УТВЕРЖДАЮ
Генеральный директор
ООО «НАЙС СОФТ ГРУПП»
_____ С.С. Беликов
«____» _____ 2026 г.

ПРОГРАММНЫЙ КОМПЛЕКС

«НАЙС СОФТ ИИ СТУДИЯ»

версия 1.0.0

РУКОВОДСТВО ПО УСТАНОВКЕ

НССГ.10001-01 32 02-ЛУ

Лист утверждения

Красногорск
2026

Утвержден НССГ.10001-01 32 02-ЛУ

ООО «НАЙС СОФТ ГРУПП»

ПРОГРАММНЫЙ КОМПЛЕКС «НАЙС СОФТ ИИ СТУДИЯ»

Версия 1.0.0

РУКОВОДСТВО ПО УСТАНОВКЕ

НССГ.10001-01 32 02

Листов 50

Красногорск
2026

АННОТАЦИЯ

Настоящее руководство устанавливает порядок подготовки вычислительной среды, установки, первоначального запуска, проверки, ввода в эксплуатацию и удаления программного комплекса «Найс Софт ИИ Студия» версии 1.0.0.

Основной, референсной и рекомендуемой операционной системой является НАЙС.ОС CLOUD. Программный комплекс заявляется совместимым со всеми российскими серверными операционными системами, которые предоставляют необходимые Linux- и OCI-возможности и удовлетворяют опубликованным системным требованиям. Для иных российских ОС команды управления пакетами, межсетевым экраном и контейнерной средой выполняются по документации соответствующего правообладателя.

По содержанию документ относится к эксплуатационной документации системного программиста и подготовлен с учётом ГОСТ 19.101-2024, ГОСТ 19.503-79 и сложившейся практики оформления эксплуатационной документации программных комплексов в Российской Федерации. Руководство по установке выделено в самостоятельный документ для удобства внедрения и закупочной документации.

В документе используются преимущественно русские термины. Англоязычные обозначения сохранены только для точных названий программ, протоколов, команд, переменных и стандартов, когда их перевод может затруднить однозначное выполнение инструкции.

ПРЕДУПРЕЖДЕНИЕ. Перед промышленной установкой администратор должен сверить номер поставки, контрольные суммы, подписанный манифест и системные требования именно той редакции 1.0.0, которая передана заказчику. Значения аппаратных ресурсов для локальной модели зависят от выбранного модельного артефакта.

СОДЕРЖАНИЕ

1 Общие положения 6
2 Идентификация и комплект поставки 7
3 Варианты установки 8
4 Архитектура устанавливаемого комплекса 9
5 Подготовка сервера 10
6 Подготовка НАЙС.ОС CLOUD 11
7 Сеть и межсетевой экран 12
8 Подготовка хранилища 13
9 Проверка установочного комплекта 14
10 Установка из подключённого контура 15
11 Настройка адреса экземпляра 16
12 Предварительная проверка 17
13 Запуск установки 18
14 Проверка служб после установки 19
15 Первый запуск в браузере 20
16 Первоначальная настройка модели 21
17 Установка на сервер с графическими ускорителями 22
18 Установка без локального графического ускорителя 23
19 Доменное имя и сертификат 24
20 Первоначальная настройка администратора 25
21 Настройки безопасности после установки 26
22 Развёртывание на виртуальной машине 27
23 Развёртывание на физическом сервере 28
24 Развёртывание в облаке 29
25 Установка на других российских ОС 30
26 Установка через прокси-сервер 31
27 Установка в закрытом контуре 32
28 Полностью изолированная установка 33
29 Резервная копия после установки 34
30 Приёмочная проверка 35
31 Повторная установка и восстановление 36
32 Удаление программного комплекса 37
33 Типовые ошибки при установке 38
34 Сообщения установочных средств 39
35 Требования к протоколированию установки 40
36 Нормативные и справочные сведения 41
Приложение А. Матрица сетевых портов 42

Приложение Б. Контрольный лист подготовки сервера 43

Приложение В. Контрольный лист установки 44

Приложение Г. Команды проверки 45

Приложение Д. Шаблон протокола установки 46

Приложение Е. Контрольный лист изолированной поставки 47

Приложение Ж. Профили локальных моделей и GPU 48

Приложение И. Критерии готовности к вводу в эксплуатацию 49

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение документа

Руководство предназначено для инженеров внедрения, системных администраторов, специалистов по инфраструктуре и технических представителей заказчика, выполняющих развертывание ИИ Студии в локальной, облачной или изолированной инфраструктуре.

1.2 Основные принципы установки

- установка выполняется только из идентифицированного комплекта поставки версии 1.0.0;
- основной установочной платформой является НАЙС.ОС CLOUD;
- пользовательские и административные данные размещаются в постоянных каталогах и не должны храниться только внутри изменяемого контейнера;
- внешней поверхностью по умолчанию является единая HTTPS-точка входа; внутренние базы данных и служебные компоненты не публикуют свои порты;
- локальная модель является отдельным ресурсом и может быть установлена после запуска базового комплекса;
- при отсутствии подходящего GPU комплекс может работать с внешней или управляемой моделью;
- после установки обязательно выполняются проверка работоспособности и резервное копирование.

1.3 Термины

Термин	Значение
экземпляр	Отдельно развернутый программный комплекс ИИ Студии с собственной конфигурацией и данными.
поставочный комплект	Набор файлов, образов, манифестов, контрольных сумм и документации, переданный для установки.
локальная модель	Модель искусственного интеллекта, выполняемая на вычислительных ресурсах организации.
управляемая модель	Модель внешнего поставщика, доступ к которой выполняется через настроенный сервис.
контейнерная среда	Docker Engine и совместимый подключаемый модуль Docker Compose, используемые для запуска служб Студии.
проверка готовности	Автоматическая или ручная проверка того, что служба запущена и способна обслуживать штатные запросы.

2 ИДЕНТИФИКАЦИЯ И КОМПЛЕКТ ПОСТАВКИ

2.1 Идентификация продукта

Параметр	Значение
Наименование	Найс Софт ИИ Студия
Версия документации	1.0.0
Правообладатель	ООО «НАЙС СОФТ ГРУПП»
Официальный адрес продукта	https://studio.ncsgp.ru
Референсная ОС	НАЙС.ОС CLOUD
Запись НАЙС.ОС CLOUD в Реестре российского ПО	№30128 от 22.10.2025
Официальная запись Реестра	https://reestr.digital.gov.ru/reestr/4119206/

2.2 Состав типового комплекта поставки

- управляющий сценарий nicesoft.sh и вспомогательные сценарии;
- файл конфигурации контейнерного состава compose.yml;
- пример переменных окружения .env.example;
- конфигурация интерфейса и маршрутизации моделей;
- контейнерные образы либо сведения об их неизменяемых идентификаторах в подписанном манифесте;
- манифест версии и контрольные суммы;
- перечень сторонних компонентов и лицензий;
- эксплуатационная документация;
- для изолированной поставки - локальный набор всех требуемых контейнерных образов и, при заказе, модельных артефактов.

ПРИМЕЧАНИЕ. Файл .env содержит уникальные секреты конкретного экземпляра и не является общим поставочным файлом. Он создаётся при первоначальной настройке и должен защищаться как конфиденциальная эксплуатационная информация.

3 ВАРИАНТЫ УСТАНОВКИ

Вариант	Когда применяется	Особенности
Подключённый контур	Есть контролируемый выход в Интернет или корпоративные зеркала	Получение необходимых образов и модельных артефактов из разрешённых источников.
Корпоративный закрытый контур	Прямой Интернет запрещён, но есть внутренний реестр/прокси	Образы и обновления поступают через инфраструктуру организации.
Полностью изолированный контур	Сеть не имеет внешнего выхода	Используется заранее подготовленный переносимый комплект с образами и моделями.
Без локальной модели	Нет подходящего GPU или локальный вывод не требуется	Используется внешний совместимый поставщик модели или управляемая модель.
С локальной моделью	Данные должны обрабатываться внутри контура	Требуется совместимый NVIDIA GPU и доступ контейнерной среды к ускорителю.

ПРИМЕЧАНИЕ. Обычный заказчик не должен использовать сборочные команды разработчика для промышленной эксплуатации. Производственная поставка 1.0.0 должна использовать подготовленные и идентифицированные образы/артефакты, соответствующие манифесту выпуска.

4 АРХИТЕКТУРА УСТАНАВЛИВАЕМОГО КОМПЛЕКСА

ИИ Студия устанавливается как совокупность изолированных контейнерных служб. Единой внешней точкой входа является обратный посредник. Базы данных, поисковые службы, служба резервного копирования, управление моделями, интеграционный шлюз и другие внутренние компоненты работают во внутренних сетях контейнерной среды.

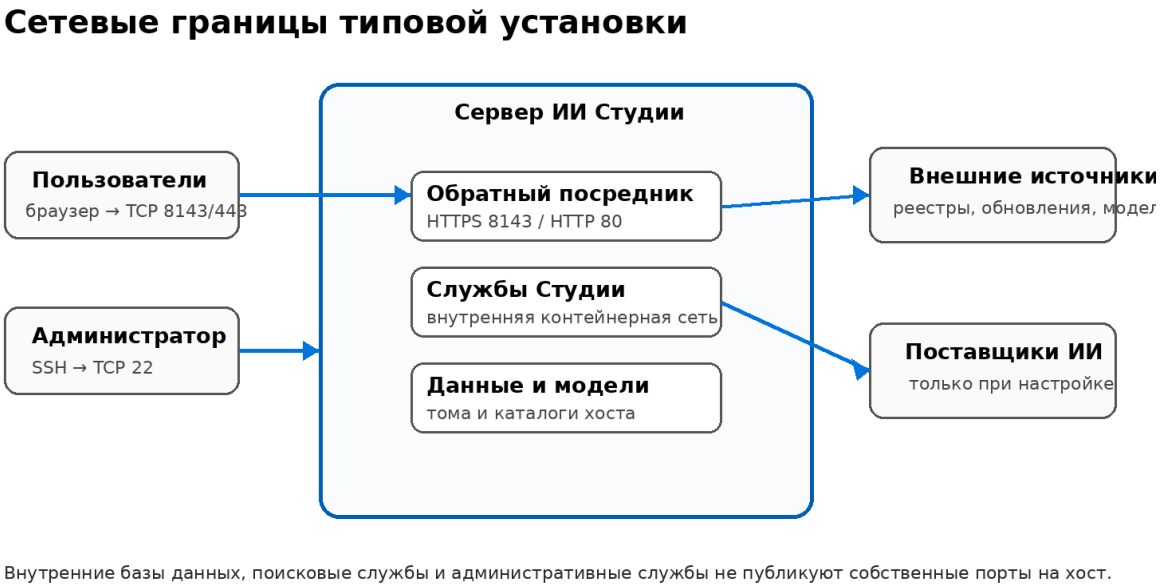


Рисунок 1 - Сетевые границы типовой установки

4.1 Постоянные данные

Постоянное состояние размещается в каталогах data/, backups/ и других каталогах поставочного дерева, определённых конфигурацией. При переносе или восстановлении нельзя ограничиваться копированием только контейнеров: контейнер является исполняемым слоем, а авторитетные данные находятся в постоянных хранилищах.

5 ПОДГОТОВКА СЕРВЕРА

До начала установки должны быть определены: имя или IP-адрес экземпляра, способ доступа пользователей, способ доступа администратора, режим локальной/внешней модели, объём хранения, схема резервного копирования и сетевые ограничения.

5.1 Базовые программные зависимости

Компонент	Назначение	Проверка
Docker Engine	Запуск контейнеров	docker version
Docker Compose	Оркестрация служб	docker compose version
Python 3	Работа установочных и проверочных сценариев	python3 --version
curl	Сетевые проверки	curl --version
iproute2 / ip	Определение сетевых адресов и маршрутов	ip -4 addr
OpenSSL	Первоначальный сертификат и проверки TLS	openssl version

5.2 Аппаратные ресурсы

Точные минимальные и рекомендуемые ресурсы задаются документом «Системные требования». Для установки базовых служб требуется сервер x86_64 с достаточным объёмом оперативной памяти и диска. Для локального вывода дополнительно требуется совместимый NVIDIA GPU. Дисковое пространство для модели рассчитывается отдельно от пространства базового комплекса.

ПРИМЕЧАНИЕ. Установщик локальной модели дополнительно проверяет свободное место с запасом: размер загружаемого артефакта × 1,15 + не менее 5 ГБ служебного резерва.

6 ПОДГОТОВКА НАЙС.ОС CLOUD

НАЙС.ОС CLOUD является основной и рекомендуемой платформой для ИИ Студии. В базовой серверной установке Docker входит в платформу. После установки ОС следует использовать модель «обычный пользователь + sudo», а удалённый вход root по SSH оставлять запрещённым.

6.1 Создание администратора ОС

```
USER="admin"
useradd -m -s /bin/bash "$USER"
passwd "$USER"
usermod -aG wheel "$USER"
```

ПРЕДУПРЕЖДЕНИЕ. Перед изменением SSH и межсетевого экрана обязательно проверьте вход под созданным пользователем через отдельный сеанс. Потеря единственного удалённого канала администрирования может потребовать консоль гипервизора или облачного провайдера.

6.2 Проверка Docker

```
systemctl is-active docker
docker version
docker info
docker compose version
```

6.3 Системное время и DNS

```
timedatectl status
resolvectl status 2>/dev/null || cat /etc/resolv.conf
getent hosts studio.ncsgp.ru
```

Расхождение времени нарушает TLS, подписи и срок действия токенов. Перед установкой необходимо обеспечить устойчивую синхронизацию времени.

6.4 Рекомендуемый каталог

```
sudo install -d -m 0750 /opt/nicesoft-ai-studio
sudo chown -R "$USER":"$USER" /opt/nicesoft-ai-studio
```

ПРИМЕЧАНИЕ. Допускается другой каталог, если обеспечены достаточное место, резервное копирование, права доступа и неизменность пути при эксплуатации.

7 СЕТЬ И МЕЖСЕТЕВОЙ ЭКРАН

По умолчанию ИИ Студия публикует HTTPS на TCP/8143. TCP/80 используется только для подтверждения домена и выпуска/продления сертификата Let's Encrypt. SSH на TCP/22 относится к операционной системе, а не к ИИ Студии.

Направление	Порт	Назначение	Обязательность
входящий	8143/tcp	Веб-интерфейс ИИ Студии по HTTPS	обязательно при стандартной схеме
входящий	80/tcp	HTTP-01 для сертификата Let's Encrypt	только при использовании Let's Encrypt
входящий	22/tcp	Администрирование ОС по SSH	по политике организации
исходящий	443/tcp	Образы, обновления, модели и настроенные внешние сервисы	по выбранному режиму

На НАЙС.ОС базовая политика межсетевого экрана ориентирована на явное разрешение требуемых соединений. Правила необходимо добавлять с учётом цепочек Docker и не очищать таблицы без анализа.

```
# пример просмотра
iptables -L -n -v --line-numbers
iptables -S

# пример разрешения стандартного порта Студии; позицию правила выберите по своей политике
iptables -I INPUT 3 -p tcp --dport 8143 -m conntrack --ctstate NEW -j ACCEPT
```

ПРИМЕЧАНИЕ. Если политика FORWARD=DROP блокирует исходящий трафик контейнеров, необходимо настроить точечные правила Docker согласно документации НАЙС.ОС. Не рекомендуется без необходимости переводить всю цепочку FORWARD в ACCEPT.

8 ПОДГОТОВКА ХРАНИЛИЩА

Для производственного экземпляра желательно использовать отдельный том или логический раздел для данных Студии, а для каталогов локальных моделей - достаточный быстрый SSD/NVMe. История мониторинга и модельные веса могут существенно увеличивать объём хранения.

Категория	Содержимое	Рекомендация
Каталог установки	Сценарии, compose.yml, конфигурация выпуска	резервировать вместе с эксплуатационной конфигурацией
data/	Базы, загрузки, состояние служб, TLS, реестр моделей	обязательное постоянное хранение
backups/	Локальные зашифрованные резервные копии	копировать хотя бы в одно внешнее хранилище
каталог моделей	Веса локальных моделей	быстрый накопитель; объём по выбранной модели
журналы	Служебная диагностика	учесть ротацию и требования ИБ

9 ПРОВЕРКА УСТАНОВОЧНОГО КОМПЛЕКТА

Перед распаковкой следует проверить источник получения, имя версии, контрольную сумму и, если поставка содержит подписанный манифест, криптографическую подпись. Контрольная сумма должна поступать по доверенному каналу.

```
sha256sum NiceSoft_AI_Studio_1.0.0.tar.gz
# сравните результат с контрольной суммой поставки
```

После распаковки рекомендуется проверить наличие основных файлов:

```
ls -la
test -x ./nicesoft.sh && echo OK
test -f ./compose.yml && echo OK
test -f ./.env.example && echo OK
test -f ./VERSION && cat ./VERSION
```

ПРЕДУПРЕЖДЕНИЕ. Не продолжайте установку, если контрольная сумма не совпадает, отсутствует манифест ожидаемой версии или состав поставки отличается от переданного правообладателем.

10 УСТАНОВКА ИЗ ПОДКЛЮЧЁННОГО КОНТУРА



Рисунок 2 - Последовательность установки

10.1 Размещение поставки

```
cd /opt/nicesoft-ai-studio
# распакуйте сюда полученный комплект версии 1.0.0
chmod 0750 nicesoft.sh
find scripts -maxdepth 1 -type f -name "*.sh" -exec chmod 0750 {} \;
```

10.2 Инициализация

```
./nicesoft.sh init
```

Команда создаёт или дополняет .env, генерирует уникальные секреты экземпляра, создаёт каталоги постоянных данных, определяет оборудование и формирует локальный TLS-комплект. На новой установке будет запрошен IP-адрес или DNS-имя, которым пользователи обращаются к Студии.

10.3 Предварительная проверка

```
./nicesoft.sh check
```

10.4 Установка

```
./nicesoft.sh install
```

Команда выполняет проверку конфигурации, подготавливает требуемые образы, запускает службы, применяет управляемые настройки и завершает работу только после штатной проверки работоспособности.

ПРИМЕЧАНИЕ. На промышленной поставке 1.0.0 предпочтительно использование заранее собранных и подписанных образов. Инженерная сборка компонентов из исходного дерева является отдельным режимом разработчика/интегратора и не должна быть обязательной процедурой на узле заказчика.

11 НАСТРОЙКА АДРЕСА ЭКЗЕМПЛЯРА

У ИИ Студии различаются внешний адрес для браузера и локальный адрес, на котором Docker публикует порты. Их нельзя механически заменять друг другом при использовании NAT.

Переменная	Назначение	Типовое значение
NICESOFT_PUBLIC_HOST	IP/DNS, которым пользуются пользователи	ai.example.ru или публичный/внутренний IPv4
NICESOFT_BIND_ADDRESS	Локальный адрес интерфейса хоста	0.0.0.0 либо конкретный локальный IPv4
NICESOFT_HTTP_PORT	Внешний HTTPS-порт Студии	8143
DOMAIN_CLIENT / DOMAIN_SERVER	Производные URL	формируются автоматически

```
./nicesoft.sh instance-setup
./nicesoft.sh instance-status
```

Для автоматизированного развёртывания:

```
python3 scripts/instance_config.py setup \
  --public-host 192.0.2.25 \
  --bind-address 0.0.0.0
```

ПРИМЕЧАНИЕ. IPv4 или DNS является проверенным вариантом установочного контракта. Использование IPv6 должно подтверждаться отдельной матрицей совместимости конкретного выпуска.

12 ПРЕДВАРИТЕЛЬНАЯ ПРОВЕРКА

Команда ./nicesoft.sh check выполняет два уровня: проверку сервера и статическую проверку проекта/конфигурации.

Проверка	Успешный результат	Действие при ошибке
docker	команда найдена, daemon доступен	запустить/исправить Docker
docker compose	подключаемый модуль доступен	установить совместимый модуль Compose
python3, curl, ip, openssl	команды доступны	установить системные зависимости
адрес экземпляра	NICESOFT_INSTANCE_CONFIGURED=true	выполнить instance-setup
bind-адрес	принадлежит хосту либо 0.0.0.0	исправить NICESOFT_BIND_ADDRESS
GPU	при наличии виден хосту и контейнерной среде	проверить драйвер/набор средств NVIDIA
vm.overcommit_memory	предпочтительно 1	при необходимости применить sysctl

```
sudo sysctl -w vm.overcommit_memory=1
# для постоянной настройки используйте отдельный файл /etc/sysctl.d по политике ОС
```

13 ЗАПУСК УСТАНОВКИ

Запуск выполняется из корневого каталога поставки. Во время первого запуска не закрывайте административный сеанс до завершения команды и не изменяйте вручную compose.yml/.env из другого сеанса.

```
./nicesoft.sh install
```

Успешная установка завершается штатной проверкой служб. При ошибке команда должна завершиться с ненулевым кодом возврата. Не следует скрывать ошибку запуском отдельных контейнеров вручную до выявления первопричины.

13.1 Наблюдение за установкой

```
./nicesoft.sh status
./nicesoft.sh logs
# либо журнал конкретной службы
./nicesoft.sh logs model-manager
```

14 ПРОВЕРКА СЛУЖБ ПОСЛЕ УСТАНОВКИ

```
./nicesoft.sh health
./nicesoft.sh status
```

Проверка охватывает контейнеры, пользовательский интерфейс, внутренние зависимости, Redis, интеграционный шлюз и иные компоненты, входящие в критерий готовности. Интеграции, которые требуют внешних учётных данных, не должны делать базовый экземпляр неисправным только из-за отсутствия этих учётных данных.

14.1 Сетевая проверка с рабочего места

```
curl -kI https://<адрес>:8143/
```

ПРИМЕЧАНИЕ. Ключ -k допустим только для первичной проверки локального самоподписанного сертификата. В промышленной эксплуатации необходимо доверие к корпоративному или публичному сертификату.

15 ПЕРВЫЙ ЗАПУСК В БРАУЗЕРЕ

Откройте https://<адрес>:8143/. При локальном сертификате браузер может сообщить об отсутствии доверия к локальному центру сертификации. Шифрование при этом присутствует, но перед эксплуатацией для пользователей следует настроить доверенный сертификат.

1. создайте или активируйте первый локальный административный аккаунт;
2. войдите повторно и убедитесь, что административные разделы доступны;
3. проверьте раздел «Параметры → Система»;
4. проверьте раздел «Модели» и состояние первого запуска;
5. не отключайте регистрацию/другие механизмы входа до подтверждения наличия как минимум одного рабочего администратора.

16 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА МОДЕЛИ

На новой установке мастер первого запуска определяет CPU, RAM, свободное место и, при наличии, GPU/VRAM. Он может предложить временную модель первоначального запуска, затем подобрать производственный артефакт и выполнить проверку перед загрузкой.

16.1 Порядок

6. Откройте «Модели → Обзор».
7. Проверьте обнаруженное оборудование.
8. Выберите рекомендованную локальную модель либо внешний/управляемый вариант.
9. Выполните предварительную проверку.
10. Запустите установку модели.
11. Дождитесь проверки готовности и назначения модели активной.
12. Создайте новый диалог и выполните контрольный запрос.

ПРИМЕЧАНИЕ. Модель первоначального запуска не является производственной рекомендацией. На сервере без поддерживаемого NVIDIA GPU локальный производственный вывод не имитируется; следует использовать внешний или управляемый источник модели.

17 УСТАНОВКА НА СЕРВЕР С ГРАФИЧЕСКИМИ УСКОРИТЕЛЯМИ

Для локального вывода моделью основной производственный профиль использует NVIDIA GPU, доступный контейнерной среде. Поддержка конкретного ускорителя определяется вычислительной возможностью, объёмом видеопамяти, числом устройств и выбранной моделью.

17.1 Проверка хоста

```
nvidia-smi
nvidia-smi -L
```

17.2 Проверка доступа из Docker

```
docker run --rm --gpus all nvidia/cuda:12.8.1-base-ubuntu24.04 nvidia-smi -L
```

17.3 Проверка профиля Студии

```
./scripts/compose.sh --print-gpu-profile
```

Результат	Смысл
gpu-production	GPU отвечает требованиям основного локального vLLM-профиля.
gpu-test	GPU может использоваться только диагностическим/временным профилем.
none	локальный GPU-профиль не выбран; используйте внешний/управляемый источник модели либо исправьте драйвер/контейнерный доступ.

ПРИМЕЧАНИЕ. Основная локальная среда выполнения требует ускоритель NVIDIA с вычислительной способностью (compute capability) 7.5 или выше. Более старые ускорители могут быть видны системе, но не считаются производственно совместимыми с основным профилем vLLM.

18 УСТАНОВКА БЕЗ ЛОКАЛЬНОГО ГРАФИЧЕСКОГО УСКОРИТЕЛЯ

Базовые функции Студии устанавливаются без GPU. В этом случае источник генеративной модели настраивается отдельно: внешний OpenAI-совместимый сервер, другой поддерживаемый поставщик через Реестр моделей либо управляемая модель Яндекса. Базы знаний, интеграции, управление пользователями и административные функции остаются локальными в соответствии с конфигурацией.

```
./nicesoft.sh model-setup
./nicesoft.sh model-status
./nicesoft.sh model-check
```

ПРИМЕЧАНИЕ. Перед подключением внешней модели согласуйте границу передачи данных. Запрос пользователя, история и извлечённый контекст могут покидать локальный контур в объёме, необходимом для выполнения запроса.

19 ДОМЕННОЕ ИМЯ И СЕРТИФИКАТ

При чистой установке создаётся локальный центр доверия и серверный сертификат длительного срока действия для локального имени. Для промышленной эксплуатации рекомендуется корпоративный сертификат или Let's Encrypt.

19.1 Let's Encrypt

13. назначьте постоянный IP-адрес;
14. создайте DNS A-запись домена на адрес экземпляра;
15. разрешите TCP/80 для HTTP-01 и пользовательский HTTPS-порт;
16. в разделе «Параметры → Сертификат и домен» укажите доменное имя и выполните проверку;
17. после успешной проверки запросите сертификат;
18. после установки сертификата повторно проверьте доступ и срок действия.

19.2 Сертификат организации

Администратор может загрузить сертификат, закрытый ключ и, при необходимости, цепочку. Перед заменой проверяются срок действия и соответствие открытого/закрытого ключа. Закрытый ключ не должен возвращаться через пользовательский интерфейс.

20 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА АДМИНИСТРАТОРА

- Проверьте, что существует минимум один активный локальный администратор.
- Используйте пароль длиной не менее требований продукта и политики организации.
- После временного пароля выполните обязательную установку постоянного пароля и повторный вход.
- Не выдавайте административную роль для повседневной пользовательской работы.
- Зафиксируйте ответственных за ОС, приложение, резервное копирование и криптографические ключи.

ПРИМЕЧАНИЕ. Операции, которые могли бы оставить экземпляр без активного администратора, должны отклоняться серверной логикой. Тем не менее перед массовыми изменениями пользователей рекомендуется проверить наличие резервного административного аккаунта по внутренней процедуре организации.

21 НАСТРОЙКИ БЕЗОПАСНОСТИ ПОСЛЕ УСТАНОВКИ

- заменить временный/локальный TLS-сертификат на доверенный, если экземпляр вводится в постоянную эксплуатацию;
- ограничить доступ к SSH по адресам/сегментам администрирования;
- не включать root-login по SSH;
- не предоставлять пользователям членство в группе docker без необходимости, поскольку оно фактически даёт административный контроль над хостом;
- закрыть все входящие порты, кроме обоснованных;
- сохранить ключ восстановления резервных копий вне сервера;
- выполнить контрольную резервную копию и тест проверки архива;
- настроить системное время, DNS и журналирование;
- проверить канал обновлений и политику выхода во внешние сети;
- зафиксировать исходное состояние в протоколе установки.

22 РАЗВЁРТЫВАНИЕ НА ВИРТУАЛЬНОЙ МАШИНЕ

Виртуальная машина является типовым вариантом. Для локальной модели с GPU требуется сквозное предоставление GPU или виртуализированный GPU, поддерживаемый драйвером и контейнерной средой. Снимок гипервизора не заменяет штатную резервную копию приложения, поскольку согласованность внутренних БД должна обеспечиваться средствами ИИ Студии.

22.1 Рекомендации

- использовать статический внутренний IP либо стабильную DNS-запись;
- не менять MAC/IP без обновления сетевой конфигурации и проверки TLS;
- для дисков с данными использовать класс хранения, допускающий требуемые IOPS;
- не полагаться только на снапшоты VM как на резервное копирование;
- при пробросе GPU в виртуальную машину проверять nvidia-smi как в основной системе, так и внутри гостевой системы и контейнера Docker.

23 РАЗВЁРТЫВАНИЕ НА ФИЗИЧЕСКОМ СЕРВЕРЕ

На физическом сервере дополнительно проверяются прошивки устройств, исправность накопителей, аппаратный мониторинг, резервирование питания и сетевых интерфейсов. Для НАЙС.ОС при необходимости можно использовать средство обнаружения требуемых прошивок.

```
sudo niceos-detect-firmware
# после установки требуемых прошивок при необходимости
sudo reboot
```

24 РАЗВЁРТЫВАНИЕ В ОБЛАКЕ

При установке в облаке публичный IP может быть реализован через NAT и не принадлежать сетевому интерфейсу VM. Поэтому NICESOFT_PUBLIC_HOST должен содержать адрес, доступный пользователю, а NICESOFT_BIND_ADDRESS - локальный адрес публикации Docker, обычно 0.0.0.0.

19. создать VM на НАЙС.ОС CLOUD или совместимой российской ОС;
20. назначить постоянный IP или DNS;
21. настроить облачную группу безопасности для 8143/443, при необходимости 80 и административного 22;
22. при использовании GPU выбрать поддерживаемую конфигурацию и проверить доступ внутри контейнера;
23. учесть плату за внешний трафик и управляемые модели;
24. создать внешнее хранилище для резервных копий.

25 УСТАНОВКА НА ДРУГИХ РОССИЙСКИХ ОС

ИИ Студия заявляется совместимой со всеми российскими серверными ОС, применимыми для данного класса программ и удовлетворяющими системным требованиям. Референсная инструкция дана для НАЙС.ОС CLOUD; различия других ОС находятся ниже уровня приложения.

Область различий	Что требуется
Пакетный менеджер	установить Python 3, curl, iproute2, OpenSSL, Docker по правилам ОС
Служба Docker	обеспечить запуск при старте и доступ администратора
Межсетевой экран	открыть требуемые порты средствами ОС/СЗИ
SELinux/МАК	разрешить требуемые монтирования, порты и контейнерную среду выполнения согласно политике ОС
Системное время	обеспечить синхронизацию
NVIDIA	установить сертифицированный/поддерживаемый драйвер и контейнерный набор средств
Файловая система	обеспечить требуемый объём, права и производительность

ПРИМЕЧАНИЕ. Подтверждение конкретной версии ОС оформляется матрицей совместимости и протоколом испытаний. Отсутствие конкретной версии в матрице означает отсутствие завершённой индивидуальной квалификации, а не автоматическую техническую несовместимость.

26 УСТАНОВКА ЧЕРЕЗ ПРОКСИ-СЕРВЕР

Если организация разрешает исходящие соединения только через прокси, контейнерный механизм загрузки образов и процесс получения локальных моделей должны быть настроены раздельно. Для Docker/BuildKit используются системные настройки Docker. Для загрузки моделей предусмотрены отдельные переменные NICESOFT_MODEL_HTTP_PROXY и NICESOFT_MODEL_HTTPS_PROXY.

```
# пример в .env (значения задаются организацией)
NICESOFT_MODEL_HTTP_PROXY=http://proxy.example:3128
NICESOFT_MODEL_HTTPS_PROXY=http://proxy.example:3128
NICESOFT_MODEL_NO_PROXY=localhost,127.0.0.1,model-manager,model-runtime,model-
runtime-test
```

ПРИМЕЧАНИЕ. Не записывайте пароль к корпоративному прокси в общедоступные журналы, снимки экрана или заявку в техническую поддержку.

27 УСТАНОВКА В ЗАКРЫТОМ КОНТУРЕ

В закрытом контуре рекомендуется использовать внутренний реестр контейнеров, внутренний источник обновлений и, при локальном выводе, внутреннее хранилище модельных артефактов. Внешние поставщики моделей и интернет-поиск отключаются или ограничиваются политикой организации.

25. перенести и проверить подписанный установочный комплект;
26. зеркалировать все контейнерные образы по неизменяемым идентификаторам;
27. перенести выбранные модельные артефакты с контрольными суммами;
28. настроить внутренний DNS/NTP;
29. указать внутренние адреса источников, если они предусмотрены поставочным профилем;
30. выполнить установку и приёмочные проверки без обращения к общедоступной сети;
31. зафиксировать фактические разрешённые направления связи.

28 ПОЛНОСТЬЮ ИЗОЛИРОВАННАЯ УСТАНОВКА

Полностью изолированная установка выполняется только из заранее подготовленного переносимого комплекта. Попытка запустить обычную сетевую загрузку образов или моделей в изолированном сегменте не должна рассматриваться как штатный способ установки.

28.1 Состав переносимого комплекта

- архив ИИ Студии 1.0.0;
- подписанный манифест и контрольные суммы;
- все контейнерные образы, используемые конкретным профилем;
- при необходимости - образ GPU-проверки;
- локальные модельные артефакты, если выбран локальный режим;
- перечень лицензий и SBOM;
- копия документации;
- протокол формирования переносимого носителя.

28.2 Порядок импорта

```
# пример импорта предварительно сохранённого OCI/Docker-образа
docker load -i images/example-image.tar
docker image ls

# после импорта всех образов выполняется штатная настройка экземпляра и запуск
./nicesoft.sh init
./nicesoft.sh check
```

ПРЕДУПРЕЖДЕНИЕ. Конкретная команда запуска изолированного промышленного комплекта должна соответствовать сопровождающему манифесту поставки. Если стандартная команда install требует сетевой сборки/получения образов, в изолированном профиле используется подготовленный правообладателем комплект среды выполнения без обращения к внешним источникам.

29 РЕЗЕРВНАЯ КОПИЯ ПОСЛЕ УСТАНОВКИ

После завершения первоначальной настройки следует создать контрольную резервную копию и отдельно сохранить ключ восстановления. Резервная копия имеет расширение .nsbackup, а ключ восстановления не помещается внутрь архива.

```
./nicesoft.sh backup
```

ПРИМЕЧАНИЕ. Хранение единственной резервной копии в каталоге backups/ на том же диске не защищает от потери VM или накопителя. Минимум одна актуальная копия и ключ восстановления должны храниться вне сервера.

30 ПРИЁМОЧНАЯ ПРОВЕРКА

Установка считается технически завершённой после выполнения минимального набора проверок.

Область	Критерий
Службы	./nicesoft.sh health завершается успешно
Веб-доступ	страница входа открывается по утверждённому HTTPS-адресу
Администратор	вход под административной учётной записью успешен
Модель	контрольный запрос возвращает ответ выбранной модели
Файлы/RAG	тестовый документ загружается и доступен для поиска, если функция включена
Система	административная страница показывает состояние служб
TLS	сертификат соответствует выбранному режиму
Резервирование	создана и проверена резервная копия, ключ сохранён отдельно
Журналы	нет необъяснённых циклических перезапусков и критических ошибок
Сеть	не опубликованы внутренние служебные порты

31 ПОВТОРНАЯ УСТАНОВКА И ВОССТАНОВЛЕНИЕ

При полной потере сервера нельзя восстанавливать только пользовательские базы поверх произвольно созданного нового .env: часть данных связана с секретами конкретного экземпляра. Сначала восстанавливается конфигурация развёртывания, затем данные.

```
./nicesoft.sh recovery-config /путь/к/backup.nsbackup /путь/к/recovery-config.tar.gz
# после подготовки среды и ключа восстановления
./nicesoft.sh restore /путь/к/backup.nsbackup
```

Перед восстановлением на новый сервер должны быть установлены совместимая ОС и контейнерная среда, а ключ NICESOFT_BACKUP_ENCRYPTION_KEY должен соответствовать архиву.

32 УДАЛЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

Удаление выполняется только после решения владельца данных. Остановка контейнеров сама по себе не удаляет постоянные данные. Перед удалением необходимо создать последнюю резервную копию либо документированно подтвердить, что сохранение не требуется.

```
cd /opt/nicesoft-ai-studio
./nicesoft.sh down
```

- сохранить необходимые .nsbackup и ключ восстановления;
- при необходимости сохранить журналы и протоколы аудита в соответствии с политикой организации;
- удалить контейнеры/образы согласно политике освобождения ресурсов;
- безвозвратно удалить каталоги data/ и backups/ только после санкционирования;
- удалить DNS-записи, правила публикации и сертификаты, относящиеся к выведенному экземпляру;
- зафиксировать вывод из эксплуатации актом/записью.

ПРЕДУПРЕЖДЕНИЕ. Команда down не должна восприниматься как команда уничтожения данных. Удаление постоянных каталогов выполняется отдельным осознанным действием.

33 ТИПОВЫЕ ОШИБКИ ПРИ УСТАНОВКЕ

Сообщение/симптом	Вероятная причина	Действие
missing: docker	Docker отсутствует в PATH	На НАЙС.ОС проверить штатный Docker; на другой ОС установить поддерживаемый Docker Engine.
Docker daemon not reachable	служба не запущена или нет прав	systemctl status docker; проверить права/использовать sudo.
docker compose unavailable	нет подключаемого модуля Compose	установить поддерживаемый Docker Compose plugin.
instance address is not configured	не задан внешний IP/DNS	./nicesoft.sh instance-setup.
host does not own Docker bind address	в bind указан NAT/публичный IP, которого нет на интерфейсе	оставить публичный адрес в NICESOFT_PUBLIC_HOST, bind заменить на 0.0.0.0/локальный IP.
GPU visible on host, Docker probe failed	не настроен NVIDIA Container Toolkit/CDI	проверить docker run --gpus all и конфигурацию NVIDIA.
контейнеры без доступа в Интернет	FORWARD=DROP блокирует docker bridge	настроить точечные FORWARD-правила по документации НАЙС.ОС.
браузер не доверяет сертификату	используется локальный CA	временно добавить доверие либо настроить корпоративный/публичный сертификат.
модель не загружается	недостаточно места/VRAM или недоступен источник	выполнить предварительную проверку модели, проверить диск, GPU и сетевой доступ.
health не проходит	одна или несколько служб не готовы	./nicesoft.sh status и ./nicesoft.sh logs <service>.

34 СООБЩЕНИЯ УСТАНОВОЧНЫХ СРЕДСТВ

Префикс	Значение	Реакция
[OK]	проверка выполнена успешно	дополнительное действие не требуется
[INFO]	информационное состояние	учесть при выборе режима
[WARN]	установка может продолжаться, но есть риск/ограничение	оценить и устранить до промышленного ввода
[FAIL] / ERROR	условие установки не выполнено	устранить причину; не считать установку завершённой

Код возврата команды также является частью результата. Автоматизированная установка должна проверять ненулевой код завершения, а не только текст вывода.

35 ТРЕБОВАНИЯ К ПРОТОКОЛИРОВАНИЮ УСТАНОВКИ

- дата и время установки;
- идентификатор поставки и контрольная сумма;
- ОС и её версия;
- аппаратная/виртуальная конфигурация;
- IP/DNS экземпляра и опубликованные порты;
- результаты ./nicesoft.sh check и ./nicesoft.sh health;
- выбранный режим модели;
- тип сертификата;
- факт создания резервной копии и место хранения ключа без раскрытия самого ключа;
- отклонения от типового порядка и согласование этих отклонений;
- ФИО/роль ответственного специалиста либо идентификатор автоматизированного конвейера.

36 НОРМАТИВНЫЕ И СПРАВОЧНЫЕ СВЕДЕНИЯ

Источник	Применение
ГОСТ 19.101-2024	Виды программ и программных документов.
ГОСТ 19.503-79	Содержание руководства системного программиста.
Официальный сайт ИИ Студии	https://studio.ncsgp.ru
Официальный сайт НАЙС.ОС	https://niceos.ru
Документация НАЙС.ОС	https://niceos.ru/docs
Реестр российского ПО: НАЙС.ОС CLOUD	https://reestr.digital.gov.ru/reestr/4119206/
Реестровая запись НАЙС.ОС CLOUD	№30128 от 22.10.2025

При противоречии между общим примером настоящего руководства и подписанным манифестом конкретной поставки приоритет имеет манифест и сопровождающее извещение правообладателя, если оно не ухудшает обязательные требования договора и нормативных документов.

ПРИЛОЖЕНИЕ А. МАТРИЦА СЕТЕВЫХ ПОРТОВ

Порт	Протокол	Направление	Компонент	Назначение	Публикация
8143	TCP/HTTPS	входящий	proxy	основной веб-доступ	да, по умолчанию
80	TCP/HTTP	входящий	proxy/ACME	только /.well-known/acme-challenge/	при необходимости
22	TCP/SSH	входящий	ОС	администрирование хоста	по политике
443	TCP/HTTPS	исходящий	разные	обновления, образы, внешние модели/интеграции	по режиму
внутренние	TCP	внутри Docker	БД, RAG, Redis, мониторинг и др.	межслужебное взаимодействие	нет

ПРИЛОЖЕНИЕ Б. КОНТРОЛЬНЫЙ ЛИСТ ПОДГОТОВКИ СЕРВЕРА

☐ Выбрана поддерживаемая российская серверная ОС.

☐ Для референсного внедрения установлена НАЙС.ОС CLOUD.

☐ Создан обычный административный пользователь ОС.

☐ SSH под root запрещён.

☐ Docker Engine работает.

☐ Docker Compose доступен.

☐ Синхронизация времени работает.

☐ DNS разрешает необходимые имена.

☐ Подготовлен постоянный диск/каталог для данных.

☐ Определён IP/DNS экземпляра.

☐ Открыты только необходимые входящие порты.

☐ Для GPU-сервера nvidia-smi работает.

☐ Для GPU-сервера контейнер Docker видит GPU.

☐ Определён способ получения образов/моделей.

☐ Подготовлено внешнее хранилище резервных копий.

ПРИЛОЖЕНИЕ В. КОНТРОЛЬНЫЙ ЛИСТ УСТАНОВКИ

☐ Получена поставка версии 1.0.0.

☐ Проверена контрольная сумма.

☐ Проверен манифест/подпись.

☐ Поставка размещена в утверждённом каталоге.

☐ Выполнен ./nicesoft.sh init.

☐ Настроен адрес экземпляра.

☐ Выполнен ./nicesoft.sh check без ошибок FAIL.

☐ Выполнена установка.

☐ ./nicesoft.sh health успешен.

☐ Веб-интерфейс доступен.

☐ Проверен административный вход.

☐ Настроена модель.

☐ Выполнен тестовый запрос.

☐ Настроен доверенный TLS для промышленной эксплуатации.

☐ Создана первая резервная копия.

☐ Ключ восстановления сохранён отдельно.

☐ Заполнен протокол установки.

ПРИЛОЖЕНИЕ Г. КОМАНДЫ ПРОВЕРКИ

```
# ОС и сеть
uname -a
ip -4 addr
ip route
timedatectl status

# Docker
systemctl is-active docker
docker version
docker compose version
docker info

# ИИ Студия
./nicesoft.sh instance-status
./nicesoft.sh check
./nicesoft.sh status
./nicesoft.sh health

# GPU
nvidia-smi -L
./scripts/compose.sh --print-gpu-profile

# журналы
./nicesoft.sh logs <служба>
```

ПРИЛОЖЕНИЕ Д. ШАБЛОН ПРОТОКОЛА УСТАНОВКИ

Поле	Значение
Организация заказчика	
Площадка / контур	
Дата установки	
Версия ИИ Студии	1.0.0
Контрольная сумма поставки	
Операционная система	
Реестровая запись ОС	
Адрес экземпляра	
Порт HTTPS	
Конфигурация CPU/RAM	
GPU / VRAM	
Тип модели	локальная / внешняя / управляемая
Сертификат	локальный / корпоративный / Let's Encrypt
Результат ./nicesoft.sh check	
Результат ./nicesoft.sh health	
Резервная копия создана	да / нет
Ключ восстановления вынесен	да / нет
Отклонения	
Ответственный специалист	

ПРИЛОЖЕНИЕ Е. КОНТРОЛЬНЫЙ ЛИСТ ИЗОЛИРОВАННОЙ ПОСТАВКИ

☐ В составе есть архив продукта 1.0.0.

☐ Есть подписанный манифест и контрольные суммы.

☐ Есть все контейнерные образы требуемого профиля.

☐ Образы идентифицированы неизменяемыми digest.

☐ Есть выбранные локальные модели и их контрольные суммы.

☐ Есть SBOM и сведения о лицензиях.

☐ Носитель учтён и проверен на вредоносный код по процедуре организации.

☐ Внутренние DNS/NTP доступны.

☐ Установка не требует обращения в Интернет.

☐ Проверка работоспособности командой ./nicesoft.sh health выполняется полностью внутри контура.

☐ Внешние интеграции отключены либо направлены на разрешённые внутренние адреса.

ПРИЛОЖЕНИЕ Ж. ПРОФИЛИ ЛОКАЛЬНЫХ МОДЕЛЕЙ И GPU

Перечень ниже является ориентиром выбора установочного профиля. Окончательное решение принимает мастер моделей по фактически обнаруженному оборудованию и зафиксированному каталогу 1.0.0.

Пример класса оборудования	Пример назначения	Особенность
NVIDIA T4 16 ГБ	компактная универсальная/кодовая модель	пограничный класс; требуется оптимизированный артефакт
NVIDIA A100 80 ГБ	универсальная модель среднего/крупного класса	достаточный резерв для производственного вывода
2×A100 и выше	длинный контекст/более крупные модели	может применяться параллелизм по нескольким GPU
GPU с вычислительной способностью (compute capability) ниже 7.5	диагностика/временный профиль	не является основным производственным vLLM-профилем
без GPU	внешняя/управляемая модель	локальный производственный вывод не используется

ПРИЛОЖЕНИЕ И. КРИТЕРИИ ГОТОВНОСТИ К ВВОДУ В ЭКСПЛУАТАЦИЮ

Область	Критерий
Установка	поставка идентифицирована; ./nicesoft.sh check и ./nicesoft.sh health выполнены успешно
Сеть	доступен утверждённый HTTPS-адрес; лишние порты не опубликованы
Учётные записи	есть рабочий администратор; временные пароли заменены
TLS	для постоянной эксплуатации настроен доверенный сертификат
Модель	активный источник модели определён и тестовый запрос успешен
Данные	каталоги постоянного состояния находятся на утверждённом хранилище
Резервирование	создана резервная копия; ключ хранится отдельно
Мониторинг	системная страница отображает состояние служб
Документация	протокол установки заполнен и сохранён
Безопасность	сетевые и административные ограничения соответствуют политике организации

После выполнения всех критериев экземпляр может быть передан администратору системы для дальнейшей настройки пользователей, интеграций, политик доступа и эксплуатационных регламентов.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов	Основание	Дата	Подпись