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

# ПРОГРАММНЫЙ КОМПЛЕКС «НАЙС СОФТ ИИ СТУДИЯ»

версия 1.0.0

# ОПИСАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НССГ.10001-01 95 01-ЛУ

Лист утверждения

Красногорск
2026

Утвержден НССГ.10001-01 95 01-ЛУ

**ООО «НАЙС СОФТ ГРУПП»**

# ПРОГРАММНЫЙ КОМПЛЕКС «НАЙС СОФТ ИИ СТУДИЯ»

Версия 1.0.0

# ОПИСАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НССГ.10001-01 95 01

Листов 64

Красногорск
2026

## АННОТАЦИЯ

Настоящий документ описывает архитектуру и механизмы информационной безопасности программного комплекса «Найс Софт ИИ Студия» версии 1.0.0, границы доверия, защищаемые активы, модель угроз, управление идентификацией и доступом, защиту учётных данных интеграций, сетевую безопасность, безопасное применение моделей искусственного интеллекта, защиту автоматизаций, резервного копирования и обновлений, а также требования безопасной эксплуатации в локальном, закрытом и полностью изолированном контуре.

Документ предназначен для подразделений информационной безопасности, ИТ-архитекторов, системных администраторов, специалистов по защите информации, владельцев информационных систем, закупочных и экспертных комиссий. Он применяется совместно с паспортом продукта, функциональным описанием, руководствами, системными требованиями, матрицей совместимости, описанием обновлений и политикой жизненного цикла.

**Граница заявления**

ИИ Студия содержит собственные прикладные механизмы защиты, однако настоящий документ не является сертификатом ФСТЭК России, ФСБ России, заключением об аттестации или подтверждением соответствия конкретной информационной системы требованиям регуляторов. Необходимость сертифицированных средств защиты определяется категорией и моделью угроз целевого контура заказчика.

## СТАТУС И ОБЛАСТЬ ПРИМЕНЕНИЯ

Документ описывает базовую защищённую архитектуру продукта и рекомендации по её включению в систему защиты информации заказчика. Там, где требования законодательства зависят от вида информационной системы, уровня защищённости персональных данных, категории значимости объекта КИИ или класса защищённости, документ указывает условия применимости и не подменяет моделирование угроз и проектирование системы защиты конкретного заказчика.

## НОРМАТИВНЫЕ И СПРАВОЧНЫЕ ОСНОВАНИЯ

| Документ | Применение |
|---|---|
| Федеральный закон №149-ФЗ, статья 16 | Правовые, организационные и технические меры защиты информации от неправомерного доступа, уничтожения, изменения, блокирования, копирования, предоставления и распространения. |
| Федеральный закон №152-ФЗ, статья 19 | Меры обеспечения безопасности персональных данных при обработке в информационных системах. |
| Постановление Правительства РФ №1119 | Уровни защищённости и требования к защите персональных данных в ИСПДн. |
| Приказ ФСТЭК России №21 | Состав и содержание организационных и технических мер защиты персональных данных. |
| Приказ ФСТЭК России №117 от 11.04.2025, ред. 08.05.2026 | Требования о защите информации в ГИС и иных информационных системах государственных органов, предприятий и учреждений; действует вместо утратившего силу приказа №17. |
| Методический документ ФСТЭК России от 12.04.2026 | Состав и содержание мероприятий и мер по защите информации в информационных системах. |
| Федеральный закон №187-ФЗ и приказ ФСТЭК №239 | Требования, применимые при использовании продукта в составе значимых объектов критической информационной инфраструктуры. |
| ГОСТ Р 56939-2024 | Безопасная разработка программного обеспечения и устранение уязвимостей. |
| ГОСТ Р 59898-2021 | Оценка качества систем искусственного интеллекта, включая надёжность, безопасность и функциональность. |
| ГОСТ Р 72514-2026 | Оценка воздействия системы искусственного интеллекта и документирование воздействия. |
| ГОСТ Р 72515-2026 | Прозрачность систем искусственного интеллекта и информационные элементы для заинтересованных сторон. |

Официальные сведения о нормативных документах приведены в приложении Ж. При применении ИИ Студии в регулируемом контуре заказчик обязан проверить актуальную редакцию применимых требований на дату проектирования и аттестации.

# СОДЕРЖАНИЕ

1 Общие положения 9
2 Термины и сокращения 10
3 Цели информационной безопасности 11
4 Принципы защищённой архитектуры 12
5 Архитектура доверия и границы безопасности 13
6 Защищаемые активы 14
7 Категории обрабатываемой информации 15
8 Модель угроз 16
9 Нарушители и сценарии атак 17
10 Управление идентификацией 18
11 Аутентификация и сеансы 19
12 Управление пользователями и жизненным циклом учётной записи 20
13 Ролевая модель и разграничение доступа 21
14 Защита административного контура 22
15 Защита секретов и ключевого материала 23
16 Изоляция учётных данных интеграций 24
17 Прикладные учётные данные 25
18 Карантин устаревших учётных данных 26
19 Безопасность внешних поставщиков моделей 27
20 Защита от SSRF и повторной привязки DNS 28
21 Политика перенаправлений и TLS внешних соединений 29
22 Безопасность моделей искусственного интеллекта 30
23 Защита от внедрения вредоносных инструкций 31
24 Безопасность RAG и документов 32
25 Вызов инструментов и подтверждение действий 33
26 Безопасность автоматизаций 34
27 Сетевая архитектура и сегментация 35
28 TLS, сертификаты и домены 36
29 Защита данных при хранении 37
30 Журналирование и аудит 38
31 Мониторинг безопасности 39
32 Резервное копирование и восстановление 40
33 Безопасность обновлений и цепочки поставки 41
34 Управление уязвимостями 42
35 Безопасная разработка и выпуск 43
36 Сторонние компоненты и SBOM 44
37 Локальный и закрытый режим 45
38 Полностью изолированный контур 46
39 Персональные данные 47
40 Государственные информационные системы 48
41 Критическая информационная инфраструктура 49
42 Криптографическая защита и сертифицированные средства 50
43 Реагирование на инциденты 51
44 Восстановление и непрерывность 52
45 Обязанности администратора и заказчика 53
46 Остаточные риски и ограничения 54
47 Проверка защищённости и приёмка 55
48 Поддержание безопасности в эксплуатации 56
Приложение А - Каталог угроз и мер 56
Приложение Б - Матрица потоков данных 58
Приложение В - События аудита 59
Приложение Г - Контрольный лист ИБ 60
Приложение Д - Контрольный лист закрытого контура 61
Приложение Е - Матрица нормативного соответствия 62

Приложение Ж - Официальные источники 63
Лист регистрации изменений 64

# 1 Общие положения

Информационная безопасность ИИ Студии строится по принципу нескольких независимых защитных границ. Пользовательская сессия, права доступа, принадлежность учётных данных внешней системы, возможность выполнения конкретного действия и сетевой доступ к внешнему ресурсу проверяются независимо друг от друга. Компрометация или ошибочная настройка одной границы не должна автоматически предоставлять полномочия другой.

Безопасность продукта рассматривается как совместная ответственность: НАЙС СОФТ отвечает за механизмы и свойства программного комплекса, а заказчик - за безопасность операционной системы, сети, аппаратной платформы, учётных записей администраторов, правила обработки данных и выбор допустимых внешних сервисов.

## 2 Термины и сокращения

| Термин | Определение |
|---|---|
| Владелец учётных данных | Аутентифицированный пользователь, чья внешняя учётная запись должна использоваться при обращении к ресурсу. |
| Прикладные учётные данные | Секреты, принадлежащие экземпляру Студии, например технический токен приложения; они хранятся отдельно от пользовательских секретов. |
| Профиль подключения | Именованная конфигурация подключения пользователя к внешней системе. |
| Шлюз интеграций | Внутренний компонент, который публикует разрешённые действия и применяет правила доступа перед вызовом внешней системы. |
| Реестр моделей | Хранилище поставщиков, физических моделей, подтверждённых возможностей и безопасных параметров подключения. |
| RAG | Получение контекста из локальных источников знаний для формирования ответа модели. |
| SSRF | Попытка заставить сервер выполнить сетевой запрос к непредусмотренному внутреннему или служебному адресу. |
| Повторная привязка DNS | Атака с изменением адреса, в который разрешается доменное имя, между проверкой политики и фактическим соединением. |
| HITL | Подтверждение потенциально изменяющего действия человеком перед выполнением. |
| SBOM | Машиночитаемый перечень программных компонентов поставки. |

## 3 Цели информационной безопасности

- сохранение конфиденциальности пользовательских данных, секретов, документов и истории работы;
- сохранение целостности данных, конфигурации, ролей, политик, моделей и результатов автоматизаций;
- поддержание доступности критических служб в пределах инфраструктурных возможностей;
- невозможность использования учётных данных одного пользователя другим пользователем или администратором без отдельного предусмотренного механизма;
- контроль изменяющих действий, выполняемых моделью или автоматизацией;
- минимизация сетевого доступа внутренних служб и внешних поставщиков;
- воспроизводимая цепочка поставки и проверяемое обновление;
- обнаруживаемость административных и интеграционных действий посредством аудита;
- сохранение возможности автономной работы без передачи данных внешним поставщикам.

# 4 Принципы защищённой архитектуры

| Принцип | Реализация |
|---|---|
| Минимальные полномочия | Внутренние сервисы получают только необходимые сети, каталоги и секреты; административные операции дополнительно проверяются на сервере. |
| Разделение полномочий и личности | Право выполнить действие и учётная запись, от имени которой действие будет выполнено, проверяются независимо. |
| Запрет неявного повышения привилегий | Роль ADMIN не превращается в пользовательский секрет и не передаётся автоматизации как пользовательская внешняя идентичность. |
| Отказ по умолчанию | Неизвестные действия, некорректные владельцы, неподтверждённые соединения и нарушенные политики завершаются отказом либо запросом подтверждения. |
| Защита по нескольким уровням | Сетевые ограничения, серверная авторизация, шифрование секретов, аудит и проверка конечного состояния дополняют друг друга. |
| Минимизация раскрытия | Браузеру и журналам не передаются пароли, токены, закрытые ключи, тела доверенных сертификатов и ответы поставщика, если они не нужны пользователю. |

# 5 Архитектура доверия и границы безопасности




*Рисунок 1 - Архитектура доверия ИИ Студии*

Пользовательская сеть заканчивается на обратном посреднике. Базы данных, служба сертификатов, мониторинг, резервное копирование, реестр моделей и внутренние административные службы не должны иметь собственных публичных портов. Внешний сетевой обмен инициируется только теми компонентами, которым он функционально необходим.

# 6 Защищаемые активы

| Актив | Критичность | Основные меры |
|---|---|---|
| Учётные записи и роли | Высокая | Серверная авторизация, блокирование, отзыв сессий, защита последнего администратора. |
| Учётные данные интеграций | Критическая | AES-256-GCM, привязка к владельцу, отдельный домен прикладных секретов, отсутствие возврата в браузер. |
| Ключи экземпляра и внутренние секреты | Критическая | Генерация при установке, ограничение доступа к файлам конфигурации, включение в зашифрованный аварийный комплект. |
| Документы и база знаний | Высокая | Локальное хранение, права пользователя, управление передачей внешней модели. |
| Реестр поставщиков моделей | Высокая | Шифрование секретов, сетевые политики, TLS, аудит. |
| Резервные копии | Критическая | Шифрование, контроль целостности, отдельный ключ восстановления, проверка восстановления. |
| Механизм обновлений | Критическая | Ed25519, SHA-256, точные контрольные суммы образов, резервирование и контроль работоспособности. |
| Журналы аудита | Высокая | Запрет секретов в событиях, контроль доступа, сохранение хронологии административных действий. |

## 7 Категории обрабатываемой информации

- общедоступные данные и документы;
- служебная информация организации;
- коммерческая тайна и иная конфиденциальная информация при наличии оснований и утверждённых правил обработки;
- персональные данные, если заказчик использует Студию в составе ИСПДн;
- учётные данные, токены и ключи интеграций;
- программный код и репозитории;
- технические журналы, сведения об инфраструктуре и метаданные;
- запросы пользователей, ответы моделей и результаты автоматизаций.

**Передача внешней модели**

Любая внешняя или управляемая модель образует самостоятельную внешнюю границу. Заказчик обязан определить, какие категории информации разрешено передавать выбранному поставщику. Локальный режим позволяет исключить такую передачу для модельного вывода.

# 8 Модель угроз

Модель угроз продукта охватывает угрозы со стороны внешнего нарушителя, обычного пользователя, привилегированного пользователя, скомпрометированного внешнего сервиса, вредоносного документа, вредоносной модели или поставщика зависимости. Конкретная модель угроз информационной системы заказчика должна дополнительно учитывать инфраструктуру, назначение системы, данные и требования регулятора.

| Группа угроз | Примеры |
|---|---|
| Нарушение идентификации | Кража сессии, попытка использовать чужую учётную запись, обход блокировки. |
| Повышение полномочий | Подмена роли, попытка использовать ADMIN как владельца пользовательского секрета. |
| Кража секретов | Извлечение токена из браузера, журнала, БД, резервной копии или ошибки. |
| Сетевые атаки | SSRF, повторная привязка DNS, перенаправление с утечкой Authorization, обращение к служебным адресам метаданных. |
| ИИ-атаки | Внедрение вредоносных инструкций, подмена контекста, попытка модели инициировать запрещённое действие. |
| Автоматизации | Запуск от неверного владельца, использование старого разрешения после ротации секрета, рекурсивное самоуправление. |
| Цепочка поставки | Подмена образа, манифеста, обновления или сторонней зависимости. |
| Доступность | Истощение CPU/RAM/GPU, зависший внешний поток, большая нагрузка RAG, отказ внешней системы. |

# 9 Нарушители и сценарии атак

| Нарушитель | Возможности | Основная защита |
|---|---|---|
| Внешний неаутентифицированный | Сетевой доступ к опубликованному HTTPS интерфейсу | TLS, обратный посредник, отсутствие публичных портов внутренних служб. |
| Обычный пользователь | Доступ к собственному интерфейсу, документам, интеграциям и разрешённым действиям | Серверный контроль пользователя, ролей и владельца секрета. |
| Администратор Студии | Управление пользователями, моделями, интеграциями и настройками | Разделение пользовательских и прикладных секретов; отсутствие API чтения чужого секрета. |
| Администратор ОС | Полный контроль хоста при наличии root | Организационная защита, ОС, журналирование; этот уровень находится выше границы приложения. |
| Скомпрометированный внешний сервис | Возвращает вредоносные данные или меняет API | TLS, ограничение действий, подтверждение записи, обработка внешних данных как недоверенных. |
| Вредоносный документ | Содержит инструкции для модели | Разделение контента и полномочий, политики инструментов, подтверждение изменяющих действий. |

## 10 Управление идентификацией

Источником истины для локальных пользователей, групп и ролей остаётся штатная модель идентичностей Студии; НАЙС СОФТ не создаёт отдельную параллельную базу полномочий. Состояния блокирования, отзыва сессий и дополнительные политики хранятся отдельно и применяются сервером при каждом защищённом запросе.

Архитектура предусматривает источники идентичности LDAP/AD/OIDC/SAML и другие федеративные способы, однако фактическая поддержка конкретного способа определяется матрицей функциональности версии 1.0.0. Наличие поля источника идентичности не означает автоматическое заявление поддержки всех каталогов.

## 11 Аутентификация и сеансы

- минимальная длина локального пароля в базовой конфигурации - 12 символов;
- восстановление пароля через публичную саморегистрацию по умолчанию отключено; административное восстановление выполняется штатным механизмом жизненного цикла;
- браузерный код НАЙС СОФТ не сохраняет bearer-токен в localStorage/sessionStorage;
- блокирование пользователя и отзыв сессий проверяются серверным механизмом контроля и применяются к уже выданным сессиям;
- смена основной роли отзывает ранее выданные сессии;
- самоблокирование, самоудаление, самопонижение администратора и потеря последнего активного ADMIN запрещены сервером.

**Многофакторная аутентификация**

Встроенная локальная модель 1.0.0 не должна заявляться как самостоятельное сертифицированное средство многофакторной аутентификации. При требовании MFA рекомендуется применять поддерживаемый внешний контур идентификации либо инфраструктурные средства доступа.

## 12 Управление пользователями и жизненным циклом учётной записи

Административные изменения выполняются через отдельную серверную службу, которая повторно проверяет сессию и роль ADMIN. Скрытие вкладки интерфейса не используется как средство авторизации.

- браузерный API возвращает только разрешённые поля и не выдаёт пароль, хеш пароля, токен обновления или секрет подключения;
- изменение пользователя подтверждается повторным чтением фактического состояния, а не только кодом HTTP 2xx;
- удаление проверяется последующим отсутствием объекта;
- изменение состава группы проверяется по свежему составу;
- сброс пароля не создаёт новую базу и при сомнительном состоянии завершается отказом.

## 13 Ролевая модель и разграничение доступа

У пользователя имеется основная роль, членство в группах и отдельные разрешения. Системные роли USER и ADMIN защищены от удаления и недопустимого изменения. Права функций Студии не смешиваются с владением внешними учётными данными.

| Проверка | Где выполняется | Результат при отказе |
|---|---|---|
| Аутентифицирован ли пользователь | Обратный посредник / штатный контур сессий | 401/переход к входу |
| Имеет ли пользователь право функции | Серверная политика роли/разрешения | 403/отказ действия |
| Принадлежит ли секрет пользователю | Разрешитель подключений (Connection Resolver) | credential_owner_mismatch / отсутствие подключения |
| Разрешено ли конкретное действие | Политика инструмента/шлюз интеграций | отказ либо запрос подтверждения |
| Разрешена ли сеть назначения | Сетевая политика поставщика | блокировка соединения |

## 14 Защита административного контура

- административные операции повторно проверяют роль на сервере;
- службы управления пользователями, сертификатами, резервными копиями, мониторингом и обновлениями не публикуют собственные административные порты наружу;
- внутренние службы используют отдельные служебные ключи и внутренние сети;
- пароль или токен пользователя не должен возвращаться административному интерфейсу;
- операции удаления, отзыва и изменения безопасности требуют явной административной последовательности и проверяемого конечного состояния.

## 15 Защита секретов и ключевого материала

Секреты приложения генерируются при инициализации экземпляра и используются отдельными службами по назначению. К ним относятся ключи шифрования ConnectionStore, секреты сессий, внутренние токены служб, пароли внутренних БД, ключ резервного копирования, ключи шлюзов и служебные токены.

- секреты не должны храниться в исходном коде и публичных репозиториях;
- файл конфигурации с секретами должен быть доступен только уполномоченному администратору ОС;
- значения CHANGE_ME недопустимы в рабочей установке;
- ротация прикладного секрета не должна открывать старое значение интерфейсу;
- ключ восстановления резервной копии хранится отдельно от сервера Студии.

# 16 Изоляция учётных данных интеграций




*Рисунок 2 - Изоляция пользовательских и прикладных учётных данных*

ConnectionStore v2 идентифицирует пользовательское подключение комбинацией connector_id, owner_user_id и profile_id. Секрет шифруется AES-256-GCM. В дополнительные аутентифицируемые данные включаются идентификатор коннектора, владелец, профиль и способ авторизации; прямое изменение владельца или профиля в базе приводит к ошибке аутентификации шифротекста.

Закрытые метаданные пользователя - имя профиля, адрес сервера, база, бакет, имя пользователя - могут храниться отдельно в зашифрованном виде. Публичное представление подключения не содержит расшифрованного секрета.

Для отслеживания ротации и привязки автоматизаций используется HMAC-SHA-256 отпечаток по владельцу и секретному материалу. Отпечаток пригоден для проверки изменения секрета, но не является его открытым хешем.

## 17 Прикладные учётные данные

Секреты приложения экземпляра - например технический токен бота или OAuth-клиент приложения - хранятся отдельно в AppCredentialStore. Для них используется отдельный домен аутентифицируемых данных, поэтому шифротекст пользовательского ConnectionStore нельзя перенести в прикладное хранилище и получить корректную расшифровку.

**Разделение идентичностей**

Техническая учётная запись приложения может обеспечивать соединение со службой, но не определяет владельца пользовательского ресурса. Например, токен бота не должен заменять привязку получателя сообщения.

## 18 Карантин устаревших учётных данных

Устаревшие системные, групповые или глобальные подключения без доказуемого владельца не назначаются администратору или произвольному пользователю при миграции. Они перемещаются в карантин, недоступный рабочему разрешению соединений.

- карантин сохраняет шифротекст и служебные сведения для контролируемого аварийного восстановления;
- рабочий код карантина не имеет интерфейса расшифрования секрета;
- обычный откат версии не восстанавливает старую базу общих секретов;
- возвращение к старому среда выполнения завершается отсутствием подключения, а не восстановлением общего системного секрета.

## 19 Безопасность внешних поставщиков моделей

Управление внешним поставщиком выполняется через административный серверный интерфейс. Секрет поставщика не включается в ответы GET и отображается только как факт настройки и безопасная маска. Проверка соединения выполняется сервером с ограничениями времени и размера ответа.

| Механизм | Политика |
|---|---|
| Протокол | Для публичной сети - HTTPS; HTTP допускается только в явно выбранном частном режиме локальной сети/Docker. |
| DNS | Все разрешённые адреса проверяются политикой до соединения. |
| Соединение | Открывается к уже проверенному IP; HTTP Host и TLS SNI сохраняют исходное имя. |
| Перенаправления | Не выполняются. |
| TLS | Проверка сертификата обязательна; verify=false отсутствует; поддерживается корпоративный CA. |
| Минимальная версия TLS для проверки | TLS 1.2. |
| Ответ проверки | Ограничение 1 МиБ и 30 секунд; тело ответа не сохраняется в журнале. |

## 20 Защита от SSRF и повторной привязки DNS

В режиме публичного поставщика разрешаются только глобально маршрутизируемые адреса. Частные адреса, адреса обратной петли, локальные канальные, многоадресные, неопределённые, зарезервированные адреса и адреса служб метаданных облачной среды блокируются. В частном режиме администратор может разрешить RFC1918/ULA и Docker-сети, но адреса обратной петли, локальные канальные адреса и адреса служб метаданных остаются запрещёнными.

Защита от повторной привязки DNS строится на единой операции: имя разрешается один раз, все полученные адреса проверяются политикой, выбирается проверенный IP и TCP-соединение открывается именно к нему. Повторное разрешение между проверкой и соединением не используется.

## 21 Политика перенаправлений и TLS внешних соединений

HTTP 301/302/303/307/308 при проверке поставщика не следуются. Это исключает перенос Authorization или API-ключа с разрешённого origin на иной адрес.

Для корпоративного центра сертификации загружается PEM-сертификат; сервер проверяет его корректность и сохраняет отдельно от общих метаданных поставщика. В интерфейс возвращается отпечаток SHA-256 и признак настройки, но не тело сертификата или секрет авторизации.

## 22 Безопасность моделей искусственного интеллекта

Модель рассматривается как недоверенный вероятностный вычислительный компонент: её ответ не является командой операционной системе и не получает полномочий сам по себе. Структурные возможности модели - вызов инструментов, форматированный ответ, изображения и другие - фиксируются в Реестре моделей по результатам проверки.

- неподтверждённая возможность не должна автоматически считаться доступной;
- если модель не поддерживает обязательный вызов инструментов, запрос завершается локальным отказом вместо скрытого обхода политики;
- маршрутизатор не должен скрытно подменять модель только ради обхода структурной политики;
- выход модели должен проверяться прикладным кодом перед изменяющим действием.

## 23 Защита от внедрения вредоносных инструкций

Текст веб-страницы, письма, документа, базы знаний или ответа внешнего API считается данными, а не доверенной системной политикой. Он может содержать инструкции, направленные на изменение поведения модели, раскрытие секретов или выполнение действий.

- секреты интеграций не помещаются в контекст модели как открытый текст;
- разрешение действия проверяется сервером независимо от текста диалога;
- неизвестное действие требует подтверждения либо блокируется;
- изменяющие действия через шлюз интеграций приостанавливаются для подтверждения человеком в соответствии с политикой;
- прямые диагностические облачные интерфейсы ограничены фиксированным набором чтения и дополнительно отвергают запись;
- результат RAG или веб-поиска не может изменить роль пользователя или владельца учётных данных.

**Остаточный риск**

Невозможно гарантировать, что генеративная модель никогда не интерпретирует вредоносный текст ошибочно. Поэтому критическая защита строится вне модели - в серверной авторизации, политике инструментов, изоляции секретов и подтверждении изменяющих действий.

## 24 Безопасность RAG и документов

Документы, загруженные пользователем или полученные из внешней системы, должны считаться недоверенным содержимым. Индексация и извлечение фрагментов не предоставляют документу дополнительных полномочий.

- доступ к базе знаний определяется пользовательским контекстом и конфигурацией Студии;
- документ не может самостоятельно выбрать внешний профиль подключения;
- данные RAG, передаваемые внешней модели, считаются передачей информации внешнему получателю и должны соответствовать политике заказчика;
- в закрытом режиме RAG и модель могут полностью оставаться внутри локального контура;
- для особо чувствительных данных рекомендуется отдельный набор знаний и отдельная политика моделей/интеграций.

## 25 Вызов инструментов и подтверждение действий

Политика инструментов делит действия на безопасные операции чтения, операции, требующие подтверждения, и запрещённые действия. Неизвестный идентификатор не считается безопасным и переводится в режим запроса подтверждения.

| Класс | Поведение |
|---|---|
| Чтение | Может выполняться автоматически при наличии права пользователя и корректного подключения. |
| Изменение | Приостанавливается для явного подтверждения, если политика не предусматривает более строгий запрет. |
| Административное изменение | Дополнительно требует ADMIN и предусмотренной процедуры. |
| Неизвестное действие | Не выполняется автоматически; требуется ручная проверка. |
| Разрушительное действие, не опубликованное модели | Отсутствует из перечня действий, доступных модели и выполняется только человеком через отдельный административный интерфейс. |

## 26 Безопасность автоматизаций

Авторитетной идентичностью автоматизации является сохранённый владелец, а не пользователь или администратор, который нажал кнопку запуска. Перед выполнением заголовки пользователя формируются из владельца, а роль сбрасывается до USER. Административное право инициатора не наследуется фоновым сценарием.

- автоматизация без владельца не запускается;
- привилегированная автоматизация требует неизменяемого разрешения, привязанного к конкретному действию и конкретному подключению;
- ротация секрета, замена профиля или изменение политики делает старое разрешение недействительным и отключает автоматизацию;
- старые разрешения не повышаются автоматически до новой схемы;
- новая автоматизация создаётся выключенной и включается отдельным действием;
- встроенный шаг CODE не имеет fetch, Node.js API, секретов поставщиков или внутренних служебных токенов;
- условия выполняются декларативными операторами, без eval/new Function;
- управление automation.* запрещено внутри собственных шагов автоматизации, что предотвращает рекурсивное самоуправление.

## 27 Сетевая архитектура и сегментация

Внутренние контейнерные сети разделяют пользовательский контур, автоматизации, резервное копирование и служебные компоненты. Для отдельных операций используются сети с internal=true, не имеющие внешнего маршрута. Базы данных и внутренние административные службы не должны публиковаться на интерфейс хоста без отдельной проектной необходимости.

| Компонент | Публичный доступ | Примечание |
|---|---|---|
| Обратный посредник | Да, HTTPS | Единая внешняя точка входа. |
| MongoDB/PostgreSQL/Redis | Нет | Только внутренние сети. |
| Prometheus/node_exporter/system-monitor | Нет | Сводка доступна через административный шлюз. |
| Служба сертификатов | Нет | Операции через внутренний защищённый интерфейс. |
| Служба резервного копирования | Нет | Каталог резервных копий и внутренние БД доступны только службе. |
| Служба обновления | Нет | Административное управление через шлюз. |

## 28 TLS, сертификаты и домены

При чистой установке создаётся локальный центр доверия и серверный сертификат для шифрования соединения. Для производственной эксплуатации рекомендуется доменное имя и сертификат корпоративного центра доверия либо публично доверенного удостоверяющего центра.

- закрытый ключ собственного сертификата не возвращается административным API и не показывается браузеру;
- перед установкой проверяется соответствие открытого и закрытого ключа и срок действия сертификата;
- предыдущий комплект сохраняется для контролируемого возврата;
- порт HTTP при выпуске публичного сертификата обслуживает только путь проверки права на домен; прочие запросы получают отказ;
- операции с сертификатами вынесены в отдельную внутреннюю службу с правом записи в TLS-хранилище.

## 29 Защита данных при хранении

Защита данных при хранении строится на сочетании прав ОС, изоляции внутренних сетей, шифрования наиболее чувствительных секретов и зашифрованного резервирования. Не все прикладные базы полностью шифруются самой Студией на уровне файлов; при нормативном требовании полного шифрования диска это реализуется средствами операционной системы или инфраструктуры заказчика.

| Данные | Механизм |
|---|---|
| Пользовательские секреты интеграций | AES-256-GCM с привязкой к владельцу и профилю. |
| Секреты реестра поставщиков моделей | AES-256-GCM. |
| Резервный архив | AES-256-CTR + HMAC-SHA256, ключ выводится из отдельного 256-битного ключа восстановления. |
| Пароли внутренних БД и служебные ключи | Секретная конфигурация экземпляра, защищаемая правами ОС и резервным архивом. |
| Документы/история/БД | Права ОС, изолированные сервисы; при необходимости - шифрование диска/тома инфраструктурой заказчика. |

## 30 Журналирование и аудит

Аудит предназначен для подтверждения административных и интеграционных действий без превращения журнала в хранилище секретов. События управления поставщиками моделей, подключениями, пользователями, автоматизациями и обновлениями фиксируются с идентификатором действия и временем.

- аудит поставщика модели не содержит токен/API key, Authorization, тело доверенного CA или тело ответа поставщика;
- операции ConnectionStore не возвращают секрет в публичное представление;
- для расследования сохраняются безопасные идентификаторы владельца, действия, профиля и результата;
- внешние данные высокой чувствительности не должны без необходимости записываться в диагностический журнал;
- сроки хранения и централизованный сбор журнала определяются политикой заказчика.

## 31 Мониторинг безопасности

Встроенный мониторинг использует Prometheus и системные источники, но не публикует интерфейс Prometheus и node_exporter пользователям. Административный интерфейс получает агрегированную сводку через внутреннюю службу. Для реестра моделей собираются показатели проверок, маршрутизации и ошибок без секретных или высококардинальных меток.

Рекомендуется интегрировать критические события Студии с внешней системой мониторинга или SIEM заказчика, если такая система предусмотрена проектом защиты информации.

## 32 Резервное копирование и восстановление

Резервная копия формата .nsbackup шифруется AES-256-CTR, целостность всего шифротекста защищается HMAC-SHA256. Ключи выводятся из уникального 256-битного ключа восстановления экземпляра. Ключ восстановления не записывается в архив и должен храниться отдельно от сервера.

- восстановление проверяет целостность архивов и согласованность БД;
- живые SQLite БД снимаются согласованным Backup API, а не простым копированием WAL-файлов;
- после восстановления реестра моделей выполняется PRAGMA quick_check;
- очередь автоматизаций не восстанавливается, чтобы старое задание не повторило внешний побочный эффект;
- запуски, которые на момент копии находились в ожидании или выполнялись, переводятся в состояние ошибки и не возобновляются автоматически;
- текущие сетевые файлы запуска не заменяются молча при восстановлении из работающей системы.

# 33 Безопасность обновлений и цепочки поставки

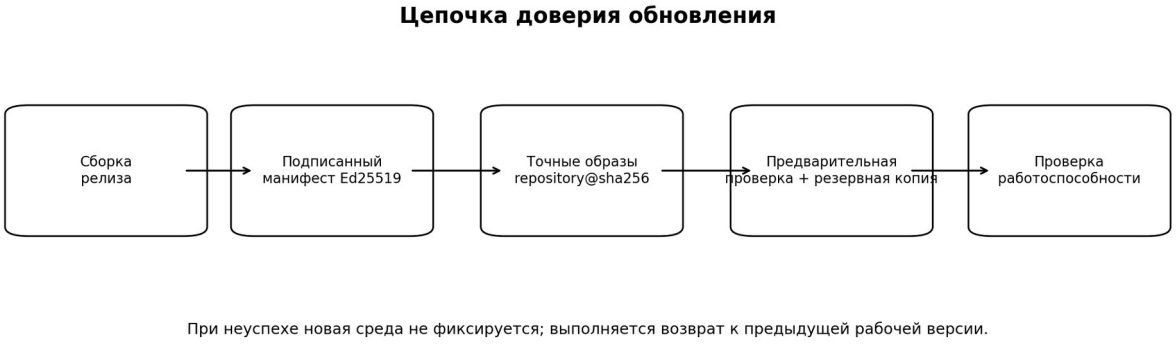



*Рисунок 3 - Цепочка доверия обновления*

- манифест выпуска и канал подписываются Ed25519;
- служба обновления доверяет только встроенному открытому ключу/набору доверия;
- контейнеры фиксируются как repository@sha256;
- опубликованный стабильный выпуск не перезаписывается; исправление получает новый номер;
- перед переключением выполняется предварительная проверка и проверенная резервная копия;
- новая версия проходит контроль работоспособности; при ошибке выполняется возврат к предыдущей среде;
- ротация ключа подписи выполняется в две фазы, чтобы новый ключ не начал использоваться раньше доставки его открытой части клиентам.

## 34 Управление уязвимостями

Процесс разработки и сопровождения ориентирован на ГОСТ Р 56939-2024: выявление, анализ, устранение и проверка уязвимостей должны быть встроены в жизненный цикл. Уязвимость оценивается не только по численной шкале, но и по доступности эксплуатации, типу данных, сетевой достижимости и наличию компенсирующих мер.

| Уровень | Примерный ориентир | Подход |
|---|---|---|
| Критический | Удалённое выполнение кода, обход аутентификации, массовая утечка секретов | Немедленный анализ, ограничение эксплуатации, внеплановое исправление. |
| Высокий | Повышение привилегий, доступ к чувствительным данным, существенный обход политики | Приоритетное исправление и уведомление. |
| Средний | Ограниченное воздействие при дополнительных условиях | Исправление в поддерживаемом выпуске. |
| Низкий | Незначительное воздействие либо сложная эксплуатация | Плановое устранение. |

## 35 Безопасная разработка и выпуск

- изменения проходят машиночитаемые проверки и тесты безопасности соответствующей подсистемы;
- критические инварианты безопасности закрепляются регрессионными тестами;
- релиз собирается воспроизводимым сценарием, без сборки рабочего кода на сервере заказчика;
- версии сторонних образов закрепляются по контрольной сумме;
- проверяются миграции, резервирование, откат и контроль работоспособности;
- изменения базовой версии LibreChat выполняются через собственные надстройки и дополнительные службы, что уменьшает объём трудно сопровождаемого ответвления кода.

## 36 Сторонние компоненты и SBOM

Поставка содержит как собственные компоненты НАЙС СОФТ, так и стороннее свободное программное обеспечение. Для безопасности цепочки поставки необходимы реестр сторонних компонентов, их лицензии и SBOM конкретного выпуска. Уязвимость стороннего компонента анализируется на применимость к способу использования в Студии.

- сторонний образ закрепляется версией и контрольной суммой;
- замена компонента выполняется только в новом выпуске после проверки;
- секреты реестра контейнеров не должны передаваться публичным исходным реестрам;
- по возможности собственные образы дополнительно подписываются в корпоративном реестре;
- SBOM хранится как доказательный материал релиза и используется при анализе уязвимостей.

## 37 Локальный и закрытый режим

В локальном режиме модель, RAG, база знаний и основные пользовательские данные могут работать внутри инфраструктуры организации. В закрытом корпоративном контуре внешние интеграции и внешние поставщики моделей запрещаются сетевой политикой либо не настраиваются.

**Принцип минимального выхода**

Сам факт наличия функции внешней модели не означает передачу данных. Передача возникает только при выборе и использовании внешнего поставщика или внешней интеграции. Для чувствительных рабочих процессов заказчик может оставить только локальные модели и внутренние источники.

## 38 Полностью изолированный контур

Полностью изолированный режим исключает штатный сетевой выход в Интернет. Все контейнерные образы, модели, документы, обновления и доверенные сертификаты доставляются контролируемым способом через внутренний реестр или проверенный переносимый носитель.

- внутренние DNS и NTP предоставляются внутри контура;
- автономное обновление проверяет подпись и хеши так же, как сетевое;
- внешние модельные и интеграционные сервисы имеют статус «не применяется»;
- все нужные модели должны быть заранее импортированы и квалифицированы;
- переносимый носитель проверяется по процедуре заказчика до подключения к контуру.

## 39 Персональные данные

Если через ИИ Студию обрабатываются персональные данные, заказчик является оператором либо лицом, обрабатывающим данные по поручению оператора, в зависимости от фактической схемы. Он определяет цели, правовые основания, категории данных, угрозы, требуемый уровень защищённости и состав организационных и технических мер.

- применяются статья 19 Федерального закона №152-ФЗ, постановление Правительства №1119 и приказ ФСТЭК №21 в применимом объёме;
- при выборе внешней модели заказчик обязан учитывать правовые основания передачи персональных данных соответствующему получателю;
- для минимизации передачи рекомендуется локальная модель и локальный RAG;
- резервные копии и журналы также должны учитываться в перечне мест обработки и хранения персональных данных;
- права на удаление/блокирование данных реализуются с учётом назначения конкретной базы и требований хранения.

## 40 Государственные информационные системы

При использовании ИИ Студии в государственной информационной системе или иной информационной системе государственного органа требования к защите определяются действующим приказом ФСТЭК России №117 от 11.04.2025 с изменениями 2026 года и другими применимыми актами. Приказ ФСТЭК №17 с 1 марта 2026 года утратил силу.

ИИ Студия может быть компонентом такой системы, однако класс защищённости, модель угроз, необходимость аттестации и состав сертифицированных средств определяются проектом конкретной информационной системы, а не настоящим документом.

## 41 Критическая информационная инфраструктура

Если ИИ Студия включается в состав объекта КИИ, субъект КИИ обязан самостоятельно определить наличие объекта, провести категорирование в установленном порядке и выполнить требования Федерального закона №187-ФЗ и применимых приказов ФСТЭК, включая требования к значимым объектам.

Студия не должна рассматриваться как самостоятельная замена системе безопасности значимого объекта. Её журналы, сетевые потоки, обновления, резервирование и административные роли включаются в общую архитектуру защиты КИИ.

## 42 Криптографическая защита и сертифицированные средства

Продукт использует общепринятые прикладные криптографические механизмы AES, HMAC, TLS и Ed25519 для защиты собственных данных и обновлений. Эти реализации не заявляются как сертифицированные российские средства криптографической защиты информации.

**Если требуется сертифицированная криптография**

В информационных системах, где нормативные документы или модель угроз требуют сертифицированных СКЗИ, VPN, TLS с отечественными алгоритмами, защищённого канала или сертифицированного шифрования носителей, соответствующие средства должны быть выбраны и внедрены заказчиком на уровне ОС, сети, шлюзов или иных компонентов защищённого контура.

## 43 Реагирование на инциденты

1. Зафиксировать время, источник сообщения и затронутый экземпляр.
2. Ограничить развитие инцидента: заблокировать учётную запись, отключить интеграцию, вывести внешний поставщик из маршрутизации либо перевести Студию в режим обслуживания.
3. Сохранить журналы и иные доказательства без изменения оригиналов.
4. Определить затронутые данные, секреты, пользователей и внешние системы.
5. При компрометации секрета выполнить его ротацию; связанные разрешения автоматизаций должны стать недействительными.
6. Устранить первопричину и установить исправление/компенсирующую меру.
7. Восстановить работоспособность из проверенного состояния.
8. Выполнить анализ причин и обновить меры защиты.

## 44 Восстановление и непрерывность

Безопасное восстановление важнее простого запуска контейнеров. При полной потере сервера сначала восстанавливается конфигурация и исходные внутренние секреты, затем выполняется восстановление данных зашифрованной копии. Нельзя создавать новые внутренние ключи и ожидать, что старые зашифрованные хранилища расшифруются корректно.

- ключ восстановления хранится отдельно и проверяется в учебном восстановлении;
- резервная копия должна проходить проверку перед тем, как считаться пригодной;
- после восстановления проверяются пользователи, роли, интеграции, Реестр моделей, автоматизации, TLS и аудит;
- неоконченные автоматизации не запускаются повторно автоматически;
- для критического контура рекомендуется регулярное восстановление на отдельном испытательном стенде.

## 45 Обязанности администратора и заказчика

| Сторона | Основные обязанности |
|---|---|
| НАЙС СОФТ | Исправление уязвимостей поддерживаемой версии, безопасный механизм обновлений, документирование механизмов защиты, квалификационные тесты, сведения о сторонних компонентах. |
| Администратор Студии | Управление пользователями и моделями, установка обновлений, контроль резервных копий, сертификатов, журналов и состояния служб, минимизация внешних интеграций. |
| Администратор ОС/инфраструктуры | Патчи ОС, права файлов, межсетевой экран, защита гипервизора, дисков, сети, физического доступа, журналов системы и времени. |
| Владелец информации/оператор | Классификация данных, правовые основания, модель угроз, допустимость внешних поставщиков, сроки хранения, реагирование и выполнение требований регулятора. |

## 46 Остаточные риски и ограничения

- генеративная модель может сформировать ошибочный, неполный или вредоносный ответ;
- внедрение вредоносных инструкций нельзя полностью устранить только фильтрацией текста;
- администратор ОС с root-доступом находится выше прикладной границы защиты Студии;
- внешний поставщик модели или интеграции может изменить условия, безопасность или доступность сервиса;
- слабая защита файла конфигурации экземпляра может привести к компрометации внутренних ключей;
- неустановленные обновления ОС, контейнерной среды и Студии увеличивают риск;
- резервная копия бесполезна при утрате отдельного ключа восстановления;
- сертификация или аттестация конкретного контура не возникает автоматически из наличия описанных механизмов.

## 47 Проверка защищённости и приёмка

Перед вводом в эксплуатацию рекомендуется выполнить функциональные и негативные проверки защитных границ. Критерий приёмки - не только успешный нормальный сценарий, но и корректный отказ при нарушении владельца, права, сети или целостности.

| Проверка | Ожидаемый результат |
|---|---|
| Пользователь пытается получить чужое подключение | Не найдено/отказ; секрет не раскрывается. |
| В базе изменён owner_user_id зашифрованного секрета | Расшифрование не проходит аутентификацию. |
| Поставщику разрешён адрес обратной петли или службы метаданных | Соединение блокируется. |
| Поставщик отвечает перенаправлением | Перенаправление не выполняется. |
| Неизвестное действие инструмента | Не выполняется автоматически. |
| Изменяющее действие | Требуется подтверждение согласно политике. |
| Секрет автоматизации ротирован | Старое разрешение становится недействительным, автоматизация отключается. |
| Подмена манифеста обновления | Проверка подписи/хеша завершается ошибкой. |
| Восстановление повреждённой копии | Проверка целостности не допускает восстановление. |

## 48 Поддержание безопасности в эксплуатации

- ежедневно контролировать критические ошибки служб и состояние резервного копирования;
- регулярно просматривать административный аудит и необычные события интеграций;
- еженедельно проверять наличие обновлений и бюллетеней безопасности;
- ежемесячно проверять срок сертификата, свободное место, права администраторов и активные внешние поставщики;
- ежеквартально выполнять тест восстановления и пересмотр привилегированных автоматизаций;
- при увольнении пользователя немедленно блокировать его, отзывать сессии и при необходимости отзывать/ротировать внешние подключения;
- при изменении модели угроз пересматривать сетевые правила, локальный режим и перечень допустимых внешних сервисов.

# ПРИЛОЖЕНИЕ А - КАТАЛОГ УГРОЗ И МЕР

| ID | Угроза | Последствие | Основные меры |
|---|---|---|---|
| T01 | Кража пользовательской сессии | Чужой доступ к данным и функциям | TLS, отзыв сессий, короткий жизненный цикл сессии, блокирование пользователя |
| T02 | Подмена роли | Повышение полномочий | Серверная проверка роли, защищённые системные роли, отзыв сессий при смене роли |
| T03 | Использование чужого секрета интеграции | Выдача себя за другого пользователя | ConnectionStore с привязкой к владельцу, проверка совпадения владельца в разрешителе, отсутствие подстановки учётных данных ADMIN |
| T04 | Перенос шифротекста между пользователями | Компрометация секрета | AAD включает владельца, профиль и тип авторизации; AES-GCM не проходит проверку |
| T05 | Использование прикладного секрета вместо пользовательского | Обход персональной идентичности | Отдельный AppCredentialStore и независимый домен AAD |
| T06 | Восстановление старого общего секрета откатом | Возврат уязвимой модели доступа | Карантин устаревших записей; среда выполнения не имеет доступа к их расшифрованию; откат не восстанавливает общий секрет |
| T07 | SSRF к внутренней сети | Доступ к служебным интерфейсам | Сетевые режимы публичный/частный; запрет адресов обратной петли, локального канала и служб метаданных |
| T08 | Повторная привязка DNS | Обход проверки адреса | Проверка всех IP-адресов и соединение только с проверенным адресом |
| T09 | HTTP-перенаправление с заголовком Authorization | Утечка токена | Перенаправления провайдера запрещены |
| T10 | Недоверенный TLS | Атака посредника (MITM) | Обязательная проверка CA; отключение проверки сертификата не допускается; поддерживается корпоративный CA |
| T11 | Внедрение вредоносной инструкции из документа | Навязывание модели действий | Контент не меняет права; политика инструментов; подтверждение записи; секреты вне контекста |
| T12 | Модель пытается выполнить неизвестный инструмент | Непредусмотренное действие | Неизвестное действие -> запрос подтверждения/отказ; безопасный отказ по умолчанию |
| T13 | Автоматизация наследует ADMIN | Повышение прав фона | Владелец автоматизации авторитетен; роль выполнения USER |
| T14 | Автоматизация использует старый секрет после ротации | Действие от неверной идентичности | Привязка по отпечатку; аннулирование разрешения; отключение автоматизации |
| T15 | Рекурсивное самоуправление автоматизацией | Неконтролируемое размножение действий | Действия пространства automation.* запрещены внутри шагов |
| T16 | Вредоносный код в шаге выполнения кода автоматизации | Сетевой выход/кража секрета | Отсутствуют сетевые функции и интерфейсы Node.js; учётные данные поставщика и внутренние токены недоступны |
| T17 | Подмена контейнерного образа | Выполнение чужого кода | Точная ссылка repository@sha256, подписанный манифест, неизменяемый выпуск |
| T18 | Подмена манифеста обновления | Загрузка произвольной версии | Ed25519 и проверка канала/манифеста |
| T19 | Повреждение резервной копии | Невозможность восстановления/подмена | HMAC-SHA256, проверка, тест восстановления |
| T20 | Кража резервной копии | Раскрытие данных | AES-256-CTR; ключ восстановления отдельно |
| T21 | Повтор незавершённой автоматизации после восстановления | Повтор внешнего изменяющего действия | Незавершённые запуски переводятся в состояние ошибки; Redis не восстанавливается |
| T22 | Публичный доступ к БД/мониторингу | Обход приложения | Отсутствуют опубликованные порты хоста; используются внутренние сети |

| ID | Угроза | Последствие | Основные меры |
|---|---|---|---|
| T23 | Утечка закрытого TLS-ключа через интерфейс | Компрометация HTTPS | Ключ не возвращается API/браузеру |
| T24 | Секрет в аудите | Вторичная утечка | Запрет учётных данных, заголовка Authorization и тела ответа в журнале аудита |
| T25 | Компрометация хоста root-пользователем | Полный контроль экземпляра | Инфраструктурная граница: усиление защиты ОС, ограничение пользователя root, физическая и административная защита |

# ПРИЛОЖЕНИЕ Б - МАТРИЦА ПОТОКОВ ДАННЫХ

| Источник | Получатель | Данные | По умолчанию | Контроль |
|---|---|---|---|---|
| Браузер | ИИ Студия | Запросы, файлы, сессия | HTTPS | TLS, сессия, права доступа |
| ИИ Студия | Локальная модель | Контекст запроса | Локально | Внутренняя сеть/среда выполнения |
| ИИ Студия | Внешняя модель | Контекст запроса | Только если настроена и выбрана | TLS, политика поставщика, решение заказчика о допустимости данных |
| Шлюз интеграций | Jira/Confluence/Git/почта и др. | Параметры действия | По запросу пользователя/автоматизации | Секрет с привязкой к владельцу, права, политика подтверждения |
| RAG | Модель | Найденные фрагменты | По сценарию | Права к источнику и политика модели |
| Служба обновления | studio.ncsgp.ru | Метаданные выпуска | При проверке обновления | HTTPS + подпись + контрольная сумма |
| Служба резервного копирования | Каталог backups | Авторитетные данные | По расписанию/команде | Шифрование + HMAC |
| Prometheus | Внутренние службы | Метрики | Локально | Не публикуется наружу |

# ПРИЛОЖЕНИЕ В - СОБЫТИЯ АУДИТА

| Категория | Примеры событий | Что не должно попадать |
|---|---|---|
| Поставщики моделей | создание, изменение, удаление, проверка, ротация секрета, изменение CA | секрет, заголовок Authorization, тело CA, тело ответа поставщика |
| Пользователи | создание, роль, блокирование, отзыв сессий, удаление | пароль, хеш пароля, токен обновления |
| Интеграции | создание/проверка/отзыв профиля, вызов действия | полный секрет, лишнее содержимое ответа |
| Автоматизации | создание, включение, запуск, подтверждение, изменение разрешения | провайдерские секреты и внутренние идентификаторы движка |
| Обновления | проверка, подготовка, установка, откат | закрытые ключи подписи |
| Резервирование | создание, проверка, восстановление | ключ восстановления |

# ПРИЛОЖЕНИЕ Г - КОНТРОЛЬНЫЙ ЛИСТ ИБ

| № | Проверка | Статус |
|---|---|---|
| 1 | Внешний адрес опубликован только через HTTPS | ☐ |
| 2 | Пароль ADMIN изменён и соответствует политике | ☐ |
| 3 | Удалённый root-доступ к ОС запрещён либо ограничен политикой | ☐ |
| 4 | Внутренние БД не опубликованы наружу | ☐ |
| 5 | Межсетевой экран разрешает только необходимые порты | ☐ |
| 6 | В рабочем .env отсутствуют CHANGE_ME | ☐ |
| 7 | Ключ восстановления резервной копии сохранён отдельно | ☐ |
| 8 | Выполнена проверенная резервная копия | ☐ |
| 9 | Сертификат действителен и соответствует домену | ☐ |
| 10 | Проверены роли и отсутствие лишних ADMIN | ☐ |
| 11 | Ненужные внешние поставщики моделей отключены | ☐ |
| 12 | Для каждого внешнего поставщика проверены TLS и сеть | ☐ |
| 13 | Ненужные интеграции не настроены | ☐ |
| 14 | Изменяющие действия требуют подтверждения согласно политике | ☐ |
| 15 | Привилегированные автоматизации пересмотрены | ☐ |
| 16 | Выполнен тест изоляции владения между двумя пользователями | ☐ |
| 17 | Проверен отказ SSRF при обращении к адресу обратной петли или службы метаданных | ☐ |
| 18 | Проверен отказ HTTP-перенаправления поставщика | ☐ |
| 19 | Проверено, что секреты отсутствуют в аудите | ☐ |
| 20 | Обновления проверяются по подписи | ☐ |
| 21 | Все рабочие образы закреплены контрольными суммами | ☐ |
| 22 | SBOM выпуска сохранён | ☐ |
| 23 | Выполнена проверка восстановления | ☐ |
| 24 | Настроен сбор/просмотр событий безопасности | ☐ |
| 25 | Определён порядок реагирования на инцидент | ☐ |

# ПРИЛОЖЕНИЕ Д - КОНТРОЛЬНЫЙ ЛИСТ ЗАКРЫТОГО КОНТУРА

| № | Требование | Статус |
|---|---|---|
| 1 | Определён перечень разрешённых внешних соединений; для полностью изолированного режима он пуст | ☐ |
| 2 | Используются локальные модели либо внутренний корпоративный поставщик | ☐ |
| 3 | Все необходимые модели импортированы заранее | ☐ |
| 4 | Контейнерные образы доступны во внутреннем реестре/на проверенном носителе | ☐ |
| 5 | Проверены подписи и контрольные суммы автономного обновления | ☐ |
| 6 | DNS и NTP доступны внутри контура | ☐ |
| 7 | Сертификат выдан внутренним доверенным УЦ либо иным допустимым способом | ☐ |
| 8 | Отключены внешние веб-поиск и облачные интеграции, если они не разрешены | ☐ |
| 9 | Политикой запрещена передача чувствительных данных внешним моделям | ☐ |
| 10 | Резервные копии хранятся внутри контролируемой зоны | ☐ |
| 11 | Ключ восстановления хранится в отдельной защищённой зоне | ☐ |
| 12 | Определён процесс ввоза обновлений и моделей | ☐ |
| 13 | Проверен журнал действий администратора | ☐ |
| 14 | Выполнено восстановление на испытательном стенде | ☐ |
| 15 | Определена процедура вывоза журналов/диагностики без раскрытия конфиденциальных данных | ☐ |

# ПРИЛОЖЕНИЕ Е - МАТРИЦА НОРМАТИВНОГО СООТВЕТСТВИЯ

| Норма/документ | Что покрывает Студия | Что остаётся заказчику |
|---|---|---|
| 149-ФЗ, ст.16 | Технические меры приложения: доступ, секреты, аудит, TLS, резервирование, обновления | Организационные меры, защита инфраструктуры, классификация информации |
| 152-ФЗ, ст.19; ПП №1119; ФСТЭК №21 | Локальный режим, разграничение доступа, журналирование, резервирование, изоляция секретов | Определение уровня защищённости, модели угроз, правовых оснований, сертифицированных СЗИ при необходимости |
| ФСТЭК №117 | Может использоваться как компонент защищаемой ИС с журналами, ролями, обновлениями и сегментацией | Класс/требования системы, проект защиты, аттестация, сертифицированные средства |
| 187-ФЗ; ФСТЭК №239 | Технические механизмы приложения и события для общей системы защиты | Категорирование КИИ, система безопасности значимого объекта, взаимодействие с ГосСОПКА если применимо |
| ГОСТ Р 56939-2024 | Безопасный выпуск, регрессионные тесты, управление уязвимостями, фиксированные зависимости | Корпоративная оценка процесса и независимая сертификация, если требуется |
| ГОСТ Р 59898-2021 | Квалификация моделей и возможностей, функциональные/безопасностные проверки | Отраслевая программа оценки качества конкретного применения |
| ГОСТ Р 72514-2026 | Документирование сценариев, рисков и воздействия через документацию продукта | Оценка воздействия конкретного применения заказчика |
| ГОСТ Р 72515-2026 | Сведения о модели, поставщике, возможностях, границах передачи данных | Требуемый уровень раскрытия для конкретной заинтересованной стороны |

# ПРИЛОЖЕНИЕ Ж - ОФИЦИАЛЬНЫЕ ИСТОЧНИКИ

| Источник | Адрес |
|---|---|
| Федеральный информационный фонд стандартов - ГОСТ Р 56939-2024 | https://protect.gost.ru/gost/details/f3818925-a96f-4f55-96e9-46b44720ee64 |
| ГОСТ Р 59898-2021 | https://protect.gost.ru/gost/details/51f65c79-5f22-4a2e-96d9-fe9503459852 |
| ГОСТ Р 72514-2026 | https://protect.gost.ru/gost/details/1532adb0-298e-42d3-b265-cd74afbc8ac6 |
| ГОСТ Р 72515-2026 | https://protect.gost.ru/gost/details/df47ff5a-169b-4ee6-a9da-b45f7742d432 |
| 149-ФЗ, статья 16 | https://www.consultant.ru/document/cons_doc_LAW_61798/0e9ec16b786dcbdaaa7f44abfc4a15e601d5be22/ |
| 152-ФЗ, статья 19 | https://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/ |
| Постановление Правительства РФ №1119 | https://www.consultant.ru/document/cons_doc_LAW_137356/ |
| Приказ ФСТЭК №21 | https://www.consultant.ru/document/cons_doc_LAW_146520/ |
| Приказ ФСТЭК №117 (ред. 08.05.2026) | https://www.consultant.ru/document/cons_doc_LAW_507869/ |
| Методический документ ФСТЭК от 12.04.2026 | https://www.consultant.ru/document/cons_doc_LAW_531896/ |
| 187-ФЗ | https://www.consultant.ru/document/cons_doc_LAW_220885/ |
| Приказ ФСТЭК №239 | https://www.consultant.ru/document/cons_doc_LAW_294287/ |

## ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

| Изм. | Номера листов | Всего листов | № документа | Входящий № и дата | Подпись | Дата |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |