

Инструкция по установке

ВЫШКА Регламент • версия 0.1.0, выпуск R2

Документ РГЛ-R2-УСТ-01. Редакция от 09.10.2026. ООО «НЬЮ-ССТ», ИНН 7733311994.

1. Назначение и условия установки

Инструкция предназначена администратору разрешённого Linux-хоста. Проверенная конфигурация: Ubuntu 24.04.5 LTS, Python 3.12.3, 4 vCPU, 8 ГБ оперативной памяти, 80 ГБ диска. Эта конфигурация фактически использовалась при проверке R2; минимальные ресурсы и нагрузочная ёмкость не установлены.

Приложение использует стандартную библиотеку Python 3.12 и статические HTML/CSS/JavaScript. Для эксплуатации не требуются pip, pmt, серверная база данных и внешние API моделей. Nginx применяется для размещения за обратным прокси. Node.js нужен только дополнительным проверкам JavaScript, но не рабочему приложению.

Браузеру необходимы JavaScript, fetch, Web Crypto, dialog и localStorage для явного сохранения. Для Web Crypto используется HTTPS либо доверенный браузером loopback-адрес. Совместимость с российскими ОС этим документом не подтверждается.

2. Дистрибутив и контроль целостности

Идентификатор дистрибутива: vyshka-reglament-0.1.0-r2.tar.gz. Контрольный SHA-256:

```
79c33e07c48f3f8708d3d8680c195db2c383dcd90c7aee14e3a030ef23b74f1f
```

До распаковки сравните SHA-256 с независимой записью выпуска. Просмотрите список tar: допустимы только ожидаемые относительные пути; пути с ../, абсолютные пути и неожиданные ссылки требуют остановки установки. Распакуйте архив в новый каталог, отдельно от работающей версии. Сверьте встроенный RELEASE-MANIFEST.json и состав src/, web/, data/, tests/, docs/, а также предусмотренные выпуском evidence/ и ops/. Отдельно предоставленный RELEASE-MANIFEST-R2.json является побайтово идентичной копией встроенного манифеста.

Сохраняйте предшествующую версию и конфигурацию отдельно. Закрытые SSH/TLS-ключи, данные ACME-аккаунтов и пользовательские документы в дистрибутив не включаются. Дополнение r2-docs-20261009 уточняет документацию; оно не изменяет байты исходного архива R2.

3. Проверка установки

Команды выполняются из корня отдельного каталога дистрибутива. Выходные файлы обучения должны отсутствовать либо быть выделены именно этой проверке; нужные ранее полученные результаты не перезаписываются.

```
python3 --version
python3 -B -m src.train \
  --model /tmp/reglament-model-check.json \
  --metrics /tmp/reglament-metrics-check.json
sha256sum /tmp/reglament-model-check.json data/model.json
PYTHONDONTWRITEBYTECODE=1 python3 -m unittest discover -s tests -v
```

Для неизменённых входов ожидаемый SHA-256 модели:

```
60e5deaa1f98d8cfa147412248e8aee3b4b800a76169579a341b618953f7cdc3
```

Сохранённые результаты выпуска R2: 52/52 Python-проверки, 14/14 проверки исправлений интерфейса, 15/15 JS-регрессии. Эти результаты относятся к проверенному R2. Изменение кода, модели, корпуса или среды требует соответствующей повторной проверки.

4. Пробный запуск

Выберите свободный loopback-порт в изолированной среде. Пример запуска на 18643:

```
python3 -B -m src.server \
  --bind 127.0.0.1 --port 18643 \
  --allowed-host 127.0.0.1:18643 \
  --allowed-host localhost:18643 \
  --public-origin http://127.0.0.1:18643
```

Проверьте GET /api/health, GET /api/model и POST /api/analyze на синтетическом тексте. Откройте интерфейс через разрешённый доступ к этому адресу, выполните встроенный пример и проверьте источники карточек. По окончании остановите только свой временный процесс. На рабочем порту не запускайте второй экземпляр.

Параметры окружения: REGLAMENT_BIND, REGLAMENT_PORT, REGLAMENT_ALLOWED_HOSTS, REGLAMENT_PUBLIC_ORIGIN. В REGLAMENT_ALLOWED_HOSTS значения разделяются запятыми. Флаги --model и --web-root задают пути. Повторяемый --allowed-host содержит имя и порт; --public-origin имеет вид scheme://host[:port] без завершающего слеша.

5. Постоянный запуск и публикация

Для постоянной установки используется каталог /opt/new-sst-reglament и unit reglament.service. Администратор проверяет поставленный кандидат ops/reglament.service.candidate, соответствие путей и доступ чтения для DynamicUser, затем устанавливает unit и выполняет daemon-reload и запуск службы.

Рабочий backend привязывается к 127.0.0.1:18642. Защита unit включает DynamicUser, NoNewPrivileges, ProtectSystem=strict, ProtectHome, PrivateTmp/Devices, пустые capabilities, MemoryMax=512M, CPUQuota=200%, TasksMax=32. Это настройки ограничения процесса, а не измеренная производительность.

Публикация выполняется через согласованный обратный прокси с HTTPS. До открытия доступа согласуйте Host, allowed-host, public-origin, лимиты запросов, таймауты и политику журналов. Проверьте nginx -t, службу, health, реальный браузерный сценарий, цепочку сертификата и механизм продления. На дату редакции публичная доступность reglament.vyshka.cloud отдельно не подтверждена. Наличие сертификата в панели провайдера само по себе не означает работающий публичный маршрут.

Дистрибутив содержит отдельную вспомогательную ветку Certbot. Её установка не нужна для анализа текста. Не запускайте альтернативный выпуск сертификата параллельно управляемому TLS без решения администратора. Инструменты TLS и сопровождающие лицензии сверяются отдельно; полный состав их дистрибутивов в R2 не включён.

6. Резервирование, восстановление и откат

Сохраняйте дерево приложения, модель, manifest, unit и конфигурацию прокси как отдельную версию. Бэкап VPS не восстанавливает localStorage браузера: пользовательские проекты резервируются полным JSON-файлом и проверкой его импорта.

Для восстановления разверните подтверждённый архив в новом каталоге, проверьте manifest, повторите обучение с отдельными выходами, выполните проверки и синтетический анализ на

временном порту. После приёма администратор переключает рабочую версию, сохранив прежнюю. Для отката возвращаются сохранённые дерево, модель, unit и конфигурация прокси с повторной проверкой службы, health и интерфейса. Секретные материалы восстанавливаются через защищённый администраторский маршрут.

Изолированное восстановление приложения из R2 ранее проверено. Полное восстановление дискового бэкапа провайдера не проверено и данным документом не заявляется.

7. Диагностика и завершение установки

```
systemctl status reglament.service --no-pager
systemctl show reglament.service -p ActiveState -p SubState -p NRestarts
nginx -t
curl --fail --silent http://127.0.0.1:18642/api/health
```

При изменённом allowlist используйте разрешённый Host. В протокол установки внесите версию, контрольные суммы, среду, результаты проверок, фактический адрес доступа и сведения о сохранённом варианте отката. Не включайте секреты и полные пользовательские документы в диагностические журналы.