского ПО сообщаем по запросу.
- **Платформа не терминирует TLS.** Внешний обратный прокси, сертификаты и их продление — на стороне заказчика.
- **Картографические подложки и сервис дорожной маршрутизации в комплект закрытого контура не входят.** Расчёты, узлы и связи работают в полном объёме, для подложки нужен собственный сервер тайлов в контуре заказчика.
- **Штатный состав рассчитан на один сервер.** Отказоустойчивая схема и балансировка нескольких узлов в составе поставки не описаны.
- **Удалённый доступ поставщика к установке в контуре заказчика штатным сопровождением не предусмотрен.** Обращения разбираются по фрагментам журналов и данным, которые передаёт

заказчик; воспроизведение выполняется на стенде разработчика.

- **Телефонного канала поддержки нет**, круглосуточное дежурство не предусмотрено: приём обращений — почта и форма обратной связи в рабочие часы, расширенный режим — по отдельному соглашению о сопровождении.
- **Ссылок на действующие внедрения справка не содержит** — приведены только результаты собственных испытаний и параметры, зафиксированные в документации поставки.

ООО «ИНТЕБРИКС», ИНН 9707059284, ОГРН 1267700207895, Москва — аккредитованная ИТ-компания (реестр Минцифры России № 107180). Программное обеспечение «INTEBRIX Optimization Platform», свидетельство Роспатента о государственной регистрации программы для ЭВМ № 2026684186 от 09.08.2026. Документ носит информационный характер и не является публичной офертой. Актуальная версия — intebrix.ru.