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

ПРОГРАММНЫЙ КОМПЛЕКС
«НАЙС СОФТ ИИ СТУДИЯ»
версия 1.0.0

РУКОВОДСТВО СИСТЕМНОГО ПРОГРАММИСТА
РУКОВОДСТВО АДМИНИСТРАТОРА

НССГ.10001-01 32 01-ЛУ
Лист утверждения

Красногорск
2026

Утвержден НССГ.10001-01 32 01-ЛУ



ООО «НАЙС СОФТ ГРУПП»

ПРОГРАММНЫЙ КОМПЛЕКС «НАЙС СОФТ ИИ СТУДИЯ» Версия 1.0.0

Руководство системного программиста
Руководство администратора
НССГ.10001-01 32 01
Листов 57

Красногорск
2026

АННОТАЦИЯ

Настоящий документ содержит сведения, необходимые для установки эксплуатационных настроек, проверки, администрирования, сопровождения, диагностики и восстановления программного комплекса «Найс Софт ИИ Студия» версии 1.0.0. Документ предназначен для системных администраторов, инженеров эксплуатации, специалистов информационной безопасности и иных работников, которым предоставлены административные полномочия в ИИ Студии.

По назначению документ соответствует виду «Руководство системного программиста» по ГОСТ 19.101-2024 и построен с учётом структуры ГОСТ 19.503-79. Наименование «Руководство администратора» используется как понятное эксплуатационное наименование для корпоративного применения.

В документе преимущественно используется русская терминология. Англоязычные обозначения сохранены только для собственных имён программных компонентов, международных протоколов, форматов, команд, путей, переменных среды и иных идентификаторов, перевод которых сделал бы инструкцию неточной.

Референсной операционной системой является НАЙС.ОС CLOUD. Описанные административные действия применимы к поддерживаемым российским серверным операционным системам при выполнении системных требований и наличии совместимой контейнерной среды.

> **Внимание.** Администратор не должен изменять постоянные данные приложения напрямую в базах данных, вручную редактировать зашифрованные хранилища учётных данных либо удалять постоянные тома контейнеров. Для штатных операций используются административный интерфейс и предусмотренные команды управления.

СОДЕРЖАНИЕ

1 Общие сведения....6
2 Структура программного комплекса....8
3 Подготовка к администрированию....10
4 Первоначальная настройка экземпляра....11
5 Административный интерфейс и области управления....13
6 Управление пользователями....14
7 Группы, роли и права доступа....15
8 Управление моделями: общие принципы....16
9 Управление локальными моделями....17
10 Подключение внешних поставщиков моделей....18
11 Управление текущей моделью и параметрами....20
12 Проверка возможностей моделей....22
13 Модели Яндекса....23
14 Корпоративные знания и поиск....24
15 Управление интеграциями....25
16 Настройка отдельных интеграций....26
17 Учётные данные и изоляция подключений....27
18 Управление автоматизациями....28
19 Состояние системы и мониторинг....29
20 Сертификат, доменное имя и защищённое соединение....30
21 Резервное копирование....31
22 Восстановление....33
23 Управление обновлениями....34
24 Политика информационной безопасности администратора....36
25 Локальный и изолированный режимы....37
26 Журналы и диагностика....38
27 Командная строка аварийного администрирования....39
28 Регламентное обслуживание....40
29 Действия при отказах и инцидентах....41
30 Аварийное восстановление после потери сервера....42
31 Вывод экземпляра из эксплуатации....43
32 Сообщения администратору и типовые ошибки....44
33 Проверка программного комплекса....45
34 Дополнительные возможности администратора....46
35 Нормативные и справочные сведения....47
Приложение А. Контрольный лист первоначального ввода в эксплуатацию....48
Приложение Б. Регламент ежедневного, еженедельного и ежемесячного обслуживания 49
Приложение В. Справочник команд управления....50

Приложение Г. Матрица административных операций и подтверждений.....51
Приложение Д. Матрица настройки интеграций.....52
Приложение Е. Сценарии резервного копирования и восстановления.....53
Приложение Ж. Диагностика моделей и графических ускорителей.....54
Приложение И. Контрольный лист информационной безопасности.....55
Приложение К. Критерии эксплуатационной приёмки.....56

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение руководства

Руководство определяет штатные действия администратора при вводе ИИ Студии в эксплуатацию, настройке пользователей и моделей, подключении корпоративных систем, наблюдении за состоянием служб, создании резервных копий, обновлении, диагностике и восстановлении. Руководство не заменяет документ «Руководство по установке»: действия до первого успешного запуска будут подробно закреплены в отдельном документе комплекта.

1.2 Идентификация продукта

Параметр	Значение
Наименование	Программный комплекс «Найс Софт ИИ Студия»
Версия	1.0.0
Правообладатель	ООО «НАЙС СОФТ ГРУПП»
Официальный адрес продукта	https://studio.ncsgp.ru
Референсная операционная система	НАЙС.ОС CLOUD
Основной способ эксплуатации	Серверное размещение с доступом пользователей через веб-интерфейс
Назначение административного документа	Настройка, проверка, обеспечение функционирования и сопровождение программного комплекса

1.3 Требования к квалификации администратора

- понимание принципов администрирования Linux и контейнерных приложений;
- умение работать с командной строкой и журналами служб;
- понимание DNS, TLS, сетевой маршрутизации и межсетевого экранирования;
- для локальных моделей - базовое понимание графических ускорителей NVIDIA, видеопамяти и драйверов;
- для интеграций - понимание принципов учётных данных, прав доступа и минимально необходимых полномочий;
- для промышленной эксплуатации - знание внутренних регламентов резервного копирования, ИБ и управления изменениями организации.

1.4 Роли и границы ответственности

Администратор ИИ Студии управляет конфигурацией программного комплекса, но не должен подменять собой администратора внешних систем. Например, выдача прав в Jira, GitLab, Яндекс Облаке или почтовой системе выполняется средствами соответствующей системы, после чего необходимые учётные данные подключаются к ИИ Студии.

Примечание. Для критичных изменений рекомендуется правило двух лиц: один администратор подготавливает изменение, второй проверяет резервную копию, область воздействия и план возврата к предыдущему состоянию.

2 СТРУКТУРА ПРОГРАММНОГО КОМПЛЕКСА

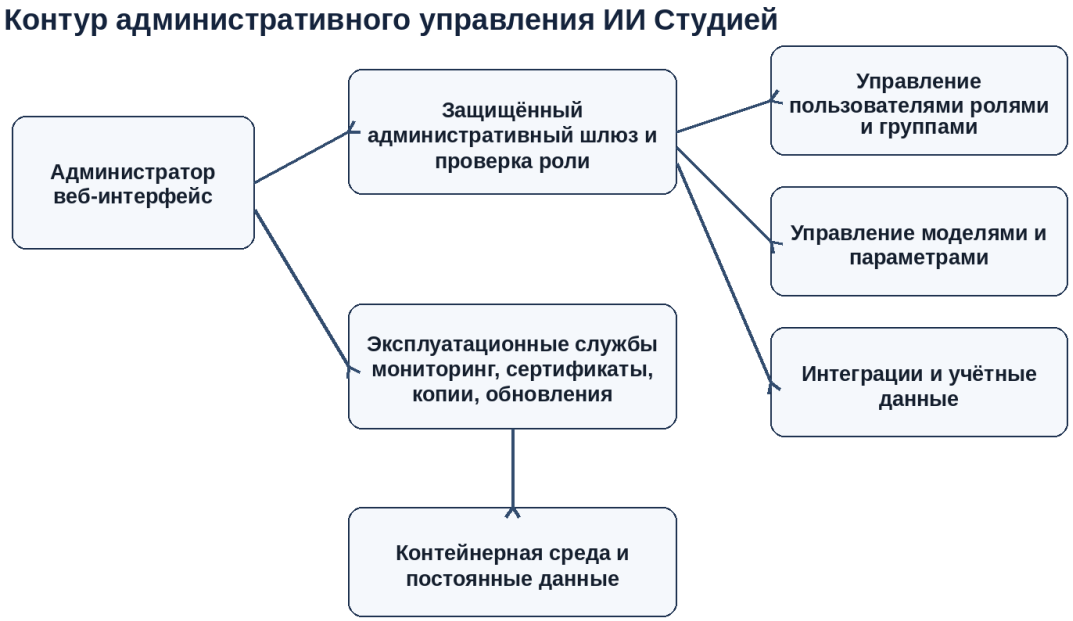


Рисунок 1 - Контур административного управления ИИ Студией

2.1 Основные подсистемы

Подсистема	Административное назначение
Обратный прокси-сервер	Завершение TLS, маршрутизация запросов и защита внешней границы.
Основной интерфейс	Работа пользователей и административные разделы продукта.
Центр управления пользователями	Создание и сопровождение локальных учётных записей, групп, ролей и жизненного цикла доступа.
Реестр моделей и маршрутизатор	Учёт поставщиков и моделей, выбор активной модели, проверка возможностей и маршрутизация запросов.
Среда локальных моделей	Запуск локальных моделей, управление графическими ускорителями, контекстом и памятью.
Шлюз интеграций	Подключение внешних систем, разрешения, аудит и безопасное получение учётных данных.
Подсистема автоматизаций	Исполнение расписаний и событийных процессов в изолированной среде.
Корпоративные знания	Загрузка документов, векторный поиск и извлечение контекста.

Подсистема	Административное назначение
Мониторинг	Сбор показателей состояния сервера и внутренних служб.
Служба сертификатов	Локальный сертификат, собственный сертификат организации и получение сертификатов Let’s Encrypt.
Служба резервного копирования	Создание, проверка, хранение и восстановление зашифрованных копий.
Служба обновления	Проверка подписанных выпусков, подготовка, установка и откат.

2.2 Службы контейнерной среды

Типовая поставка включает отдельные службы пользовательского интерфейса, административной панели, управления идентификацией, баз данных, поиска, векторного хранилища, мониторинга, сертификатов, резервного копирования, обновления, управления моделями, интеграций и автоматизаций. Администратор не обязан управлять каждой службой вручную: штатным способом является общий сценарий управления `nicesoft.sh`.

```
./nicesoft.sh status
./nicesoft.sh health
./nicesoft.sh logs <имя_службы>
```

Внимание. Не используйте команду `docker compose down -v` в штатной эксплуатации. Ключ `-v` удаляет постоянные тома и способен привести к потере данных.

3 ПОДГОТОВКА К АДМИНИСТРИРОВАНИЮ

3.1 Доступ к экземпляру

Администрирование выполняется через защищённый веб-интерфейс. В промышленной эксплуатации рекомендуется использовать собственное доменное имя организации и доверенный сертификат. Для временной первичной настройки допускается локальный сертификат, созданный установщиком.

3.2 Административная учётная запись

Операции, влияющие на пользователей, модели, подключения, сертификаты, резервные копии и обновления, дополнительно проверяют административную роль на сервере. Скрытие элемента интерфейса не рассматривается как средство защиты. Даже при прямом обращении к внутреннему маршруту операция должна быть отклонена без роли администратора.

> **Внимание.** Никогда не блокируйте и не удаляйте последнего действующего администратора. ИИ Студия содержит серверную защиту от такого действия, однако эксплуатационный регламент также должен предусматривать не менее двух административных учётных записей для промышленной системы.

3.3 Перед любым существенным изменением

1. Проверить состояние системы в разделе «Параметры → Система».
2. Убедиться, что нет активного восстановления, обновления или изменения среды выполнения модели.
3. Создать актуальную резервную копию перед изменениями, способными затронуть постоянные данные.
4. Проверить наличие свободного места и отсутствие критических предупреждений.
5. Зафиксировать текущую конфигурацию и ожидаемый результат изменения.
6. После изменения выполнить контроль работоспособности и функциональную проверку.

4 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА ЭКЗЕМПЛЯРА

Последовательность первоначальной настройки



Все изменяющие операции выполняются сервером. Одновременно допускается только одна операция первоначальнс

Рисунок 2 - Основные этапы первоначальной настройки

4.1 Общий принцип

На новой установке первоначальная настройка является серверным процессом. Состояние хранится на стороне ИИ Студии, поэтому смена браузера, очистка файлов cookie или вход с другого рабочего места не сбрасывают этапы. Одновременно допускается только одна операция, изменяющая состояние первоначальной настройки; другие администраторы могут наблюдать ход выполнения.

4.2 Проверка аппаратных ресурсов

Мастер получает фактические сведения о графических ускорителях, доступной видеопамяти, количестве процессорных ядер, оперативной памяти и свободном месте. Рекомендация основной модели должна основываться на фактических ресурсах, а не только на названии облачного профиля виртуальной машины.

4.3 Временная локальная модель

Для первоначального ввода в работу может применяться небольшая временная локальная модель «NiceSoft Bootstrap · Qwen3 0.6B». Она предназначена для базовой работоспособности на этапе загрузки основной модели и не должна рассматриваться как рекомендуемая промышленная модель для продуктивной эксплуатации.

4.4 Выбор и установка основной модели

7. Откройте раздел «Модели».
8. Проверьте аппаратный отчёт и рекомендации.
9. Выберите рекомендуемую либо иную совместимую модель.
10. Запустите предварительную проверку доступности ресурсов и источника модели.
11. Начните установку. Во время загрузки не перезапускайте сервер без необходимости.
12. Дождитесь запуска среды выполнения и подтверждения готовности модели.

13. Проверьте, что активный маршрут модели переведён в готовое состояние.
14. Завершите мастер и выполните пробный диалог.

4.5 Режим проверки мастера

На уже настроенном экземпляре администратор может запустить безопасный предварительный просмотр мастера из раздела управления моделями. Такой режим использует реальные данные оборудования и рекомендации, но не скачивает модели, не переключает активную модель и не изменяет состояние экземпляра.

5 АДМИНИСТРАТИВНЫЙ ИНТЕРФЕЙС И ОБЛАСТИ УПРАВЛЕНИЯ

Административные возможности собраны в основных разделах «Пользователи», «Модели», «Интеграции» и «Параметры». Конкретный набор пунктов зависит от роли, состояния экземпляра и подключённых возможностей.

Раздел	Основные действия администратора
Пользователи	Учётные записи, блокирование, изменение профиля, группы, роли, права.
Модели	Локальные модели, внешние поставщики, модели Яндекса, проверка возможностей, активация.
Интеграции	Подключения к корпоративным системам, права, состояние и диагностика.
Параметры → Текущая модель	Параметры запросов и, для локальной модели, параметры среды выполнения.
Параметры → Система	Состояние узла, служб, дисков, сети, ускорителей и сертификата.
Параметры → Сертификат и домен	Домен, Let’s Encrypt, загрузка сертификата организации.
Параметры → Резервное копирование	Создание, проверка, скачивание, загрузка, восстановление, расписание.
Параметры → Обновление	Канал, проверка выпуска, подготовка, установка и возврат к предыдущей версии.

6 УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

6.1 Основные принципы

Центр управления пользователями использует штатные пользовательские сущности ИИ Студии и не создаёт параллельную базу учётных записей. Состояния блокирования и отзыва сеансов контролируются дополнительным защитным слоем НАЙС СОФТ.

6.2 Создание локального пользователя

15. Откройте «Пользователи».
16. Нажмите создание пользователя.
17. Укажите адрес электронной почты и иные обязательные поля.
18. Назначьте основную роль и при необходимости группы.
19. Задайте первоначальный пароль согласно политике сложности.
20. Сохраните пользователя и убедитесь, что запись появилась в перечне.
21. Передайте пользователю порядок первого входа безопасным каналом.

6.3 Изменение профиля и роли

Изменение основной роли выполняется отдельной административной операцией и приводит к отзыву прежних сеансов. Это предотвращает сохранение старых полномочий в уже выданных сеансах. Системные роли пользователя и администратора защищены от переименования и удаления.

6.4 Блокирование и разблокирование

Блокирование предназначено для временного прекращения доступа без удаления пользовательских данных. После блокирования уже выданные сеансы также перестают предоставлять доступ. Причина блокирования должна фиксироваться в эксплуатационном журнале организации.

6.5 Удаление пользователя

Удаление является разрушительной операцией и выполняется штатным каскадом удаления связанных пользовательских данных. Перед удалением необходимо проверить требования организации к хранению переписки, файлов и аудита. Самоудаление администратора и удаление последнего активного администратора запрещены серверными правилами.

6.6 Сброс пароля

Основной способ - административная операция управления пользователем. Если веб-интерфейс недоступен, допускается безопасный консольный путь, который не пересоздаёт экземпляр и не выполняет операций с постоянными томами.

```
./nicesoft.sh user-password-reset user@example.ru
```

Внимание. Не используйте `init`, `rebuild`, удаление томов или ручное редактирование базы данных как способ сброса пароля. Консольная команда проверяет наличие существующей базы и пользователя и при несоответствии завершается без изменения данных.

7 ГРУППЫ, РОЛИ И ПРАВА ДОСТУПА

7.1 Модель прав

Пользователь имеет одну основную роль и может входить в несколько групп. Группы используются для коллективного назначения политик и доступов к интеграциям. Пользовательские роли позволяют сформировать необходимый набор разрешений, не выдавая полные административные полномочия.

7.2 Защищённые роли

Системные роли `USER` и `ADMIN` являются зарезервированными. Их нельзя удалить или переименовать. Изменение полномочий, способное уменьшить число активных администраторов, проходит серверную проверку актуального состояния непосредственно перед записью.

7.3 Рекомендуемый подход

- не выдавать роль администратора для обычной работы с ИИ;
- создавать отдельные группы по подразделениям или функциям;
- выдавать интеграционные разрешения группам, если это соответствует модели доступа организации;
- периодически пересматривать неиспользуемые роли и группы;
- после увольнения сотрудника сначала блокировать доступ и отзывать сеансы, затем выполнять предусмотренную политикой организации процедуру удаления.

8 УПРАВЛЕНИЕ МОДЕЛЯМИ: ОБЩИЕ ПРИНЦИПЫ

ИИ Студия предоставляет единый административный контур для локальных моделей, внешних поставщиков и управляемых моделей Яндекса. Пользовательский интерфейс обращается к стабильной логической активной модели, а физическая модель может быть заменена администратором без перенастройки пользовательских клиентов.

8.1 Источники моделей

Тип	Где выполняется	Что контролирует администратор
Локальная модель	На сервере или графических ускорителях экземпляра	Установка, выбор, параметры памяти, контекст, параллелизм, запуск.
Внешний поставщик	Во внешней или корпоративной системе	Адрес, протокол, шифрование, учётные данные, список моделей, активация.
Управляемая модель Яндекса	В Яндекс Облаке	Область, модель, разрешения, доступ и политика передачи данных.

8.2 Принцип безопасного переключения

Активная физическая модель должна пройти проверку доступности перед тем, как начать обслуживать пользовательские запросы. Для локальной модели изменение параметров среды выполнения выполняется транзакционно: новая конфигурация сначала запускается как кандидат, проходит проверку готовности и только после этого становится действующей.

9 УПРАВЛЕНИЕ ЛОКАЛЬНЫМИ МОДЕЛЯМИ

9.1 Аппаратный отчёт

Раздел локальных моделей показывает обнаруженные графические ускорители, видеопамять, вычислительные возможности, процессор, оперативную память и свободное место. При изменении оборудования или драйверов рекомендуется обновить аппаратный отчёт до установки или перенастройки модели.

9.2 Установка модели

22. Откройте «Модели → Каталог».
23. Выберите модель, подходящую под объём видеопамяти и назначение.
24. Запустите предварительную проверку.
25. Проверьте оценку объёма загрузки и свободного места.
26. Запустите установку и дождитесь подтверждения целостности артефактов.
27. Активируйте установленную модель.
28. Выполните тестовый запрос и проверьте состояние среды выполнения.

9.3 Удаление модели

Удаление выполняется из каталога моделей. Если удаляется активная модель, среда выполнения останавливается, выбор очищается, после чего система по возможности выбирает другую уже установленную локальную модель. Если подходящей локальной модели нет, может использоваться заранее настроенный внешний поставщик.

> **Внимание.** Нельзя удалять модель во время незавершённой загрузки. Дождитесь окончания установки или корректного завершения операции.

9.4 Диагностика

```
./nicesoft.sh logs model-manager
./nicesoft.sh logs model-runtime
./nicesoft.sh logs model-runtime-test
```

10 ПОДКЛЮЧЕНИЕ ВНЕШНИХ ПОСТАВЩИКОВ МОДЕЛЕЙ

10.1 Создание подключения

29. Откройте «Модели → Управление моделями → Внешние модели».
30. Создайте поставщика моделей.
31. Укажите понятное административное наименование.
32. Выберите протокол и базовый адрес программного интерфейса.
33. Выберите сетевую политику: публичный адрес или явно разрешённая частная сеть.
34. Настройте способ аутентификации.
35. При использовании корпоративного центра сертификации загрузите его сертификат.
36. Выполните проверку соединения.
37. Запустите обнаружение моделей.
38. Зарегистрируйте нужные модели и проверьте их возможности.
39. Только после проверки назначьте нужную модель активной.

10.2 Сетевая политика

Для публичного поставщика разрешается только защищённый протокол HTTPS. Адрес должен разрешаться в глобально маршрутизируемые адреса. Локальные, петлевые, служебные и метаданные облачных платформ блокируются. Для корпоративной сети администратор может явно разрешить частные адреса, но петлевые и служебные адреса остаются запрещёнными.

10.3 Перенаправления и повторное разрешение DNS

Проверка поставщика не следует HTTP-перенаправлениям, чтобы заголовок авторизации не мог быть передан на другой узел. После разрешения доменного имени система проверяет все полученные адреса и соединяется именно с уже проверенным адресом, сохраняя исходное имя для TLS. Это снижает риск атак повторного связывания DNS.

10.4 Аутентификация

Способ	Применение
Без аутентификации	Только для явно доверенного внутреннего сервиса.
Токен Bearer	Заголовок Authorization: Bearer …
Ключ API	Заголовок X-API-Key.
Базовая аутентификация	Имя пользователя и пароль.
Произвольный заголовок	Корпоративные шлюзы; критичные транспортные заголовки запрещены.

10.5 Сертификаты поставщика

Отключение проверки TLS не предусмотрено. Допускается системное хранилище доверенных центров сертификации либо отдельный корпоративный сертификат центра сертификации. В

интерфейсе отображается только отпечаток и состояние настройки, а не содержимое закрытых данных.

11 УПРАВЛЕНИЕ ТЕКУЩЕЙ МОДЕЛЬЮ И ПАРАМЕТРАМИ

11.1 Параметры запроса

Для параметров, передаваемых с каждым запросом, используются три режима: «Автоматически» - система не подменяет значение; «По умолчанию» - административное значение применяется только при отсутствии значения в запросе; «Принудительно» - административное значение заменяет пользовательское.

11.2 Параметры локальной среды выполнения

Параметр	Назначение	Рекомендация
Доля памяти GPU	Ограничивает долю видеопамяти, используемой vLLM.	Не повышать без измерения запаса памяти; 1,0 намеренно не допускается.
Контекст модели	Ограничивает максимальную длину контекста.	Не превышать нативное значение модели и фактические возможности памяти.
Тензорный параллелизм	Распределяет модель по нескольким GPU.	Использовать автоматический режим, если нет необходимости фиксировать число GPU.
Тип и объём KV-кэша	Управляет памятью контекста.	Менять только после проверки совместимости конкретной модели и GPU.
Параллельные последовательности	Определяет одновременную обработку запросов.	Увеличивать постепенно с наблюдением за задержкой и памятью.
Кэширование префикса	Повторно использует общие начала запросов.	Включать при типовой повторяемой системной инструкции.
Конфигурация генерации	Использует настройки модели либо нейтральные настройки vLLM.	Не использовать произвольные файловые пути.

11.3 Транзакционное применение

40. Нажмите «Проверить среду выполнения».
41. Исправьте все ошибки предварительной проверки.
42. Нажмите «Применить с перезапуском».
43. Система сохранит снимок предыдущей рабочей конфигурации.
44. Будет запущена кандидатная конфигурация и выполнена проверка готовности.
45. При успехе новая конфигурация закрепляется.
46. При неудаче выполняется автоматический возврат к предыдущей конфигурации.

Внимание. Если одновременно не запускаются и новая, и предыдущая конфигурации, это аварийное состояние. Перейдите к разделу диагностики модели и не выполняйте повторные изменения параметров вслепую.

12 ПРОВЕРКА ВОЗМОЖНОСТЕЙ МОДЕЛЕЙ

Для внешних моделей ИИ Студия может выполнять быструю и полную проверку возможностей: обычный диалог, потоковая выдача, системные инструкции, вызов инструментов, параллельные вызовы, структурированный ответ, рассуждение, изображение и известные параметры генерации.

Состояние	Смысл для администратора
Подтверждено	Возможность проверена фактическим пробным запросом.
Поддерживается	Поставщик или адаптер сообщает о поддержке, но полная поведенческая проверка не выполнена.
Неизвестно	Данных недостаточно; опасные предположения не делаются.
Не поддерживается	Проверка показала отсутствие функции.
Неисправно	Функция заявлена или ожидалась, но фактическая проверка завершилась ошибкой.
Устарело	Изменилась модель, версия поставщика или отпечаток; требуется повторная проверка.

При неопределённой или неподдерживаемой функции вызова инструментов необязательные инструменты исключаются из запроса, чтобы обычный диалог мог продолжиться. Обязательная инструментальная операция должна завершаться понятной ошибкой, а не скрытым ослаблением политики.

13 МОДЕЛИ ЯНДЕКСА

Управляемые модели Яндекса подключаются через защищённый серверный шлюз. Администратор отвечает за корректный выбор облака, каталога, служебной учётной записи и минимально необходимых прав. Пользователь не должен получать закрытый ключ или токен непосредственно в браузер.

13.1 Рекомендуемая последовательность

47. Создайте служебную учётную запись в Яндекс Облаке.
48. Назначьте только необходимые роли на требуемый каталог или сервис.
49. Создайте авторизованный ключ.
50. Загрузите JSON-файл ключа через административный интерфейс ИИ Студии.
51. Выберите облако и каталог.
52. Проверьте доступ через встроенную диагностику.
53. Подключите требуемые управляемые модели.
54. Выполните пробный запрос и зафиксируйте границы передачи данных.

13.2 Диагностика

```
./nicesoft.sh yc-doctor
./nicesoft.sh yc-check
```

Диагностические команды не должны выводить закрытый ключ или токен доступа. Ошибка 403 обычно означает недостаточные права, неверный каталог либо несоответствие области действия служебной учётной записи.

14 КОРПОРАТИВНЫЕ ЗНАНИЯ И ПОИСК

14.1 База знаний

Администратор должен определить допустимые источники документов, максимальные объёмы загрузки и правила хранения. Векторное хранилище и данные поиска входят в резервную копию, однако поисковые производные индексы, которые можно воспроизвести, могут не входить в неё.

14.2 Веб-поиск

Локальный поисковый контур используется для получения поисковой выдачи и безопасного извлечения содержимого. Перед промышленным использованием проверьте сетевые правила организации, допустимые внешние направления и политику использования Интернет-источников.

```
./nicesoft.sh web-search-check
```

14.3 Контроль данных

- не включать конфиденциальные документы в общую базу знаний без соответствующей модели доступа;
- не считать ответ модели эквивалентом первичного документа;
- при использовании внешней модели учитывать, какой извлечённый контекст может быть передан внешнему поставщику;
- проверять резервное копирование загруженных файлов и векторного хранилища.

15 УПРАВЛЕНИЕ ИНТЕГРАЦИЯМИ

Интеграционный слой построен так, чтобы модель не владела учётными данными внешних систем. Модель запрашивает разрешённое действие, сервер проверяет пользователя, права и подключение, а затем интеграционный шлюз выполняет действие с принадлежащими соответствующему субъекту учётными данными.

15.1 Общий порядок подключения

55. Откройте «Интеграции».
56. Выберите нужную систему.
57. Изучите список доступных действий и требуемые полномочия.
58. Создайте или подключите учётные данные.
59. Выполните встроенную проверку соединения.
60. Назначьте права пользователю или группе.
61. Для действий с изменением данных проверьте наличие подтверждения человеком.
62. Выполните пробный запрос под обычным пользователем с минимальными правами.
63. Проверьте запись аудита.

15.2 Принцип минимальных полномочий

Учётная запись внешней системы должна иметь только те полномочия, которые нужны конкретному сценарию. Если интеграция используется только для чтения, не выдавайте права изменения. Если система позволяет отдельные токены для проектов или групп, предпочтительно разделять их по области ответственности.

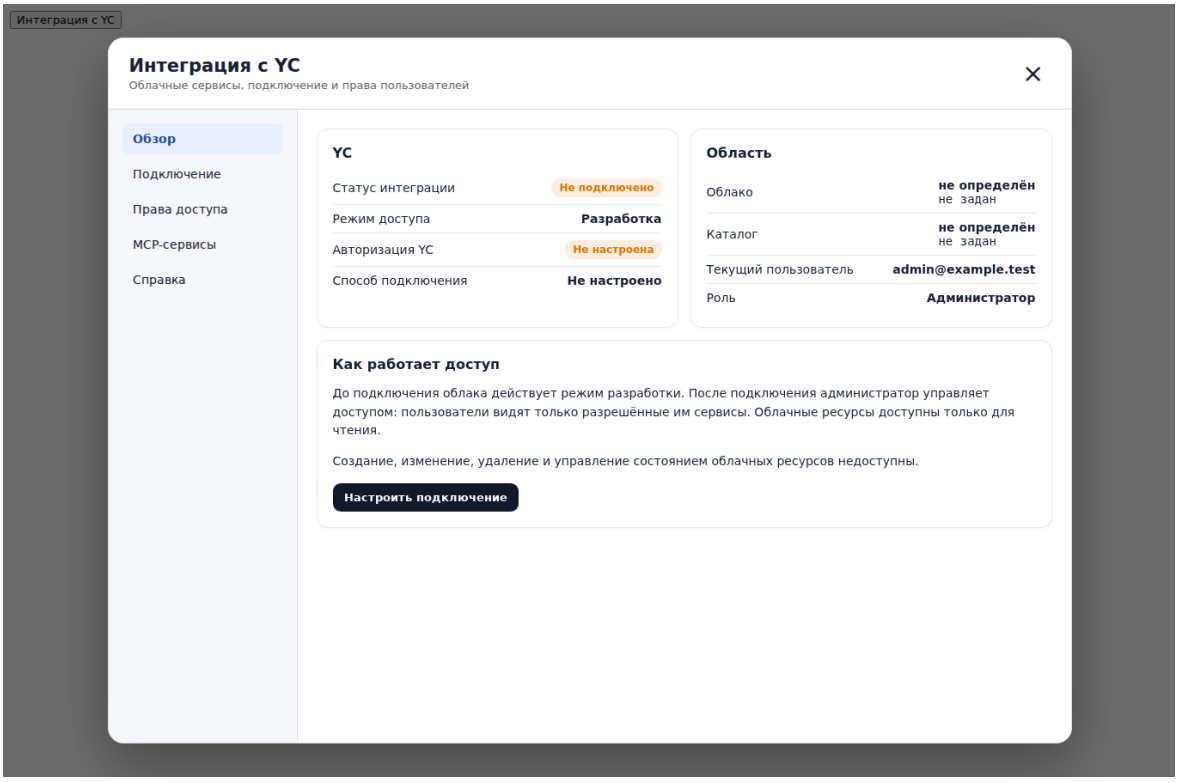


Рисунок 3 - Пример административного окна интеграции

16 НАСТРОЙКА ОТДЕЛЬНЫХ ИНТЕГРАЦИЙ

Система	Что настраивается	Административная рекомендация
Яндекс Облако	Авторизованный ключ служебной учётной записи; выбор облака и каталога.	Проверить доступ диагностикой; использовать минимальные роли. Управление инфраструктурой по умолчанию не должно разрешаться без отдельной политики.
Яндекс 360	Пользовательская авторизация в поддерживаемом режиме.	Проверить область доступа к почте/файлам и принадлежность учётных данных пользователю.
Jira	Личная или сервисная учётная запись/API-токен в зависимости от варианта Jira.	Проверить адрес, проектную область и права чтения/изменения.
Confluence	Личная или сервисная учётная запись/API-токен.	Ограничить доступ необходимыми пространствами.
GitHub	Личный токен пользователя.	Предпочитать точечные токены и минимальный доступ к репозиториям.
GitLab	Личный токен пользователя.	Ограничить группу/проекты и срок действия токена.
PostgreSQL	Отдельный пользователь БД.	Для аналитических сценариев применять только чтение; запретить изменение схемы и данных.
Электронная почта	IMAP/SMTP либо поддерживаемый способ аутентификации.	Разделять чтение и отправку, если система это позволяет; отправку считать изменяющим действием.
S3	Ключ доступа и секрет либо иной поддерживаемый способ.	Ограничить корзину и операции; не выдавать административные права хранилища.
SFTP	Пользователь/ключ.	Использовать отдельный каталог и ограниченного пользователя.
WebDAV	Учётная запись или токен.	Ограничить область и права изменения.
Telegram	Один токен бота для экземпляра и персональная привязка пользователя.	Публичный webhook не требуется; chat_id пользователь вручную не вводит.

17 УЧЁТНЫЕ ДАННЫЕ И ИЗОЛЯЦИЯ ПОДКЛЮЧЕНИЙ

Учётные данные соединений шифруются и привязываются к владельцу и профилю подключения. Серверное разрешение подключения учитывает текущего аутентифицированного пользователя. Административное право на управление политикой не должно автоматически означать право использовать чужой личный секрет.

17.1 Правила администратора

- не копировать секреты в описания автоматизаций, системные инструкции или пользовательские сообщения;
- не сохранять ключи в общедоступных файлах проекта;
- для общесистемных подключений использовать специально предназначенное хранилище прикладных учётных данных;
- для личных подключений сохранять привязку к конкретному пользователю;
- при утечке или увольнении пользователя отзывать и заменять секрет во внешней системе, затем обновлять или удалять подключение в ИИ Студии;
- проверять аудит операций ротации и отзыва.

17.2 Карантин неоднозначных старых данных

Если при миграции невозможно доказать принадлежность старого общего секрета конкретному пользователю или приложению, он не должен автоматически становиться личным подключением. Такие данные переводятся в безопасное состояние до явного решения администратора.

18 УПРАВЛЕНИЕ АВТОМАТИЗАЦИЯМИ

Автоматизация связывает событие или расписание с набором действий. Исполнение отделено от пользовательского интерфейса и не получает произвольного прямого доступа к Интернету и секретам поставщиков. Внешние действия выполняются через интеграционный шлюз с действующими разрешениями.

18.1 Типы запуска

- ручной запуск;
- расписание;
- событийный запуск от поддерживаемого внутреннего события;
- запуск из диалога по явному запросу пользователя, если это разрешено политикой.

18.2 Создание

64. Определите владельца и назначение процесса.
65. Выберите событие или расписание.
66. Добавьте действия и параметры.
67. Для каждого внешнего действия назначьте допустимое подключение и право использования.
68. Проверьте, какие действия имеют побочный эффект.
69. Для критичных действий настройте подтверждение человеком.
70. Выполните пробный запуск на тестовых данных.
71. Проверьте журнал выполнения и результат.
72. Только после проверки включите расписание в промышленном режиме.

18.3 Резервное копирование автоматизаций

Определения автоматизаций, история запусков и внутреннее состояние входят в резервную копию. Очередь временных задач не восстанавливается после возврата копии, чтобы старое незавершённое действие не могло повторно выполнить внешний побочный эффект.

19 СОСТОЯНИЕ СИСТЕМЫ И МОНИТОРИНГ

19.1 Раздел «Параметры → Система»

Администратор получает сводку по процессору, оперативной памяти, корневой файловой системе, сети, времени работы, основным внутренним службам, объёму данных, активной модели, ускорителю, сертификату и резервным копиям. Метрики собираются внутренними средствами мониторинга и не требуют публикации административных портов наружу.

19.2 История показателей

По умолчанию история показателей хранится 30 дней. Отсутствие источника метрики должно отображаться как неопределённое состояние, а не как условное нулевое значение.

19.3 Командная проверка

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

Отсутствие установленной локальной модели само по себе не должно считать всю инфраструктуру неисправной: это допустимо на новой установке до выбора модели. Если активирован локальный профиль с GPU, проверяется соответствующая среда модели.

20 СЕРТИФИКАТ, ДОМЕННОЕ ИМЯ И ЗАЩИЩЁННОЕ СОЕДИНЕНИЕ

20.1 Локальный сертификат

При чистой установке формируется локальный центр доверия и серверный сертификат длительного срока действия для локального имени экземпляра. Он обеспечивает шифрование, но не становится автоматически доверенным в браузерах рабочих мест.

20.2 Собственный домен

73. Создайте DNS-запись, ведущую на адрес экземпляра.
74. Убедитесь, что имя однозначно разрешается из пользовательской сети.
75. Откройте «Параметры → Сертификат и домен».
76. Выберите получение сертификата Let’s Encrypt либо загрузку сертификата организации.
77. При Let’s Encrypt разрешите входящий TCP/80 для проверки ACME.
78. После выпуска проверьте HTTPS и цепочку доверия с пользовательского рабочего места.

20.3 Загрузка собственного сертификата

Перед заменой проверяются срок действия и соответствие закрытого ключа сертификату. Предыдущий комплект сохраняется в служебном каталоге для возврата. Закрытый ключ не должен выдаваться обратно через веб-интерфейс.

> **Внимание.** HTTP-порт 80 в штатной конфигурации используется только для пути проверки ACME. Не публикуйте основной интерфейс ИИ Студии по незащищённому HTTP.

21 РЕЗЕРВНОЕ КОПИРОВАНИЕ



Рисунок 4 - Принцип резервного копирования

21.1 Что входит в копию

- пользователи, диалоги и состояние пользовательского слоя;
- векторное хранилище и корпоративные знания;
- загруженные файлы и изображения;
- настройки и данные интеграций, разрешений, аудита и автоматизаций;
- внутренняя база подсистемы автоматизаций;
- состояние управления моделями;
- сертификаты и состояние домена;
- навыки, расширения и важные файлы развёртывания;
- перечень локальных моделей и их объём.

21.2 Что не копируется как воспроизводимое

- сами весовые файлы локальных моделей;
- временные кэши и очереди Redis;
- воспроизводимый поисковый индекс;
- история показателей мониторинга;
- обычные журналы контейнеров.

21.3 Формат и ключ восстановления

Копия имеет расширение `.nsbackup`, шифруется алгоритмом AES-256-CTR и защищается кодом целостности HMAC-SHA256. Ключ восстановления не помещается внутрь архива. Его необходимо скачать отдельно и хранить вне сервера ИИ Студии.

21.4 Расписание

Базовая конфигурация предусматривает ежедневную копию в 03:00 и хранение семи последних копий. Администратор может изменить расписание и глубину хранения. Для промышленной системы необходимо иметь как минимум одну актуальную копию и ключ восстановления вне той же виртуальной машины или физического узла.

21.5 Действия в интерфейсе

- «Создать копию сейчас»;
- «Проверить»;
- «Скачать»;
- «Загрузить копию»;
- «Восстановить» с явным подтверждением;
- «Удалить»;
- «Скачать ключ восстановления»;
- изменение расписания и глубины хранения.

22 ВОССТАНОВЛЕНИЕ

22.1 Предварительные условия

79. Убедитесь, что выбран правильный архив и имеется соответствующий ключ восстановления.
80. Проверьте версию продукта. Копия от более новой несовместимой версии не должна восстанавливаться в старую.
81. Создайте страховочную копию текущего состояния, если экземпляр ещё работоспособен.
82. Уведомите пользователей о режиме обслуживания.
83. Проверьте свободное место.

22.2 Последовательность восстановления

Перед изменением рабочих данных проверяются код целостности, структура архива и контрольные суммы файлов. Затем включается режим обслуживания, восстанавливаются авторитетные базы и файлы, очищаются временные очереди автоматизаций, выполняются проверки баз данных и только после успеха снимается режим обслуживания.

22.3 Особенность файлов запуска

При восстановлении из работающей Студии текущие `.env`, `compose.yml` и иные файлы запуска не заменяются автоматически. Их копии хранятся внутри архива для полного аварийного восстановления. Такой подход не позволяет обычному восстановлению скрыто изменить сетевую конфигурацию или внутренние секреты работающего экземпляра.

22.4 Командный аварийный путь

```
./nicesoft.sh restore /путь/к/копии.nsbackup
./nicesoft.sh recovery-config /путь/к/копии.nsbackup
```

23 УПРАВЛЕНИЕ ОБНОВЛЕНИЯМИ



Рисунок 5 - Безопасное обновление и возврат

23.1 Каналы

Отображаемое название	Идентификатор	Назначение
Стабильный	stable	Рекомендуемый промышленный канал.
Кандидат	candidate	Предварительно проверенный выпуск перед переводом в стабильный канал.
Разработка	development	Частые инженерные сборки для испытаний и разработки.

23.2 Проверка готовности

Перед установкой служба обновления проверяет подписи и политику выпуска, архитектуру узла, свободное место, контейнерную среду и готовность службы резервного копирования. Подготовка загружает необходимые артефакты по неизменяемым контрольным суммам, не изменяя текущую версию.

23.3 Установка

84. Проверить доступный выпуск и журнал изменений.
85. Выполнить «Проверить готовность».
86. Нажать «Скачать и подготовить».
87. После успешной подготовки создать или подтвердить актуальную резервную копию.
88. Запустить обновление.

89. Дождаться режима обслуживания, запуска новой версии и проверки работоспособности.
90. Проверить основные пользовательские функции и интеграции.

23.4 Откат

Если новый выпуск не проходит контроль работоспособности, применяется предусмотренный договором миграции механизм возврата. Для совместимых выпусков возвращается предыдущая среда выполнения; для изменений, требующих восстановления данных, используется предварительно созданная копия.

> **Внимание.** Не переписывайте опубликованный стабильный выпуск тем же номером. Исправление должно иметь новый номер версии. Для клиентского экземпляра следует использовать только подписанные опубликованные выпуски.

24 ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АДМИНИСТРАТОРА

24.1 Обязательные правила

- использовать отдельные административные учётные записи;
- не передавать административные пароли и ключи в диалог с моделью;
- использовать многофакторную защиту во внешних системах, если она поддерживается;
- выдавать минимально необходимые права;
- не отключать проверку TLS для удобства;
- хранить ключ восстановления резервных копий отдельно;
- ограничить доступ к серверу ИИ Студии и файлам `.env`;
- регулярно обновлять продукт через подписанный механизм;
- контролировать аудит административных операций;
- проводить отзыв учётных данных при увольнении или компрометации;
- не публиковать внутренние административные порты во внешнюю сеть.

24.2 Административный аудит

В журнале должны различаться создание и изменение поставщика модели, проверка соединения, ротация ключа, изменение сертификата, применение параметров модели, откат, операции с пользователями и иные существенные административные действия. Секреты, тексты пользовательских запросов и ответы модели не должны попадать в журнал только ради фиксации административного события.

25 ЛОКАЛЬНЫЙ И ИЗОЛИРОВАННЫЙ РЕЖИМЫ

25.1 Локальная обработка

В локальном режиме модели и корпоративные знания могут обрабатываться внутри инфраструктуры организации. Администратор обязан понимать, что подключение внешней интеграции или внешнего поставщика модели создаёт отдельную границу передачи данных, даже если основная модель локальна.

25.2 Закрытый контур

Для закрытого контура следует запретить внешние поставщики моделей и ненужные интеграции, использовать локальные источники пакетов и образов, локальные модели и локальные корпоративные знания. Перед вводом в эксплуатацию необходимо подтвердить отсутствие непредусмотренного исходящего трафика.

25.3 Полностью изолированная среда

Полностью изолированный режим требует заранее подготовленного комплекта установки, контейнерных образов, моделей, сертификатов, резервных копий и механизма переноса подписанных обновлений. Внешние службы, включая Let’s Encrypt, публичный поиск и облачные модели, в таком режиме недоступны.

26 ЖУРНАЛЫ И ДИАГНОСТИКА

26.1 Общие команды

```
./nicesoft.sh status
./nicesoft.sh health
./nicesoft.sh logs api
./nicesoft.sh logs proxy
./nicesoft.sh logs model-manager
./nicesoft.sh logs model-runtime
./nicesoft.sh logs yandex-gateway
./nicesoft.sh logs integrations
```

26.2 Диагностика подсистемы автоматизаций

```
./nicesoft.sh logs automations
./nicesoft.sh logs automations-worker
./nicesoft.sh logs automations-db
./nicesoft.sh logs automations-redis
```

Внутренние службы автоматизаций не должны публиковать интерфейс управления наружу. Отсутствие прямого исходящего доступа из среды выполнения автоматизаций является нормальной защитной конфигурацией.

26.3 Диагностика Яндекс Облака

```
./nicesoft.sh yc-doctor
./nicesoft.sh yc-check
```

26.4 Проверка проекта

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

Эти команды полезны после изменения конфигурации или при подготовке к сопровождению. Они не заменяют функциональную проверку через пользовательский интерфейс.

27 КОМАНДНАЯ СТРОКА АВАРИЙНОГО АДМИНИСТРИРОВАНИЯ

Командная строка предназначена прежде всего для ввода в эксплуатацию, диагностики и восстановления, когда веб-интерфейс недостаточен или недоступен. Повседневное администрирование выполняется через интерфейс продукта.

Команда	Назначение
./nicesoft.sh init	Создание или актуализация конфигурации экземпляра и локального TLS.
./nicesoft.sh instance-setup	Настройка адреса, доменного имени и локального адреса привязки.
./nicesoft.sh check	Предварительная проверка сервера и конфигурации.
./nicesoft.sh install	Полный первый запуск.
./nicesoft.sh up	Запуск служб.
./nicesoft.sh down	Остановка служб без удаления постоянных данных.
./nicesoft.sh restart	Перезапуск с последующей проверкой работоспособности.
./nicesoft.sh status	Состояние контейнеров.
./nicesoft.sh logs <служба>	Просмотр журнала конкретной службы.
./nicesoft.sh health	Сводная проверка работоспособности.
./nicesoft.sh backup	Создание зашифрованной резервной копии.
./nicesoft.sh restore <файл>	Аварийное восстановление из копии.
./nicesoft.sh recovery-config <копия>	Извлечение конфигурации для полного аварийного восстановления.
./nicesoft.sh user-password-reset <email>	Безопасный сброс пароля существующего локального пользователя.

Внимание. Команды `build`, `rebuild` и публикации выпусков относятся к инженерной/сборочной инфраструктуре и не должны использоваться как обычный способ обновления клиентского промышленного экземпляра, если доступен управляемый механизм обновления.

28 РЕГЛАМЕНТНОЕ ОБСЛУЖИВАНИЕ

28.1 Ежедневно

- проверить отсутствие критичных предупреждений;
- проверить успешность последней автоматической резервной копии;
- проверить свободное место;
- при наличии локальных моделей - проверить состояние активной модели и GPU;
- просмотреть неуспешные критичные автоматизации и интеграционные ошибки.

28.2 Еженедельно

- проверить доступность обновлений;
- проверить срок сертификата;
- просмотреть административный аудит;
- проверить рост объёма загрузок и резервных копий;
- проверить неиспользуемые или просроченные подключения.

28.3 Ежемесячно

- выполнить контрольное скачивание резервной копии во внешнее хранилище;
- проверить процедуру восстановления на тестовом экземпляре или по утверждённому графику;
- пересмотреть административные роли и группы;
- проверить соответствие подключений принципу минимальных полномочий;
- проверить актуальность документации и списка ответственных лиц.

29 ДЕЙСТВИЯ ПРИ ОТКАЗАХ И ИНЦИДЕНТАХ

29.1 Общая последовательность

91. Зафиксировать время и симптомы.
92. Не выполнять разрушительные действия до сохранения журналов и состояния.
93. Запустить `./nicesoft.sh status` и `./nicesoft.sh health`.
94. Определить область: интерфейс, база, модель, интеграция, сертификат, обновление или весь узел.
95. Собрать журналы затронутых служб.
96. Если проблема возникла после изменения - применить штатный возврат, а не ручное редактирование данных.
97. При подозрении на компрометацию отозвать внешние ключи и ограничить сетевой доступ.
98. После восстановления выполнить функциональные проверки и оформить запись об инциденте.

29.2 Недоступен пользовательский интерфейс

Проверьте состояние `proxy` и `api`, затем сертификат, DNS и свободное место. Если административный интерфейс также недоступен, используйте командную проверку состояния и журналы. Не пересоздавайте постоянные тома для попытки «починить» интерфейс.

29.3 Не отвечает локальная модель

Проверьте `model-manager`, `model-runtime`, доступность GPU внутри контейнера, видеопамять и последние изменения профиля среды выполнения. Если сбой появился после изменения параметров, используйте штатный возврат к автоматической конфигурации.

29.4 Ошибка внешней модели

Выполните проверку поставщика из административного интерфейса. Проверьте DNS, сетевую политику, сертификат, срок действия ключа и наличие модели у поставщика. Не отключайте TLS-проверку для обхода ошибки сертификата.

29.5 Ошибка интеграции

Уточните, является ли ошибка общей или относится только к одному пользователю. Проверьте принадлежность подключения, права, срок действия секрета, доступ внешней системы и запись аудита.

30 АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ ПОСЛЕ ПОТЕРИ СЕРВЕРА

99. Разверните поддерживаемую версию ИИ Студии той же или более новой совместимой линии.
100. Поместите сохранённый ключ восстановления в защищённое место новой установки.
101. Запустите минимально необходимую инфраструктуру и службу резервного копирования.
102. Поместите `.nsbackup` в каталог резервных копий.
103. Извлеките комплект аварийной конфигурации командой `recovery-config`.
104. Сравните и восстановите необходимые внутренние секреты и параметры экземпляра.
105. Пересоздайте контейнеры с восстановленной конфигурацией.
106. Запустите восстановление данных из `.nsbackup`.
107. Повторно получите необходимые весовые файлы локальных моделей по сохранённому перечню.
108. Проверьте пользователей, знания, интеграции, автоматизации, модели, сертификат и резервное расписание.
109. Смените секреты, если есть основания предполагать компрометацию потерянного сервера.

```
./nicesoft.sh recovery-config /путь/к/копии.nsbackup
./nicesoft.sh restore /путь/к/копии.nsbackup
./nicesoft.sh health
```

31 ВЫВОД ЭКЗЕМПЛЯРА ИЗ ЭКСПЛУАТАЦИИ

110. Зафиксировать решение и дату прекращения эксплуатации.
111. Создать финальную резервную копию и проверить её.
112. Скачать ключ восстановления и поместить его в утверждённое хранилище.
113. Экспортировать необходимые сведения аудита согласно политике организации.
114. Отозвать ключи внешних систем и служебных учётных записей.
115. Удалить или отключить DNS-записи и внешние маршруты.
116. Остановить экземпляр.
117. Уничтожить данные на носителях согласно требованиям организации и категории информации.
118. Зафиксировать завершение процедуры в эксплуатационном журнале.

Внимание. Удаление виртуальной машины без предварительного отзыва внешних токенов и сохранения необходимой резервной копии считается некорректным выводом из эксплуатации.

32 СООБЩЕНИЯ АДМИНИСТРАТОРУ И ТИПОВЫЕ ОШИБКИ

Сообщение/ситуация	Смысл	Действие
provisioning_locked	Другая административная операция первоначальной настройки уже выполняется.	Дождаться её завершения; не запускать параллельную установку модели.
install_in_progress	Операция модели конфликтует с незавершённой установкой.	Дождаться завершения загрузки или штатного завершения операции.
provider_redirect_blocked	Внешний поставщик вернул перенаправление.	Проверить базовый адрес; не обходить защиту перенаправлением.
runtime_apply_failed_rolled_back	Новая конфигурация среды модели не запустилась, предыдущая автоматически восстановлена.	Проверить параметры и журналы; работа продолжается на старой конфигурации.
runtime_apply_failed_rollback_failed	Не запустилась новая конфигурация и не удалось вернуть предыдущую.	Аварийно диагностировать модель/GPU; не повторять изменения без анализа.
restored_incomplete_run	Запуск автоматизации был незавершён в момент копирования и после восстановления отмечен как неуспешный.	Проверить, нужен ли ручной повтор; автоматический повтор намеренно запрещён.
HTTP 403 при Яндекс Облаке	Недостаточные права или неверная область.	Проверить каталог, роли служебной учётной записи и авторизованный ключ.
Ошибка TLS внешнего поставщика	Не удалось подтвердить сертификат.	Проверить имя, цепочку сертификатов и при необходимости загрузить корпоративный ЦС.
Недостаточно свободного места	Невозможно безопасно установить модель, создать копию или подготовить обновление.	Освободить место, проверить каталоги данных и повторить предварительную проверку.

33 ПРОВЕРКА ПРОГРАММНОГО КОМПЛЕКСА

33.1 Проверка после запуска или обслуживания

119. `./nicesoft.sh health` завершается без критичных ошибок.
120. Открывается страница входа по HTTPS.
121. Администратор успешно входит в систему.
122. Раздел «Параметры → Система» отображает состояние основных служб.
123. Активная модель выполняет контрольный диалог либо, если модель ещё не настроена, интерфейс корректно показывает это состояние.
124. Создание тестового пользователя работает без выдачи административных прав.
125. Подключённые критичные интеграции проходят проверку.
126. Создание резервной копии завершается успешно и копия проходит проверку.
127. Проверка обновлений не выдаёт ошибку подписи или доверия.

33.2 Проверка после восстановления

- вход пользователей;
- история диалогов и файлы;
- корпоративные знания;
- список подключений и права;
- автоматизации и их состояние;
- активная модель и перечень локальных моделей;
- сертификат и доменное имя;
- новое резервное копирование после восстановления.

34 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ АДМИНИСТРАТОРА

34.1 Управление через внутренние программные интерфейсы

Часть административных функций реализуется через защищённые серверные маршруты, используемые самим интерфейсом. Они не предназначены для прямой публикации в пользовательскую сеть. Для промышленной интеграции с внешней системой управления следует использовать только документированные интерфейсы и отдельные сервисные учётные данные.

34.2 Испытательная проверка моделей

Для квалификации внешней модели администратор может использовать быструю и полную проверку возможностей. Для локальных артефактов доступна проверка метаданных без обязательной загрузки весов.

```
./nicesoft.sh model-artifact-test
./nicesoft.sh model-artifact-test --online-metadata
```

34.3 Машиночитаемая проверка центра пользователей

```
./nicesoft.sh user-management-test
```

Проверка предназначена для контроля защитных функций без запуска дополнительного браузерного контура и без пересоздания рабочего экземпляра.

35 НОРМАТИВНЫЕ И СПРАВОЧНЫЕ СВЕДЕНИЯ

Документ/ресурс	Назначение
ГОСТ 19.101-2024	Виды программ и программных документов; руководство системного программиста имеет код 32.
ГОСТ 19.503-79	Требования к содержанию руководства системного программиста.
ГОСТ 19.105-78	Общие требования к программным документам.
ГОСТ 19.106-78	Требования к печатным программным документам.
https://studio.ncsgp.ru	Официальный адрес продукта и публикации обновлений/сведений.
Документ «Паспорт программного продукта»	Общие сведения, назначение, комплектность и жизненный цикл.
Документ «Полное функциональное описание»	Функциональные характеристики и логическая архитектура продукта.

ПРИЛОЖЕНИЕ А. КОНТРОЛЬНЫЙ ЛИСТ ПЕРВОНАЧАЛЬНОГО ВВОДА В ЭКСПЛУАТАЦИЮ

Область	Контроль
Сервер	Выполнены системные требования, синхронизация времени, DNS, дисковое пространство.
Сеть	Открыты только необходимые входящие/исходящие направления.
HTTPS	Настроено доверенное доменное имя и сертификат для промышленного доступа.
Администраторы	Созданы не менее двух административных учётных записей; пароли переданы безопасно.
Модель	Выбрана и проверена основная модель; выполнен контрольный диалог.
Параметры модели	Зафиксированы только необходимые административные ограничения.
Пользователи	Проверено создание обычного пользователя и отсутствие административных прав.
Интеграции	Подключены только необходимые системы; проверены права и аудит.
Резервная копия	Создана, проверена и скачана первая копия; ключ восстановления сохранён отдельно.
Мониторинг	Система отображает состояние основных служб и ресурсов.
Обновления	Выбран требуемый канал и успешно выполнена проверка доступных выпусков.
Документация	Назначены ответственные за эксплуатацию, ИБ, резервные копии и обновления.

ПРИЛОЖЕНИЕ Б. РЕГЛАМЕНТ ЕЖЕДНЕВНОГО, ЕЖЕНЕДЕЛЬНОГО И ЕЖЕМЕСЯЧНОГО ОБСЛУЖИВАНИЯ

Период	Действия
Ежедневно	Состояние системы; последняя копия; свободный диск; модель/GPU; критичные ошибки интеграций и автоматизаций.
Еженедельно	Обновления; сертификат; административный аудит; объём данных; неиспользуемые подключения.
Ежемесячно	Внешняя копия; контроль восстановления; пересмотр ролей; минимальные права; актуальность ответственных.
Ежеквартально	Учебное аварийное восстановление; пересмотр сетевой схемы; проверка срока внешних секретов; сверка документации.
При каждом изменении	Резервная копия, фиксация исходного состояния, изменение, контроль работоспособности, запись результата.

ПРИЛОЖЕНИЕ В. СПРАВОЧНИК КОМАНД УПРАВЛЕНИЯ

Команда `./nicesoft.sh …`	Назначение
init	Создать/актуализировать конфигурацию и локальный TLS.
instance-setup	Настроить адрес и доменное имя.
instance-status	Показать адреса экземпляра.
instance-sync	Пересчитать производные адреса после ручной правки `.env`.
check	Проверить сервер и конфигурацию.
model-setup	Подключить внешний совместимый интерфейс модели при необходимости.
model-status	Показать адрес и модель без вывода ключа.
model-check	Повторно определить доступность внешней модели.
model-artifact-test	Проверить локальные артефакты моделей.
web-search-check	Проверить локальный поисковый контур.
yc-check	Проверить шлюз и сервисы Яндекс Облака.
yc-doctor	Диагностика доступа к Яндекс Облаку без вывода секрета.
localization-check	Проверка полноты русской локализации.
user-management-test	Машиночитаемая проверка центра пользователей.
user-password-reset	Безопасная смена пароля существующего локального пользователя.
up / down / restart	Управление запуском без удаления постоянных данных.
status	Показать состояние контейнеров.
logs	Просмотреть журналы.
health	Проверить работоспособность основных служб.
backup	Создать зашифрованную резервную копию.
restore	Восстановить данные из `.nsbackup`.
recovery-config	Извлечь конфигурацию для полной аварийной реконструкции.

ПРИЛОЖЕНИЕ Г. МАТРИЦА АДМИНИСТРАТИВНЫХ ОПЕРАЦИЙ И ПОДТВЕРЖДЕНИЙ

Операция	Подтверждение	Особенность
Создание пользователя	Нет	Проверить роль и группы после создания.
Изменение роли	Да, для понижения/критичных изменений	Отзываются прежние сеансы.
Блокирование пользователя	Да	Последний администратор защищён.
Удаление пользователя	Да	Проверить требования хранения данных.
Активация модели	Да	Только после проверки готовности.
Изменение среды локальной модели	Да	Транзакционно с автоматическим откатом.
Ротация ключа внешней модели	Да	Секрет не отображается после сохранения.
Удаление интеграции	Да	Проверить зависимые автоматизации.
Восстановление копии	Да, требуется явное подтверждение	Включается режим обслуживания.
Установка обновления	Да	Перед установкой обязательна проверенная копия.
Возврат версии	Да	Создаётся страховочная копия текущего состояния.
Смена сертификата	Да	Проверить ключ и цепочку доверия.

ПРИЛОЖЕНИЕ Д. МАТРИЦА НАСТРОЙКИ ИНТЕГРАЦИЙ

Интеграция	Основные учётные данные	Контроль администратора
Яндекс Облако	Авторизованный ключ служебной учётной записи; выбор облака и каталога.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
Яндекс 360	Пользовательская авторизация в поддерживаемом режиме.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
Jira	Личная или сервисная учётная запись/API-токен в зависимости от варианта Jira.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
Confluence	Личная или сервисная учётная запись/API-токен.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
GitHub	Личный токен пользователя.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
GitLab	Личный токен пользователя.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
PostgreSQL	Отдельный пользователь БД.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
Электронная почта	IMAP/SMTP либо поддерживаемый способ аутентификации.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
S3	Ключ доступа и секрет либо иной поддерживаемый способ.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
SFTP	Пользователь/ключ.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
WebDAV	Учётная запись или токен.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.
Telegram	Один токен бота для экземпляра и персональная привязка пользователя.	Проверка соединения; контроль минимальных прав; пробное действие под обычным пользователем.

ПРИЛОЖЕНИЕ Е. СЦЕНАРИИ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ

Сценарий	Действие	Ключевая проверка
Логическая ошибка пользователя	Восстановление выбранной рабочей копии после анализа последствий.	Убедиться, что восстановление не уничтожит более новые необходимые данные.
Неудачное обновление	Автоматический откат или восстановление предварительной копии.	Использовать встроенный механизм, не выполнять ручную подмену баз.
Потеря диска/ВМ	Новая установка + recovery-config + восстановление `.nsbackup`.	Нужны внешняя копия и отдельно сохранённый ключ.
Компрометация сервера	Развёртывание чистого экземпляра, ротация внешних секретов, восстановление проверенной копии.	Не переносить потенциально скомпрометированные ключи без анализа.
Ошибка автоматизации	Восстановление данных при необходимости; незавершённые запуски не повторяются автоматически.	Проверить внешние побочные эффекты перед ручным повтором.

ПРИЛОЖЕНИЕ Ж. ДИАГНОСТИКА МОДЕЛЕЙ И ГРАФИЧЕСКИХ УСКОРИТЕЛЕЙ

128. Проверить «Параметры → Система» и аппаратный отчёт модели.
129. Проверить, виден ли GPU внутри среды выполнения.
130. Проверить свободную видеопамять и отсутствие других процессов, занявших устройство.
131. Просмотреть журналы `model-manager` и `model-runtime`.
132. Если проблема началась после изменения профиля - выполнить проверку профиля и возврат к автоматической конфигурации.
133. Проверить соответствие числа GPU тензорному параллелизму.
134. Проверить, что длина контекста не превышает нативное значение модели и возможности памяти.
135. При ошибках внешней модели отделить сетевую диагностику поставщика от диагностики локального GPU.

```
./nicesoft.sh logs model-manager
./nicesoft.sh logs model-runtime
./nicesoft.sh model-artifact-test
```

ПРИЛОЖЕНИЕ И. КОНТРОЛЬНЫЙ ЛИСТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

☐ Административные полномочия выданы только назначенным сотрудникам.

☐ Последний администратор защищён; существует резервная административная учётная запись.

☐ Основной доступ работает по доверенному HTTPS.

☐ Закрытые ключи и токены не хранятся в пользовательских сообщениях и документации.

☐ Внешние поставщики моделей используют проверку TLS; отключение проверки не применяется.

☐ Сетевые правила ограничивают административную поверхность.

☐ Пользовательские интеграции привязаны к владельцам.

☐ Для действий с побочным эффектом применено подтверждение человеком там, где это требуется.

☐ Резервные копии шифруются; ключ хранится отдельно.

☐ Есть внешняя актуальная копия.

☐ Обновления проверяются по подписи и неизменяемым контрольным суммам.

☐ Ведётся периодический просмотр административного аудита.

☐ При увольнении/компрометации выполняется отзыв секретов внешних систем.

☐ В закрытом контуре проверено отсутствие непредусмотренного исходящего трафика.

ПРИЛОЖЕНИЕ К. КРИТЕРИИ ЭКСПЛУАТАЦИОННОЙ ПРИЁМКИ

Область	Критерий
Доступ	Администратор и обычный пользователь входят по HTTPS; обычный пользователь не видит административные разделы.
Пользователи	Создание, изменение роли, блокирование и безопасная защита последнего администратора работают.
Модель	Активная модель отвечает; изменение локальных параметров проходит предварительную проверку и транзакционное применение.
Внешняя модель	Поставщик проходит сетевую/TLS-проверку; секрет не возвращается через интерфейс.
Знания	Загрузка документа и поиск по нему работают в заданной модели доступа.
Интеграции	Критичные подключения проходят проверку и соблюдают права пользователя.
Автоматизации	Тестовый процесс запускается, журналируется и не получает прямой неограниченный доступ к секретам.
Мониторинг	Отображаются ресурсы и состояние основных служб.
Сертификат	Домен и сертификат действительны с пользовательского рабочего места.
Резервирование	Копия создаётся, проверяется, скачивается; ключ восстановления сохранён отдельно.
Обновления	Проверка канала и подписей завершается успешно.
Восстановление	На тестовом контуре подтверждена процедура восстановления или имеется актуальный протокол такого испытания.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов	Всего листов	Номер документа	Дата	Подпись