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

ПРОГРАММНЫЙ КОМПЛЕКС

«НАЙС СОФТ ИИ СТУДИЯ»

версия 1.0.0

ОПИСАНИЕ ЛОКАЛЬНОГО РЕЖИМА

НССГ.10001-01 95 02-ЛУ

Лист утверждения

Красногорск
2026

Утвержден НССГ.10001-01 95 02-ЛУ

ООО «НАЙС СОФТ ГРУПП»

ПРОГРАММНЫЙ КОМПЛЕКС

«НАЙС СОФТ ИИ СТУДИЯ»

Версия 1.0.0

ОПИСАНИЕ ЛОКАЛЬНОГО РЕЖИМА

НССГ.10001-01 95 02

Листов 69

Красногорск
2026

АННОТАЦИЯ

Настоящий документ описывает локальный режим программного комплекса «Найс Софт ИИ Студия» версии 1.0.0: варианты размещения и обработки данных внутри инфраструктуры организации, правила использования локальных моделей искусственного интеллекта, корпоративных баз знаний и внутренних интеграций, управление внешними сетевыми взаимодействиями, полностью закрытый и полностью изолированный контуры, автономную поставку обновлений и моделей, резервное копирование, мониторинг и доказательство отсутствия неразрешённой передачи данных за пределы контура.

Документ предназначен для ИТ-архитекторов, системных администраторов, подразделений информационной безопасности, владельцев информационных систем, специалистов по защите информации, государственных и коммерческих заказчиков, закупочных комиссий и интеграторов. Он применяется совместно с паспортом продукта, полным функциональным описанием, руководством администратора, руководством по установке, системными требованиями, матрицей совместимости и описанием информационной безопасности.

Ключевой принцип. Локальный режим означает, что организация может развернуть ИИ Студию на собственной инфраструктуре и самостоятельно определить границу допустимого обмена данными. Полностью изолированный режим достигается сочетанием настроек продукта и инфраструктурных мер: отсутствием внешней маршрутизации, запретом исходящих соединений и автономной поставкой необходимых артефактов.

СТАТУС И ОБЛАСТЬ ПРИМЕНЕНИЯ

Документ является нормативно-техническим документом комплекта версии 1.0.0 и описывает поддерживаемые схемы локальной эксплуатации. Он не заменяет проектирование конкретной сети заказчика, модель угроз, документацию системы защиты информации, аттестационные материалы или требования регулирующих органов, если такие требования применимы к конкретной информационной системе.

Основной референсной операционной системой является НАЙС.ОС CLOUD. Локальный режим также применяется на других российских серверных операционных системах в соответствии с системными требованиями и матрицей совместимости ИИ Студии.

Официальный адрес продукта: https://studio.ncsgp.ru. Реестровая запись НАЙС.ОС CLOUD: №30128 от 22.10.2025 в Едином реестре российского программного обеспечения.

НОРМАТИВНЫЕ И СПРАВОЧНЫЕ ОСНОВАНИЯ

- ГОСТ 19.101-2024 «Единая система программной документации. Виды программ и программных документов».
- ГОСТ 19.105-78 «ЕСПД. Общие требования к программным документам».
- ГОСТ 19.106-78 «ЕСПД. Требования к программным документам, выполненным печатным способом».
- ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».
- ГОСТ Р 59898-2021 «Оценка качества систем искусственного интеллекта».
- ГОСТ Р 72514-2026 «Искусственный интеллект. Оценка воздействия системы искусственного интеллекта».
- ГОСТ Р 72515-2026 «Искусственный интеллект. Таксономия прозрачности систем искусственного интеллекта».
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» - при обработке персональных данных.
- Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» - при применимости.
- Приказ ФСТЭК России от 11.04.2025 №117 (ред. от 08.05.2026) - при применении в государственных и иных указанных в приказе информационных системах.

Примечание. Применимость конкретных нормативных требований определяется назначением информационной системы заказчика. Наличие локального режима само по себе не означает автоматического соответствия конкретному классу защищённости, уровню защищённости персональных данных или категории значимости объекта КИИ.

СОДЕРЖАНИЕ

1 Общие положения 8
2 Термины и сокращения 9
3 Цели локального режима 10
4 Границы продукта и инфраструктуры заказчика 11
5 Классификация режимов локальной эксплуатации 12
6 Режим Л-1: локальная обработка с управляемым внешним доступом 13
7 Режим Л-2: закрытый корпоративный контур 14
8 Режим Л-3: полностью изолированный контур 15
9 Сравнение режимов 16
10 Размещение и суверенность данных 17
11 Архитектура локального контура 18
12 Локальные учётные записи и управление доступом 19
13 Локальные модели искусственного интеллекта 20
14 Реестр моделей и выбор активной модели 21
15 Внешние и управляемые модели в локальной архитектуре 22
16 Корпоративные базы знаний и RAG 23
17 Файлы, изображения и пользовательские данные 24
18 Веб-поиск в локальном контуре 25
19 Корпоративные интеграции 26
20 Автоматизации и фоновые задания 27
21 Корпоративная почта и коммуникации 28
22 Системы разработки и управления задачами 29
23 Базы данных и файловые хранилища 30
24 Сетевая сегментация 31
25 Исходящие соединения и межсетевой экран 32
26 Прокси-сервер и контролируемый внешний доступ 33
27 DNS в локальном и изолированном контуре 34
28 Синхронизация времени 35
29 TLS и корпоративная инфраструктура открытых ключей 36
30 Сертификаты в полностью изолированном контуре 37
31 Обновление в локальном режиме 38
32 Автономное обновление полностью изолированного контура 39
33 Проверка происхождения и целостности артефактов 40
34 Автономная поставка локальных моделей 41
35 Автономная поставка контейнерных образов 42
36 SBOM, лицензии и происхождение компонентов 43
37 Резервное копирование 44
38 Аварийное восстановление 45
39 Локальный мониторинг 46
40 Журналирование и аудит 47
41 Подтверждение отсутствия внешней передачи данных 48
42 Сетевые испытания локального режима 49
43 Приёмочные испытания 50
44 Эксплуатация и административные операции 51
45 Переход между режимами 52
46 Ограничения и особые условия 53
47 Персональные данные, ГИС и КИИ 54
48 Меры информационной безопасности 55
49 Отказоустойчивость и непрерывность 56
50 Вывод из эксплуатации 57
51 Типовые архитектурные сценарии 58
52 Требования для закупки и проектирования 59

53 Техническая поддержка изолированного контура 60
54 Разделение ответственности 61
Приложение А. Сводная матрица режимов 62
Приложение Б. Пример перечня разрешённых внешних соединений 63
Приложение В. Состав автономного комплекта поставки 64
Приложение Г. Протокол приёмки локального режима 65
Приложение Д. Протокол подтверждения отсутствия внешней передачи 66
Приложение Е. Контрольный лист эксплуатации 67
Приложение Ж. Нормативные и официальные источники 68
Лист регистрации изменений 69

1 Общие положения

Локальный режим является базовой архитектурной возможностью ИИ Студии и позволяет эксплуатировать продукт на вычислительных ресурсах заказчика: физическом сервере, виртуальной машине, частном облаке или выделенном облачном сегменте. Пользовательские данные, диалоги, документы, векторное хранилище, конфигурация, учётные данные интеграций и эксплуатационные журналы размещаются в постоянных хранилищах экземпляра организации.

В зависимости от политики организации локальная установка может взаимодействовать с отдельными внешними сервисами либо работать без доступа к сети Интернет. Сам факт размещения на локальном сервере не равнозначен полностью изолированному режиму: режим определяется совокупностью сетевой политики, выбранных моделей, настроенных интеграций и способа поставки обновлений.

- Референсная ОС - НАЙС.ОС CLOUD.
- Пользовательский интерфейс доступен через браузер по HTTPS.
- Внешняя идентификация не требуется: в поставку входят локальные учётные записи ИИ Студии.
- Локальные модели могут выполняться на GPU или, для отдельных сценариев, на CPU.
- Корпоративные знания и RAG размещаются внутри контура.
- Внешние сервисы используются только при их явном подключении и разрешённой сетевой доступности.

2 Термины и сокращения

Термин	Определение
Локальный режим	Размещение ИИ Студии и основных данных в инфраструктуре организации.
Закрытый контур	Сеть без прямого доступа в Интернет, в которой разрешены только внутренние корпоративные системы.
Полностью изолированный контур	Контур без маршрутизации во внешние сети; перенос ПО, моделей и обновлений выполняется контролируемым автономным способом.
Локальная модель	Модель ИИ, вычисления которой выполняются на ресурсах экземпляра или в другом доверенном внутреннем сегменте.
Поставщик модели	Сервис, предоставляющий программный интерфейс модели. Может быть локальным, корпоративным или внешним.
База знаний (RAG)	Механизм поиска релевантных фрагментов корпоративных данных и передачи их модели как контекста.
Исходящее соединение	Сетевое соединение, инициируемое компонентом Студии в другой узел.
Разрешённый список	Явно утверждённый набор адресов, имён, портов или сервисов, с которыми разрешено взаимодействие.
Автономный комплект	Набор подписанных артефактов, достаточный для установки или обновления без сетевого доступа к внешним репозиториям.
SBOM	Машиночитаемый перечень программных компонентов и их версий.

3 Цели локального режима

Локальный режим предназначен для организаций, которым требуется контролировать место обработки данных, снизить зависимость от внешних облачных сервисов и применять ИИ внутри собственной инфраструктуры. Он также является основой для построения решений в регулируемых и технологически изолированных сегментах.

- обработка конфиденциальной информации внутри контролируемой инфраструктуры;
- использование локальных моделей без передачи запросов внешнему поставщику;
- создание корпоративной базы знаний без выгрузки исходных документов за пределы контура;
- подключение внутренних Jira, Confluence, GitLab, PostgreSQL, почты и файловых хранилищ;
- контролируемое разрешение отдельных внешних сервисов при необходимости;
- полностью автономная эксплуатация при отсутствии Интернет-соединения;
- сохранение возможности обновления и аварийного восстановления через подписанный автономный комплект.

4 Границы продукта и инфраструктуры заказчика

ИИ Студия предоставляет механизмы локального хранения, локального исполнения моделей, внутренней маршрутизации, изоляции учётных данных, управления обновлениями и резервным копированием. Однако окончательная граница изоляции формируется инфраструктурой заказчика. Для полностью изолированного режима сеть должна блокировать неразрешённые исходящие маршруты независимо от состояния приложений.

Область	Ответственность ИИ Студии	Ответственность заказчика
Приложение	Локальные сервисы, учётные записи, маршрутизация моделей, RAG, аудит.	Настройка ролей и регламентов эксплуатации.
Сеть	Не требует внешнего доступа для локальных функций; внешние интеграции явны.	Маршруты, межсетевой экран, сегментация, прокси, контроль DNS.
ОС	Референсные настройки и требования.	Обновление ОС, учётные записи ОС, hardening, журналирование.
Криптография	Прикладное TLS, шифрование секретов и резервных копий.	Сертифицированные СКЗИ, если они обязательны для конкретной системы.
Носители	Проверка подписи и целостности артефактов.	Учёт, доставка, проверка и хранение переносимых носителей.
Физическая защита	Не относится к прикладному ПО.	Контроль доступа к серверу, СХД, сети и носителям.

5 Классификация режимов локальной эксплуатации



Рисунок 1 - Классификация локальных режимов

Режим выбирается не один раз на весь срок эксплуатации: организация может переходить между режимами при соблюдении процедуры изменения сетевой политики и повторной квалификации. Режим должен быть отражён в эксплуатационном паспорте конкретного экземпляра.

6 Режим Л-1: локальная обработка с управляемым внешним доступом

В режиме Л-1 основная обработка и хранение выполняются локально, однако отдельным компонентам разрешается обращаться к утверждённым внешним сервисам. Это наиболее гибкая схема для коммерческого предприятия, которому нужны локальная база знаний и локальные модели, но одновременно требуются облачная модель, GitHub, Telegram, Яндекс Облако или получение обновлений через Интернет.

- все пользовательские данные по умолчанию хранятся в локальных постоянных томах;
- локальная модель может быть основной;
- внешний поставщик модели используется только при наличии подключения и выборе соответствующего источника;
- Интернет-доступ может быть реализован через корпоративный прокси;
- исходящий трафик рекомендуется ограничивать разрешённым списком;
- обновления могут получаться штатным подписанным каналом.

Рекомендация. Даже в Л-1 не следует предоставлять серверу неограниченный доступ в Интернет. Для производственной эксплуатации предпочтителен прокси или фильтрация назначения исходящих соединений.

7 Режим Л-2: закрытый корпоративный контур

В режиме Л-2 сервер ИИ Студии не имеет доступа в публичный Интернет. Допускаются соединения только с внутренними корпоративными сервисами: локальными моделями, LDAP/SSO-посредниками при их дальнейшем внедрении, внутренними GitLab/Jira/Confluence, PostgreSQL, файловыми хранилищами, почтой, прокси-порталом организации и другими системами, расположенными в доверенной сети.

- внешние облачные модели не используются;
- публичный веб-поиск отключён либо заменён внутренним поисковым источником;
- внешние Telegram/GitHub Cloud/Yandex Cloud подключения отключены;
- обновления и модели поступают через внутренний репозиторий или контролируемый перенос;
- DNS и NTP должны предоставляться внутренними службами;
- сертификаты выдаются корпоративной инфраструктурой открытых ключей либо локальным центром доверия.

8 Режим Л-3: полностью изолированный контур

В режиме Л-3 отсутствует маршрутизация из контура во внешние сети. Доставка программного обеспечения, контейнерных образов, локальных моделей, лицензий и обновлений производится автономным комплектом после внешней проверки и контролируемого переноса. Все пользовательские операции и вычисления выполняются на локальных ресурсах.

- нет Интернет-маршрута и внешнего DNS;
- внешние поставщики моделей недоступны;
- работают только локальные модели и внутренние сервисы;
- обновление не зависит от доступности studio.ncsgp.ru;
- переносимые носители учитываются по правилам организации;
- резервные копии выводятся на внутреннее/автономное хранилище;
- доказательство режима включает сетевые испытания и фиксацию отсутствия внешних сессий.

Важно. Полностью изолированный режим должен подтверждаться инфраструктурно. Отключение внешних интеграций в интерфейсе без блокировки маршрутов не является достаточным доказательством изоляции.

9 Сравнение режимов

Характеристика	**Л-1**	**Л-2**	**Л-3**
Размещение данных	Локально	Локально	Локально
Локальные модели	Да	Да	Да
Внешние модели	По разрешению	Нет	Нет
Внутренние интеграции	Да	Да	Да
Публичные внешние интеграции	По разрешению	Нет	Нет
Публичный веб-поиск	По разрешению	Нет/внутренний источник	Нет/внутренний источник
Онлайн-обновления	Да	Через внутренний шлюз или нет	Нет
Автономные обновления	Допустимы	Да	Обязательны
DNS	Корпоративный/внешний	Внутренний	Внутренний
NTP	Корпоративный/внешний	Внутренний	Внутренний
Доказательство отсутствия внешнего трафика	Не требуется для разрешённых сервисов	Рекомендуется	Обязательно для приёмки

10 Размещение и суверенность данных

В локальном развертывании авторитетные данные Студии находятся на стороне заказчика. К ним относятся пользователи и диалоги, векторное хранилище, загрузки, конфигурация моделей, метаданные интеграций, зашифрованные учётные данные, определения автоматизаций, состояние административных подсистем, сертификаты и резервные копии.

Категория	Основное локальное хранилище	Внешняя передача
Диалоги и пользователи	MongoDB	Только если содержимое запроса отправляется явно выбранной внешней модели.
Корпоративные знания	pgvector/локальные файлы	Не требуется для локальной модели.
Загруженные файлы	Постоянное хранилище Студии	Не требуется; зависит от выбранного внешнего действия.
Учётные данные интеграций	Зашифрованные локальные хранилища	Передаётся только необходимая авторизация целевой системе.
Локальные модели	data/models и среда выполнения	Не передаются.
Журналы и метрики	Локальные службы журналирования/Prometheus	Не требуется.
Резервные копии	.nsbackup	Не требуется; место внешнего хранения выбирает заказчик.

11 Архитектура локального контура



Рисунок 2 - Логическая граница локального контура

Внутренние базы данных, служба резервного копирования, служба сертификатов, мониторинг, интеграционный шлюз и контур автоматизаций не должны публиковать собственные административные порты во внешнюю сеть. Доступ к административным операциям осуществляется через интерфейс Студии после серверной проверки роли.

12 Локальные учётные записи и управление доступом

Базовая поставка использует локальные учётные записи ИИ Студии и не требует внешней службы идентификации. Это позволяет эксплуатировать продукт в контуре, где отсутствует доступ к внешнему провайдеру идентификации. Пользовательская идентичность и состояние учётной записи хранятся внутри экземпляра.

- учётная запись создаётся и управляется администратором/штатным механизмом регистрации согласно политике экземпляра;
- блокировка и отзыв сеансов выполняются локально;
- роли и права не зависят от внешней облачной службы;
- учётные данные интеграций принадлежат конкретному аутентифицированному пользователю;
- административная роль не предоставляет автоматический доступ к пользовательским секретам.

13 Локальные модели искусственного интеллекта

Локальная модель является основным способом обеспечить отсутствие передачи текста запроса и контекста внешнему поставщику. Среда выполнения модели размещается в том же экземпляре либо в доверенном внутреннем вычислительном сегменте. Для производительного вывода могут использоваться графические ускорители NVIDIA в соответствии с системными требованиями.

- веса модели загружаются заранее или переносятся автономно;
- модель регистрируется в каталоге ИИ Студии;
- состояние и параметры модели контролируются локальным центром управления моделями;
- маршрутизация пользователя выполняется через стабильное имя активной модели;
- контекст, RAG-фрагменты и вызовы инструментов не требуют выхода в Интернет при локальной модели.

Лицензии моделей. Право использования конкретных весов модели определяется лицензией правообладателя модели и должно проверяться до переноса модели в закрытый контур.

14 Реестр моделей и выбор активной модели

Реестр моделей хранит сведения о подключённых моделях, их происхождении, параметрах, возможностях и состоянии. В локальном режиме он является единой точкой контроля: администратор может определить, какие модели разрешены, какая модель используется по умолчанию и какие возможности считаются подтверждёнными.

Состояние возможности	Смысл в локальном режиме
Подтверждено	Возможность проверена фактическим запросом или квалификацией.
Поддерживается	Заявлена адаптером/поставщиком и допустима политикой.
Не определено	Студия не считает возможность доказанной; критические действия не должны строиться на предположении.
Не поддерживается	Функция не предлагается пользователю для этой модели.
Ошибка	Последняя проверка неуспешна.
Устарело	Результат проверки требует повторной квалификации.

15 Внешние и управляемые модели в локальной архитектуре

В режиме Л-1 организация может подключить внешний совместимый программный интерфейс модели или управляемую модель. В таком случае текст запроса, контекст и при необходимости изображения могут покидать локальный контур. Это должно быть явно отражено в политике конфиденциальности и разрешённом списке соединений.

В режимах Л-2 и Л-3 внешние модели должны быть отключены или сетево недоступны. Возможен внутренний корпоративный поставщик модели, если его сервер находится внутри той же доверенной инфраструктуры и квалифицирован как внутренний ресурс.

Принцип отсутствия скрытого перехода. Локальный режим не должен автоматически переключать обработку на внешний облачный сервис при недоступности локальной модели, если такое поведение не утверждено администратором и политикой организации.

16 Корпоративные базы знаний и RAG

Корпоративная база знаний предназначена для поиска фрагментов внутренних документов и передачи их выбранной модели в качестве контекста. Индексация, векторное хранение и поиск выполняются внутри экземпляра. При локальной модели весь цикл «документ → индекс → поиск → ответ» может оставаться внутри контура.

- документы сохраняются в локальном хранилище;
- векторные представления хранятся локально;
- поисковый запрос выполняется внутри контура;
- найденные фрагменты передаются локальной модели без внешней сети;
- при использовании внешней модели выбранные фрагменты становятся частью внешнего запроса и должны учитываться политикой данных.

17 Файлы, изображения и пользовательские данные

Загруженные пользователями файлы и изображения являются данными заказчика. В локальном режиме они сохраняются в постоянных томах экземпляра и включаются в резервное копирование в соответствии с политикой продукта. Выгрузка файла внешней системе происходит только как следствие явно выбранной интеграции или внешнего поставщика модели, поддерживающего соответствующий тип данных.

Действие	**Л-1**	**Л-2/Л-3**
Загрузка файла в чат	Локально	Локально
Индексация в базе знаний	Локально	Локально
Анализ локальной моделью	Локально	Локально
Анализ внешней мультимодальной моделью	Допустим по политике	Запрещён/недоступен
Отправка вложения во внешнюю интеграцию	Только явным действием	Только внутренней системе

18 Веб-поиск в локальном контуре

В поставку входит локальная служба поиска и получения веб-страниц. Сам сервис запускается локально, однако поиск по публичной сети Интернет естественным образом требует сетевого доступа к поисковым и целевым ресурсам. Поэтому наличие локального контейнера поиска не следует смешивать с отсутствием внешнего трафика.

- Л-1: публичный веб-поиск может быть разрешён и контролироваться прокси/межсетевым экраном;
- Л-2: публичный Интернет-поиск отключается; допустим внутренний источник поиска или корпоративный индекс;
- Л-3: публичный поиск недоступен; используются локальные документы и внутренние индексированные ресурсы.

19 Корпоративные интеграции

Интеграционный шлюз может работать с системами, расположенными внутри той же сети. В закрытом контуре наиболее типичны локальные Jira/Confluence, GitLab, PostgreSQL, S3-совместимое хранилище, SFTP, WebDAV и корпоративная почта. Сетевой статус интеграции определяется расположением конкретного сервиса, а не его названием.

Интеграция	**Л-1**	**Л-2**	**Л-3**
Jira/Confluence Data Center внутри организации	Да	Да	Да
GitLab Self-Managed внутри организации	Да	Да	Да
PostgreSQL внутри организации	Да	Да	Да
Внутренний S3/SFTP/WebDAV	Да	Да	Да
Внутренний IMAP/SMTP	Да	Да	Да
GitHub.com	По разрешению	Нет	Нет
Telegram	По разрешению	Нет	Нет
Яндекс Облако / Yandex AI	По разрешению	Нет	Нет

20 Автоматизации и фоновые задания

Контур автоматизаций является внутренней исполнительной средой. Его служебные контейнеры не должны иметь прямой публичный интерфейс, а внешнее действие выполняется через интеграционный шлюз с учётом владельца, разрешений и учётных данных. В закрытом режиме автоматизации могут работать полностью внутри корпоративной сети.

- расписания выполняются локально;
- состояние заданий и история запусков хранятся локально;
- внешний побочный эффект возможен только через разрешённую интеграцию;
- при восстановлении очереди не должны молча повторять незавершённые внешние действия;
- в полностью изолированном режиме разрешёнными целями являются только внутренние системы.

21 Корпоративная почта и коммуникации

Для закрытого контура может применяться внутренний почтовый сервер по IMAP/SMTP. При этом соединение не покидает корпоративную сеть. Если используется внешний облачный почтовый сервис, режим следует классифицировать как Л-1 и включить соответствующие адреса в разрешённый список.

Telegram и аналогичные публичные мессенджеры несовместимы с требованиями Л-2/Л-3 без специального внутреннего шлюза, поскольку требуют сетевого соединения с внешним сервисом.

22 Системы разработки и управления задачами

GitLab Self-Managed, GitHub Enterprise Server, Jira Data Center и Confluence Data Center могут быть полностью внутренними источниками. Для каждого подключения администратор должен указывать внутренний адрес и проверять, что DNS не разрешает его во внешний адрес. Облачные варианты GitHub/Jira/Confluence относятся к внешним сервисам режима Л-1.

Рекомендация. В закрытом контуре используйте внутренние доменные имена и корпоративный центр сертификации; не отключайте проверку TLS как способ обхода недоверенного сертификата.

23 Базы данных и файловые хранилища

Подключение к PostgreSQL в ИИ Студии предназначено для контролируемого чтения данных. В локальном режиме БД может находиться на том же сервере, в отдельном сегменте или в корпоративном кластере. Аналогично S3, SFTP и WebDAV могут выступать внутренними хранилищами документов.

- доступ предоставляется с минимальными правами;
- для PostgreSQL рекомендуется отдельная учётная запись только для чтения;
- сетевой доступ ограничивается адресом целевой БД/хранилища;
- секрет хранится в пользовательском изолированном хранилище Студии;
- результаты запроса рассматриваются как недоверенный внешний контент перед передачей модели.

24 Сетевая сегментация

Для производственного локального размещения рекомендуется выделить сервер ИИ Студии в отдельный серверный сегмент. Пользовательский HTTPS-порт доступен рабочим местам, административный доступ - только администраторам, а внутренние БД и служебные интерфейсы не публикуются в пользовательские сети.

Зона	Назначение	Типовые направления
Пользовательская	Браузеры пользователей	HTTPS к ИИ Студии
Административная	Управление сервером и ОС	SSH/административный HTTPS по политике организации
Серверная	ИИ Студия и внутренние БД	Внутренние контейнерные сети и постоянные хранилища
Интеграционная	Корпоративные сервисы	Jira/GitLab/БД/почта/хранилища
Внешняя	Интернет и облачные сервисы	Только Л-1 через контролируемый выход

25 Исходящие соединения и межсетевой экран

Главный технический контроль локального режима - политика исходящих соединений. Для Л-2 и Л-3 рекомендуется модель «запрещено по умолчанию». Для Л-1 разрешаются только утверждённые назначения и порты. Блокировка должна выполняться вне контейнера приложения: на хосте, межсетевом экране сегмента либо на обоих уровнях.

Категория назначения	**Л-1**	**Л-2**	**Л-3**
Внутренний DNS/NTP	Разрешено	Разрешено	Разрешено
Внутренние интеграции	Разрешено	Разрешено	Разрешено
studio.ncsgp.ru / реестр обновлений	Разрешено по политике	Только через внутренний шлюз/нет	Нет
Внешний реестр контейнеров	По политике	Нет	Нет
Хранилище моделей в Интернете	По политике	Нет	Нет
Облачная модель	По политике	Нет	Нет
Произвольный Интернет	Не рекомендуется	Запрещено	Запрещено

26 Прокси-сервер и контролируемый внешний доступ

В режиме Л-1 организация может использовать корпоративный прокси-сервер. Для загрузки локальных моделей предусмотрены стандартные переменные прокси среды выполнения модели. Это позволяет направить трафик загрузки через контролируемую точку и сохранить прямые внутренние соединения в перечне исключений.

```
NICESOFT_MODEL_HTTP_PROXY=http://proxy.example.local:3128
NICESOFT_MODEL_HTTPS_PROXY=http://proxy.example.local:3128
NICESOFT_MODEL_NO_PROXY=localhost,127.0.0.1,model-manager,model-runtime,model-runtime-test
```

Фактические значения определяются инфраструктурой заказчика. Секреты аутентификации прокси не рекомендуется хранить в открытом виде в общедоступной документации или журналах.

27 DNS в локальном и изолированном контуре

Л-2 и Л-3 должны использовать внутренний DNS. Для полностью изолированного контура все имена, необходимые работе продукта, должны разрешаться без обращения к публичным резолверам. Если внутренний сервис указан по имени, его DNS-запись должна однозначно разрешаться во внутренние адреса.

- запретить публичные DNS-серверы на хосте;
- на межсетевом экране разрешить DNS только к утверждённым внутренним резолверам;
- контролировать отсутствие внешних DNS-запросов при приёмочных испытаниях;
- не использовать публичное имя как скрытый обход изоляции;
- для внутренних интеграций применять корпоративную доменную зону.

28 Синхронизация времени

Корректное время необходимо для TLS, журналов, расписаний, подписанных артефактов и расследования инцидентов. В Л-2/Л-3 сервер должен синхронизироваться с внутренним NTP-сервером или другим утверждённым источником времени. При полном отсутствии сети допускается автономный доверенный источник времени, но расхождение необходимо контролировать регламентом.

Критичность. Значительное расхождение часов может приводить к ошибкам сертификатов, неверной хронологии аудита и запуску автоматизаций в неправильное время.

29 TLS и корпоративная инфраструктура открытых ключей

Пользовательский интерфейс должен использовать HTTPS. В корпоративном контуре предпочтительно применять сертификат внутреннего удостоверяющего центра, которому доверяют рабочие станции. ИИ Студия содержит отдельную внутреннюю службу управления сертификатами; операции доступны администратору через защищённый административный интерфейс.

- закрытый ключ не передаётся пользователям;
- сертификаты резервируются вместе с конфигурацией;
- доступ к каталогу ключей ограничивается;
- для внутренних интеграций проверка сертификата должна оставаться включённой;
- не следует использовать отключение проверки TLS как постоянный способ совместимости.

30 Сертификаты в полностью изолированном контуре

Let's Encrypt и другие публичные центры сертификации требуют внешней связи, поэтому в Л-3 применяются корпоративный или локальный центр сертификации. Корневой сертификат доверия доставляется на рабочие станции средствами организации. Срок действия и порядок обновления сертификата должны быть включены в эксплуатационный регламент.

Вариант	Применимость	Комментарий
Корпоративный УЦ	Предпочтительно	Централизованное доверие и отзыв.
Локальный УЦ Студии/площадки	Допустимо	Требуется безопасная доставка корневого сертификата.
Самоподписанный серверный сертификат	Временный/ограниченный	Требует ручной установки доверия; хуже управляется.
Let's Encrypt	Л-1	Не подходит полностью изолированному контуру без специальной внешней процедуры.

31 Обновление в локальном режиме

В Л-1 может использоваться штатная служба обновления: она обращается к фиксированному источнику метаданных, проверяет канал и подпись Ed25519, получает неизменяемые контейнерные образы по digest, выполняет предварительную проверку, создаёт и проверяет резервную копию, после чего переключает версию через одноразовый исполнитель и контроль работоспособности.

В Л-2 онлайн-обновление возможно только через утверждённый внутренний шлюз/зеркало, если организация допускает такой механизм. В противном случае применяется автономный комплект, как для Л-3.

32 Автономное обновление полностью изолированного контура

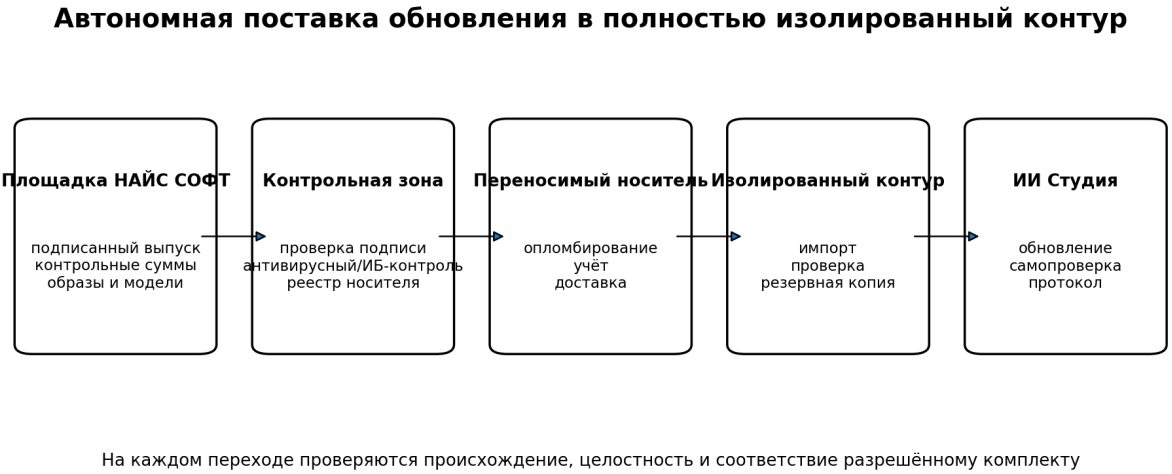


Рисунок 3 - Автономное обновление изолированного контура

1. Получить официальный автономный комплект выпуска на внешней контрольной площадке.
2. Проверить подпись, контрольные суммы, перечень файлов, SBOM и лицензии.
3. Провести установленный организацией антивирусный и ИБ-контроль носителя.
4. Зарегистрировать носитель и комплект в журнале передачи.
5. Внести комплект в изолированный контур.
6. Повторно проверить подпись и контрольные суммы уже внутри контура.
7. Создать и проверить резервную копию текущей версии.
8. Импортировать контейнерные образы и, при необходимости, веса моделей во внутреннее хранилище.
9. Запустить обновление без сборки на сервере заказчика.
10. Выполнить проверку работоспособности и оформить протокол.

33 Проверка происхождения и целостности артефактов

Автономность не должна приводить к отказу от проверки происхождения. Напротив, в изолированном контуре контроль артефактов особенно важен, так как файл проходит через физическую цепочку передачи. Для выпуска должны быть доступны подписанный манифест, контрольные суммы и точные идентификаторы контейнерных образов.

- проверка подписи доверенным открытым ключом;
- проверка SHA-256 каждого файла;
- сопоставление образа с зафиксированным repository@sha256;
- запрет сборки контейнеров из непроверенных Dockerfile на рабочем сервере;
- фиксация версии, даты и источника автономного комплекта;
- сохранение протокола проверки вместе с эксплуатационной документацией.

34 Автономная поставка локальных моделей

Для Л-3 веса локальных моделей должны быть подготовлены заранее. Рекомендуется хранить их в отдельном внутреннем каталоге артефактов или на зарегистрированном носителе. До импорта проверяются происхождение, лицензия, контрольная сумма, формат и совместимость с закреплённой средой выполнения.

Проверка модели	**Что фиксируется**
Происхождение	Правообладатель/поставщик и официальное имя модели.
Лицензия	Условия коммерческого/внутреннего использования.
Версия/ревизия	Точный checkpoint/revision.
Формат	Например, safetensors и выбранная квантизация.
Контрольная сумма	Хэш каждого артефакта или манифеста.
Совместимость	Профиль GPU, версия среды выполнения, контекст.
Возможности	Текст, изображения, инструменты, структурированный ответ - по фактической квалификации.

35 Автономная поставка контейнерных образов

Контейнерные образы автономного комплекта рекомендуется импортировать во внутренний реестр организации или доставлять как проверенные архивы образов. ИИ Студия должна запускать именно те digest, которые перечислены в подписанном манифесте. Внешний реестр в Л-3 недоступен и не должен использоваться как скрытая зависимость.

- внутренний реестр должен быть доступен только из доверенных сегментов;
- имя тега не является достаточной фиксацией версии - используется digest;
- собственные и сторонние образы различаются по происхождению;
- реестр должен поддерживать резервное копирование или повторяемый импорт комплекта;
- избыточные старые образы удаляются по регламенту после подтверждения возможности отката.

36 SBOM, лицензии и происхождение компонентов

Автономный комплект должен сопровождаться перечнем программных компонентов и лицензий. Это позволяет службе ИБ заказчика заранее оценить происхождение зависимостей без обращения к Интернету. SBOM не заменяет лицензионный реестр и уведомления сторонних компонентов, но является машиннообрабатываемой основой контроля состава.

- версия ИИ Студии;
- перечень собственных контейнеров;
- перечень сторонних контейнеров и библиотек;
- точные версии и контрольные суммы;
- лицензии;
- известные ограничения;
- дата формирования;
- связь с подписанным манифестом выпуска.

37 Резервное копирование

Резервное копирование полностью локально и не требует внешнего сервиса. Служба резервного копирования создаёт зашифрованные архивы .nsbackup, проверяет их целостность, поддерживает расписание и восстановление. Ключ восстановления не помещается внутрь архива и должен храниться отдельно.

- в копию входят пользователи, диалоги, RAG, загрузки, состояние интеграций и автоматизаций, сертификаты, конфигурация и состояние моделей;
- веса локальных моделей по умолчанию не дублируются, но сохраняется их перечень;
- временные кэши и восстанавливаемые индексы не являются источником истины;
- для промышленной эксплуатации актуальная копия должна храниться вне сервера Студии;
- в Л-3 внешним хранилищем считается внутреннее автономное хранилище организации, а не облако.

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

38 Аварийное восстановление

Полная потеря виртуальной машины не должна требовать Интернет-доступа, если организация заранее сохранила автономный комплект программы, требуемые контейнерные образы, модели, последнюю резервную копию и ключ восстановления. Процедура восстановления должна регулярно проверяться на отдельном стенде.

11. Развернуть совместимую НАЙС.ОС CLOUD или иную квалифицированную российскую серверную ОС.
12. Установить подготовленную версию ИИ Студии из автономного комплекта.
13. Вернуть исходную конфигурацию развертывания и внутренние секреты из recovery bundle.
14. Восстановить проверенную .nsbackup.
15. Импортировать веса локальных моделей по сохранённому перечню.
16. Проверить пользователей, RAG, интеграции, автоматизации, сертификаты и активную модель.
17. Провести контроль внешних маршрутов и оформить протокол восстановления.

39 Локальный мониторинг

Эксплуатационная телеметрия собирается внутри контура: node-exporter и внутренние цели → Prometheus → системный монитор → административная панель. Браузер администратора не должен напрямую обращаться к Prometheus. Отсутствие внешней системы мониторинга не мешает базовой локальной диагностике.

- состояние служб;
- CPU, память и диск;
- история системных показателей;
- состояние локальной модели;
- доступность внутренних целей;
- состояние резервного копирования и обновления.

40 Журналирование и аудит

Журналы продукта, аудит интеграций и история административных операций хранятся локально. При необходимости они могут передаваться во внутреннюю SIEM организации. Для Л-2/Л-3 адрес SIEM должен находиться в разрешённом внутреннем сегменте.

Конфиденциальность журналов. Секреты, пароли, ключи и полное содержимое чувствительных полезных нагрузок не должны записываться в журнал в открытом виде. При экспортировании журналов следует применять правила классификации информации заказчика.

41 Подтверждение отсутствия внешней передачи данных



Рисунок 4 - Последовательность подтверждения отсутствия внешней передачи

Для Л-3 рекомендуется оформлять отдельный протокол сетевой изоляции. Доказательство должно быть воспроизводимым: оно фиксирует конфигурацию, период наблюдения, набор пользовательских сценариев и полученные сетевые следы.

42 Сетевые испытания локального режима

18. Зафиксировать IP-адреса сервера, шлюза, внутренних DNS/NTP и разрешённых внутренних сервисов.
19. Убедиться, что маршрут по умолчанию отсутствует либо блокируется межсетевым экраном в соответствии с режимом.
20. Запустить захват трафика на интерфейсе сервера и, по возможности, на пограничном устройстве.
21. Выполнить вход пользователя, диалог с локальной моделью, запрос к базе знаний, загрузку файла, внутреннюю интеграцию, резервное копирование и административную проверку.
22. Проверить DNS-запросы и установленные TCP/UDP-сессии.
23. Подтвердить отсутствие соединений к публичным адресам для Л-2/Л-3.
24. Сохранить pcap/журналы, вычислить контрольные суммы и приложить к протоколу.

```
ss -lntup
ip route
resolvectl status  # если используется systemd-resolved
tcpdump -i <интерфейс> -nn -w local-mode-check.pcap
```

Конкретный набор средств сетевого контроля определяется НАЙС.ОС CLOUD и политиками организации. Команды приведены как пример и не заменяют утверждённую методику испытаний.

43 Приёмочные испытания

Проверка	Ожидаемый результат
Запуск всех обязательных служб	Работоспособны, критических ошибок нет.
Вход локального пользователя	Выполняется без внешнего провайдера идентификации.
Локальная модель	Отвечает при отсутствующем Интернет-маршруте.
База знаний	Документ индексируется и используется локальной моделью.
Внутренняя интеграция	Соединяется только с утверждённым внутренним адресом.
Публичная интеграция в Л-2/Л-3	Недоступна/отключена.
Резервная копия	Создаётся и проходит проверку.
Восстановление на стенде	Данные восстанавливаются, внешние действия не повторяются самопроизвольно.
TLS	Рабочие места доверяют сертификату.
Сетевой контроль	Не выявляет неразрешённых внешних соединений.

44 Эксплуатация и административные операции

Администратор должен иметь локальный путь управления, не зависящий от внешних сервисов. Командный интерфейс ИИ Студии предоставляет проверку состояния, запуск/остановку, просмотр журналов, резервное копирование и аварийное восстановление.

```
./nicesoft.sh status
./nicesoft.sh health
./nicesoft.sh logs [служба]
./nicesoft.sh backup
./nicesoft.sh model-status
./nicesoft.sh web-search-check
```

В Л-2/Л-3 команды, проверяющие внешние сервисы, используются только если соответствующий сервис внутренний или явно разрешён. Например, проверка Яндекс Облака не является частью приёмки полностью изолированного контура.

45 Переход между режимами

Переход из Л-1 в Л-2/Л-3 должен рассматриваться как изменение архитектуры безопасности. Недостаточно только закрыть Интернет: необходимо удалить/отключить внешние поставщики моделей, внешние интеграции и автоматизации, подготовить локальные модели и внутренние источники данных, заменить публичные DNS/NTP/сертификаты и выполнить сетевые испытания.

Переход	Основные действия
Л-1 → Л-2	Отключить публичные интеграции; настроить внутренние DNS/NTP; заблокировать Интернет; перенести обновления во внутренний канал; квалифицировать внутренние сервисы.
Л-2 → Л-3	Удалить внешнюю маршрутизацию; подготовить автономные комплекты; регламентировать носители; обеспечить внутренний УЦ; провести доказательство отсутствия внешнего трафика.
Л-3 → Л-2	Разрешить строго определённые внутренние сети; повторно проверить правила межсетевого экрана.
Л-2 → Л-1	Утвердить перечень внешних сервисов; настроить прокси/разрешённый список; обновить оценку рисков и уведомление пользователей о потоках данных.

46 Ограничения и особые условия

- Полностью изолированный режим исключает использование облачной модели, если она физически находится за пределами контура.
- Публичный веб-поиск без внешней сети невозможен; вместо него применяются внутренние документы/индексы.
- Let's Encrypt без внешнего обмена недоступен; требуется внутренний УЦ или предварительная внешняя процедура.
- Обновление без Интернет-доступа требует предварительно подготовленного автономного комплекта.
- Лицензия конкретной локальной модели может запрещать определённые способы использования независимо от возможностей ИИ Студии.
- Качество ответа локальной модели зависит от выбранной модели, аппаратных ресурсов, контекста и данных, а не от самого факта локального режима.

47 Персональные данные, ГИС и КИИ

Локальный режим может быть полезным элементом архитектуры защиты персональных данных, государственных информационных систем и объектов КИИ, поскольку позволяет контролировать место обработки и сетевые потоки. Однако режим не заменяет обязательные меры конкретной системы.

- для персональных данных оператор определяет угрозы и реализует необходимые правовые, организационные и технические меры;
- для ГИС и иных систем, подпадающих под приказ ФСТЭК №117, требования реализуются на уровне всей информационной системы;
- для значимого объекта КИИ субъект создаёт систему безопасности объекта и выполняет применимые требования;
- сертифицированные средства защиты и СКЗИ применяются дополнительно, если они требуются нормативно или моделью угроз;
- документ о локальном режиме может использоваться как часть исходных данных для проектирования, но не является аттестатом соответствия.

48 Меры информационной безопасности

Мера	Л-1	Л-2	Л-3
Локальные учётные записи	Да	Да	Да
Ролевое разграничение	Да	Да	Да
Изоляция учётных данных интеграций	Да	Да	Да
TLS	Обязательно	Обязательно	Обязательно
Запрет исходящих соединений по умолчанию	Рекомендуется	Обязательно	Обязательно
Внутренний DNS/NTP	Рекомендуется	Обязательно	Обязательно
Подписанные обновления	Да	Да	Да
Автономная поставка	Опционально	Рекомендуется	Обязательно
Контроль переносимых носителей	По политике	По политике	Обязательно
Сетевые испытания отсутствия внешнего трафика	По политике	Рекомендуется	Обязательно

49 Отказоустойчивость и непрерывность

Локальный режим переносит ответственность за инфраструктурную доступность к заказчику. Для критичных внедрений следует обеспечить отказоустойчивость вычислительных ресурсов, дискового массива, электропитания, внутренних DNS/NTP, хранилища резервных копий и при необходимости внутреннего сервера моделей.

- регулярные проверенные резервные копии;
- внешнее относительно сервера Студии хранилище копий;
- хранение автономного комплекта последней поддерживаемой версии;
- резервный сервер/виртуальная инфраструктура по требованиям заказчика;
- документированный RTO/RPO;
- периодические тренировочные восстановления.

50 Вывод из эксплуатации

25. Создать финальную резервную копию, если данные должны храниться.
26. Экспортировать требуемые документы и сведения по политике организации.
27. Отозвать/удалить пользовательские учётные данные интеграций.
28. Удалить внешние токены и ключи в целевых системах.
29. Остановить ИИ Студию и исключить сервер из сети.
30. Уничтожить или передать на хранение локальные данные, модели и резервные копии в соответствии с регламентом.
31. Отозвать серверные сертификаты при необходимости.
32. Удалить правила межсетевого экрана, DNS и служебные записи.
33. Оформить акт вывода из эксплуатации и уничтожения/архивации данных.

51 Типовые архитектурные сценарии

Сценарий	Режим	Состав
Внутренний юридический помощник	Л-3	Локальная модель + локальная база договоров + внутренний WebDAV/SFTP; без Интернет.
ИИ-помощник ИТ-службы	Л-2	Локальная модель + Jira Data Center + Confluence Data Center + GitLab + PostgreSQL.
Корпоративный помощник с Яндекс AI	Л-1	Локальные данные/RAG + управляемая модель по явной политике + контролируемый внешний доступ.
Закрытый инженерный помощник	Л-2	Локальная модель + внутренняя техдокументация + внутренний GitLab + почта.
Изолированный контур гос/промышленной системы	Л-3	НАЙС.ОС CLOUD + локальная модель + внутренний УЦ + внутренние DNS/NTP + автономные обновления.

52 Требования для закупки и проектирования

При закупке локальной ИИ-платформы заказчик может использовать следующие функциональные требования как нейтральные критерии: возможность локальной установки, локальной модели, отсутствия обязательного внешнего облачного сервиса, локального RAG, внутреннего управления пользователями, резервного копирования, автономного обновления и документированного контроля сетевых потоков.

- поставка должна позволять эксплуатацию без постоянного подключения к Интернету;
- должна существовать схема полностью изолированного режима;
- программный продукт не должен требовать облачной аутентификации производителя для обычной работы;
- должен поддерживаться автономный импорт моделей и обновлений;
- должна быть возможность доказательной проверки отсутствия внешнего трафика;
- документация должна описывать состав локальных данных и внешние зависимости.

53 Техническая поддержка изолированного контура

Поддержка полностью изолированного контура не должна требовать постоянного удалённого доступа производителя. Диагностика может выполняться по обезличенным журналам, выгруженным отчётам и заранее согласованным диагностическим пакетам. При необходимости выезда специалиста условия доступа определяются режимом объекта.

- обновления передаются подписанным автономным комплектом;
- критические исправления могут поставляться отдельным автономным выпуском;
- секреты и пользовательские данные не должны включаться в диагностический пакет без явной необходимости;
- удалённый доступ включается только по решению заказчика и не является обязательным условием стандартной эксплуатации;
- SLA учитывает ограничения физического доступа и процедуры допуска на площадку.

54 Разделение ответственности

Сторона	Основные обязанности
НАЙС СОФТ	Поставка поддерживаемой версии, документации, подписанных обновлений/автономных комплектов, исправление дефектов продукта, описание внешних зависимостей и механизмов локального режима.
Заказчик	Сетевая изоляция, межсетевой экран, ОС и инфраструктура, физическая защита, внутренние DNS/NTP/УЦ, хранение резервных копий и ключей, квалификация режимов, соблюдение законодательства и внутренних политик.
Совместно	Приёмочные испытания, разбор инцидентов, планирование обновлений, проверка совместимости оборудования/ОС, определение перечня разрешённых внешних взаимодействий в Л-1.

Итоговый критерий. Если организация требует гарантированного отсутствия передачи данных во внешние сети, это должно подтверждаться одновременно конфигурацией ИИ Студии, сетевой архитектурой, правилами межсетевого экрана и результатами фактического сетевого наблюдения.

Приложение А. Сводная матрица режимов

Параметр	Л-1	Л-2	Л-3
Интернет-маршрут	Разрешён контролируемо	Отсутствует	Отсутствует физически/логически
Локальная модель	Да	Да	Да
Облачная модель	Допустима	Нет	Нет
Внутренние интеграции	Да	Да	Да
Публичные интеграции	Допустимы	Нет	Нет
Обновления	Онлайн/автономно	Внутреннее зеркало/автономно	Автономно
Модели	Онлайн/автономно	Внутреннее зеркало/автономно	Автономно
DNS	Корпоративный/внешний	Внутренний	Внутренний
NTP	Корпоративный/внешний	Внутренний	Внутренний/автономный
Сертификаты	Публичный/корпоративный УЦ	Корпоративный УЦ	Корпоративный/локальный УЦ
Резервные копии	Локальное/внешнее хранилище	Внутреннее хранилище	Изолированное хранилище
Сетевой протокол изоляции	Опционально	Рекомендуется	Обязательно

Приложение Б. Пример перечня разрешённых внешних соединений

Таблица является шаблоном. Фактический перечень утверждается владельцем системы и подразделением информационной безопасности.

Назначение	Имя/адрес	Порт	Режим	Основание
Внутренний DNS	dns1.example.local	53 TCP/UDP	Л-1/Л-2/Л-3	Разрешение имён
Внутренний NTP	ntp1.example.local	123 UDP	Л-1/Л-2/Л-3	Синхронизация времени
Внутренний GitLab	gitlab.example.local	443 TCP	Л-1/Л-2/Л-3	Интеграция
Корпоративная почта	mail.example.local	993/465 TCP	Л-1/Л-2/Л-3	IMAP/SMTP
Источник обновлений	studio.ncsgp.ru	443 TCP	Только Л-1	Проверка/получение обновлений
Реестр НАЙС СОФТ	registry.ncsgp.ru	443 TCP	Только Л-1	Получение собственных образов
Внешний поставщик модели	по договору	443 TCP	Только Л-1	Явно выбранная внешняя модель

Приложение В. Состав автономного комплекта поставки

- дистрибутив ИИ Студии версии 1.0.0;
- подписанный манифест выпуска;
- файл(ы) контрольных сумм;
- открытый ключ проверки подписи или доверенный набор ключей;
- собственные контейнерные образы НАЙС СОФТ с точными digest;
- необходимые сторонние контейнерные образы с точными digest;
- выбранные веса локальных моделей и их контрольные суммы;
- сведения о лицензиях моделей;
- SBOM программного выпуска;
- THIRD_PARTY/перечень сторонних лицензий;
- руководство по установке;
- описание обновлений;
- данный документ;
- шаблон протокола импорта;
- при необходимости - пакет исправления безопасности и бюллетень.

Реквизит комплекта	**Значение**
Версия продукта	1.0.0
Идентификатор выпуска	_____
Дата формирования	_____
SHA-256 комплекта	_____
Подпись проверена	Да / Нет
Носитель №	_____
Ответственный за перенос	_____
Дата ввода в контур	_____

Приложение Г. Протокол приёмки локального режима

Пункт	Результат/значение
Организация	
Площадка/сегмент	
Версия ИИ Студии	1.0.0
Операционная система	
Выбранный режим	Л-1 / Л-2 / Л-3
Локальная модель	
Внешние модели	Отсутствуют / перечень
Внутренние интеграции	
Внешние интеграции	Отсутствуют / перечень
DNS	
NTP	
TLS/УЦ	
Политика исходящих соединений	
Резервная копия проверена	Да / Нет
Сетевые испытания выполнены	Да / Нет
Неразрешённые внешние соединения	Не выявлены / описание
Дата испытаний	
Ответственный	
Заключение	

Приложение Д. Протокол подтверждения отсутствия внешней передачи

Протокол рекомендуется применять для Л-3 и при необходимости для Л-2. Он должен сопровождаться исходными журналами или их защищёнными копиями.

Параметр	Содержание
Период наблюдения	
Интерфейсы наблюдения	
Средство захвата трафика	
Контроль DNS	
Контроль маршрутов	
Выполненные пользовательские сценарии	
Выполненные административные сценарии	
Количество внешних DNS-запросов	0 / иное
Количество соединений к публичным адресам	0 / иное
Разрешённые внутренние соединения	
SHA-256 файла сетевого захвата	
SHA-256 экспортированных журналов	
Вывод	Неразрешённая внешняя передача не обнаружена / обнаружена
Подпись ответственного	

Приложение Е. Контрольный лист эксплуатации

№	Контроль	Отметка
1	Режим экземпляра указан в эксплуатационном паспорте.	☐
2	Состав разрешённых внешних соединений утверждён.	☐
3	Для Л-2/Л-3 публичный Интернет заблокирован.	☐
4	Используются только утверждённые DNS и NTP.	☐
5	Сертификат действителен и доверен рабочим станциям.	☐
6	Активная модель соответствует выбранному режиму.	☐
7	Внешние поставщики моделей отключены в Л-2/Л-3.	☐
8	Публичные интеграции отключены в Л-2/Л-3.	☐
9	Веб-поиск не обращается в Интернет в Л-2/Л-3.	☐
10	Резервные копии создаются по расписанию.	☐
11	Хотя бы одна актуальная копия хранится вне сервера.	☐
12	Ключ восстановления хранится отдельно от резервной копии.	☐
13	Проверка резервной копии выполняется регулярно.	☐
14	Есть автономный комплект последней поддерживаемой версии.	☐
15	Есть автономные копии требуемых моделей.	☐
16	Контрольные суммы и подписи артефактов проверены.	☐
17	Журналы и аудит доступны локально.	☐
18	Проводится контроль свободного места.	☐
19	Проводится контроль состояния модели/GPU.	☐
20	Для Л-3 периодически повторяются сетевые испытания.	☐
21	Изменение режима оформляется отдельным изменением конфигурации.	☐
22	Список внутренних интеграций поддерживается актуальным.	☐
23	Учетные данные увольняемых пользователей отзываются.	☐
24	Сроки сертификатов контролируются.	☐
25	План аварийного восстановления проверен на стенде.	☐

Приложение Ж. Нормативные и официальные источники

Официальный адрес ИИ Студии: открыть официальный источник

НАЙС.ОС: открыть официальный источник

Реестровая запись НАЙС.ОС CLOUD №30128: открыть официальный источник

ГОСТ Р 56939-2024: открыть официальный источник

ГОСТ Р 72514-2026: открыть официальный источник

ГОСТ Р 72515-2026: открыть официальный источник

152-ФЗ, статья 19: открыть официальный источник

187-ФЗ: открыть официальный источник

Приказ ФСТЭК №117 от 11.04.2025: открыть официальный источник

Актуальность. Перед применением требований в регулируемой системе следует проверить действующую редакцию нормативных документов на дату проектирования и ввода в эксплуатацию.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов	Всего листов	№ документа	Входящий №	Подпись	Дата