ЭКСПЛУАТАЦИОННАЯ ДОКУМЕНТАЦИЯ — УСТАНОВКА И АДМИНИСТРИРОВАНИЕ

Руководство по установке, настройке и эксплуатации программы «Шлюз контроля действий «МИТР» (версия 3.0)»

Инструкция по автономному развёртыванию в закрытой сети на российских операционных системах семейства Альт и линейки «РЕД» без доступа к сети Интернет.

1. Требования к программно-аппаратной среде

Шлюз «МИТР» разработан для автономного развёртывания на серверах и рабочих станциях платформы `x86_64` под управлением российских операционных систем семейства `Linux`. Программа не требует подключения к сети Интернет ни на этапе первичной установки, ни при проверке политик и ежедневной работе.

Компонент среды	Минимальные и рекомендуемые требования
Аппаратная платформа	**Процессор** `x86_64` **(от двух ядер), основная память от 512 мегабайт (рекомендуется 2 гигабайта), свободное место на диске от 200 мегабайт плюс объём под журнал квитанций**
Проверенные российские операционные системы	**Альт Сервер на платформе** `p11` **(реестровый номер 1541, системный** `Python 3.12`**) и** `РЕД ОС 8` **версии 8.0.3 (реестровый номер 3751, системный** `Python 3.11`**); целевая двоичная совместимость** `manylinux_2_17_x86_64` **—** `Astra Linux Special Edition 1.8` **(реестровый номер 369)**
Системный интерпретатор	**Штатный интерпретатор** `Python 3.10`**,** `3.11` **либо** `3.12` **из локального репозитория операционной системы**
Внешние сетевые доступы	**Не требуются: обе сторонние библиотеки (**`z3-solver` **и** `PyYAML`**) включены в автономный каталог** `wheelhouse/` **внутри архива поставки**

2. Состав комплекта поставки и проверка контрольной суммы

Эталонный комплект распространяется единым архивом `iss-mitr-gate-3.0.0-linux-x86_64-offline.tar.gz` объёмом 30,17 мегабайта. Перед началом развёртывания администратор сверяет контрольную сумму загруженного файла со значением, опубликованным на странице `https://isslab.ru/mitr/reestr/`.

```
# Проверка контрольной суммы эталонного дистрибутива перед установкой
sha256sum -c SHA256SUMS.txt
# Ожидаемый отпечаток архива:
# 8d50af85ac9e064a541bf79cf56012eedfa487373c4f2270536f99b6020b8d40  iss-mitr-gate-3.0.0-linux-x86_64-
offline.tar.gz
```

Внутри архива находятся пакет `iss_mitr_gate/` с двадцатью двумя контрактами политики и локальный каталог колёс `wheelhouse/` для `Python 3.10–3.12`. В комплект также входят сценарий автономной установки `install_offline.sh`, файл системной службы `systemd/mitr-gate.service`, ведомость `SBOM.spdx.json` и набор автотестов `tests/`.

3. Пошаговая автономная установка без доступа к сети

Проверка базового интерпретатора из локального дистрибутива операционной системы

Операционная система	Штатная автономная команда проверки интерпретатора
Альт Сервер (p11, **№ 1541**)	`python3 --version || sudo apt-get install -y python3`
РЕД ОС 8 **(выпуск 8, № 3751)**	`python3 --version || sudo dnf install -y python3.11`
Astra Linux Special Edition 1.8 **(№ 369)**	`python3 --version || sudo apt install -y python3`

Единый сценарий автономной установки (ноль сетевых запросов)

Сценарий `install_offline.sh` не требует пакетного менеджера `pip` и не обращается к внешним узлам. Он определяет версию системного интерпретатора, распаковывает бинарные пакеты из каталога `wheelhouse/` в `/opt/iss-mitr-gate/lib`, выставляет права чтения для непривилегированной службы, создаёт команды `mitr-gate` и `mitr-verify` и запускает встроенный самотест.

```
# 1. Распаковка эталонного дистрибутива
tar -xzf iss-mitr-gate-3.0.0-linux-x86_64-offline.tar.gz
cd iss-mitr-gate-3.0.0

# 2. Автономная установка в /opt/iss-mitr-gate с автоматическим самотестом
sudo bash ./install_offline.sh --prefix /opt/iss-mitr-gate

# 3. Контрольная демонстрация перехвата опасного действия и цепи квитанций
/opt/iss-mitr-gate/bin/mitr-gate demo
```

4. Настройка системной службы и разграничение прав доступа

Для постоянной работы в режиме локального сервера администратор создаёт непривилегированную учётную запись `mitr` и выделяет защищённый каталог журналов. Шаблон службы `systemd/mitr-gate.service` запускает исполняемый файл `/opt/iss-mitr-gate/bin/mitr-gate` с запретом повышения привилегий и строгим разграничением файловой системы.

```
sudo useradd --system --home-dir /var/lib/iss-mitr-gate --shell /usr/sbin/nologin mitr
sudo mkdir -p /var/lib/iss-mitr-gate /etc/iss-mitr-gate/contracts
sudo chown -R mitr:mitr /var/lib/iss-mitr-gate && sudo chmod 0750 /var/lib/iss-mitr-gate
sudo cp systemd/mitr-gate.service /etc/systemd/system/mitr-gate.service
sudo systemctl daemon-reload && sudo systemctl enable --now mitr-gate.service
curl -s http://127.0.0.1:8787/health
```

5. Параметры конфигурации и переменные среды

Управление параметрами запуска выполняется через переменные среды в файле системной службы `/etc/systemd/system/mitr-gate.service` либо через ключи командной строки. Внесение новых правил допуска разрешается только администратору с обязательной проверкой компиляции контрактов командой `mitr-gate contracts`.

Переменная среды	Значение по умолчанию	Назначение и влияние на режим работы
`MITR_CONTRACTS_DIR`	**встроенный каталог**	**Путь к внешнему каталогу пользовательских контрактов политики формата** `pol_v1`
`MITR_LEDGER_PATH`	`/var/lib/iss-mitr-gate/gate_actions.jsonl`	**Путь к последовательному файлу журнала квитанций с двойной хэш-цепью**
`MITR_API_TOKEN`	**пусто (локальный узел)**	**Секретный токен авторизации для обращений к маршрутам** `/v1/*` **локального сервера**
`MITR_CORE_MINIMIZE`	`on`	**Вычисление минимального ядра невыполнимости при проверке формулы**
`MITR_EXTERNAL_ANCHOR`	`0`	**Отключение внешних сетевых обращений для полной автономности закрытой среды**
`MITR_HTTP_ACCESS_LOG`	`0`	**Вывод журнала обращений к локальному серверу в поток диагностики**

6. Регламент эксплуатации, резервного копирования и удаления

- **Ежедневный контроль целостности журнала** выполняется администратором либо заданием планировщика с помощью команды `/opt/iss-mitr-gate/bin/mitr-verify /var/lib/iss-mitr-gate/gate_actions.jsonl --json`, где ненулевой код возврата сигнализирует о нарушении цепи.
- **Ротация и архивирование записей** проводятся при кратковременной остановке службы с фиксацией головных отпечатков `head_gost256` и `head_sha256` и переводом архивного файла в режим только для чтения.
- **Контроль после обновления операционной системы** включает повторный запуск команды `/opt/iss-mitr-gate/bin/mitr-gate selftest --json` для документального подтверждения исправности решателя и сохранности контрактов.
- **Штатное удаление программы** предусматривает остановку службы командой `systemctl disable --now mitr-gate.service` и удаление каталога `/opt/iss-mitr-gate` при сохранении архива журналов `/var/lib/iss-mitr-gate`.

> **Быстрая проверка экспертом на чистой виртуальной машине.** Для независимой проверки достаточно выполнить три команды сценария автономной установки при отключённом сетевом интерфейсе. Демонстрационный прогон занимает менее тридцати секунд и последовательно проверяет допуск безопасной операции, перехват опасного удаления, самозащиту шлюза, расчёт поправки и обнаружение подмены записи в журнале.