Инструкция по установке ПО «Flowforge»

1. Установка ПО

Установка ПО «Flowforge» (далее также - Flowforge) выполняется из архива релиза (который предоставляется пользователю после приобретения ПО) на отдельном сервере или виртуальной машине.

1.1. Системные требования

Сервер должен соответствовать следующим требованиям:

Компонент	Требование
Операционная система	Ubuntu Server 22.04 LTS или 24.04 LTS, архитектура x86_64/amd64
Процессор	Не менее 4 виртуальных ядер; для рабочей нагрузки рекомендуется 8
Оперативная память	Не менее 8 ГБ; рекомендуется 16 ГБ
Дисковое пространство	Не менее 40 ГБ; рекомендуется 80 ГБ с учётом журналов, медиафайлов и резервных копий
Сеть	Доступ к сети Интернет
Права	Учётная запись с возможностью выполнять команды sudo

До начала установки должны быть определены DNS-имя или постоянный IP-адрес сервера, режим PostgreSQL, вариант TLS и перечень подключаемых интеграций. Для сертификата, выданного удостоверяющим центром, заранее подготовьте полный путь к файлу сертификата и закрытому ключу.

1.2. Загрузка программного обеспечения

Перенесите полученный экземпляр ПО «Flowforge» на сервер установки. В корне распакованного архива должны находиться следующие элементы:

Элемент	Назначение
Backend/	Серверная часть приложения и команды управления Django
Frontend/	Исходный код клиентской части
deploy/	Шаблоны конфигурации systemd и nginx
Install.sh	Интерактивная установка, обновление и проверка экземпляра

Архив не содержит демонстрационных данных, стендовых учётных записей, мок-сервисов и готовых файлов окружения с реквизитами доступа.

1.3. Подготовка сервера

Подключитесь к упомянутому выше серверу установки по SSH и обновите сведения о доступных пакетах:

```
sudo apt update
sudo apt upgrade -y
```

Убедитесь, что системное время синхронизировано, DNS-имя разрешается в нужный адрес, а порты 80 и 443 не заняты посторонними службами. Сам инсталлятор установит nginx, Python, PostgreSQL для локального режима, Node.js 20 и остальные необходимые системные пакеты.

```
hostname -f
timedatectl status
sudo ss -ltnp
```

Примечание. Если на этом же сервере размещён веб-интерфейс Zabbix, назначьте ему отдельный порт, например 8095, и ограничьте доступ локальным или административным сегментом. Конфигурация Flowforge не содержит проксирования Zabbix.

1.4. Распаковка архива

Создайте рабочий каталог, распакуйте архив и перейдите в его корень:

```
mkdir -p ~/flowforge-release
unzip flowforge-release.zip -d ~/flowforge-release
cd ~/flowforge-release
```

Проверьте наличие обязательных файлов:

```
test -f Install.sh
test -f Backend/manage.py
test -f Frontend/package.json
test -d deploy
```

Не запускайте Install.sh из каталога, в котором отсутствуют Backend, Frontend или deploy: инсталлятор проверяет состав релиза и прекращает работу при отсутствии обязательных элементов.

1.5. Выбор режима установки и подготовка базы данных

Install.sh поддерживает три команды:

Команда	Назначение
sudo bash ./Install.sh install	Первичная интерактивная установка
sudo bash ./Install.sh update	Обновление уже установленного экземпляра
sudo bash ./Install.sh check	Проверка конфигурации и работоспособности

При первичной установке выберите режим PostgreSQL. По умолчанию используется local: PostgreSQL устанавливается на сервер Flowforge, а роль и база данных создаются автоматически. Пароль можно задать вручную или оставить пустым для безопасной автоматической генерации.

В режиме external укажите адрес, порт, имя базы, имя прикладной роли и пароль. Внешняя база и роль должны быть созданы администратором PostgreSQL заранее. Роль должна иметь право подключаться к базе, использовать схему public, создавать в ней объекты и выполнять миграции.

```
psql -h <DB_HOST> -p <DB_PORT> -U <DB_USER> -d <DB_NAME> -c 'SELECT 1'
```

Внимание. Команда install не предназначена для повторного запуска поверх существующей управляемой установки. Для установленного экземпляра используйте update.

1.6. Установка серверной части

Рекомендуемый способ: интерактивная установка

Из корня распакованного релиза запустите:

```
sudo bash ./Install.sh install
```

Инсталлятор проверит версию Ubuntu и архитектуру, запросит параметры экземпляра, установит системные зависимости, создаст системного пользователя flowforge и развернёт приложение в /opt/flowforge.

Вопросы интерактивного режима

Параметр	Варианты или значение	Пояснение
Адрес экземпляра	DNS-имя или IPv4	Без схемы и пути; localhost не допускается

Параметр	Варианты или значение	Пояснение
TLS	self-signed / existing	Самоподписанный сертификат либо существующие сертификат и ключ
HSTS	yes / no	Включать только для сертификата, которому доверяют клиентские устройства
PostgreSQL	local / external	Локальная база используется по умолчанию
База данных	Имя базы, роль, пароль	Для external также запрашиваются узел и порт
Интеграции	yes / no	Все интеграции выключены по умолчанию
Администратор	Имя, e-mail, пароль	Создаётся интерактивной командой Django

Для каждой включённой интеграции инсталлятор запросит её адрес и необходимые реквизиты:

Интеграция	Запрашиваемые параметры	Начальное состояние
VK Teams	URL сервиса, API-токен	Выключена
ResponseInfo	URL API, API-токен	Выключена
1C OData	URL API, пользователь, пароль	Выключена
Zabbix	JSON-RPC endpoint, пользователь API, пароль	Выключена
Starline	URL API, API-токен	Выключена
TTM	Базовый URL API, API-ключ	Выключена
Яндекс Карты	Ключ JavaScript API	Выключена

Использование внешней PostgreSQL

До запуска установки проверьте сетевой маршрут, правила pg_hba.conf и TLS-политику внешнего сервера PostgreSQL. Инсталлятор проверяет подключение командой SELECT 1, но не создаёт внешнюю базу или роль. Резервное копирование внешней базы выполняется средствами, принятыми у её администратора.

После подтверждения параметров инсталлятор создаёт закрытые файлы окружения, выполняет миграции, заполняет базовые справочники, собирает статические файлы и запускает проверки Django. Создаются роли MASTER, WORKER и MAINSTAFF. Демонстрационные пользователи, заказчики, объекты, автомобили, экипажи и заявки не создаются. Состав справочников может быть изменён администратором под необходимые требования.

Путь	Содержимое и права доступа
/opt/flowforge/Backend/.env	Параметры backend и секреты интеграций; владелец flowforge, режим 0640
/opt/flowforge/Frontend/.env	Параметры сборки frontend; владелец flowforge, режим 0640
/etc/flowforge/install.conf	Метаданные управляемой установки без реквизитов; root, режим 0600
/etc/flowforge/tls/	Самоподписанный сертификат и закрытый ключ, если выбран self-signed

1.7. Установка клиентской части

Клиентская часть устанавливается тем же сценарием. Инсталлятор устанавливает Node.js 20, выполняет npm ci при наличии package-lock.json, записывает адрес API в Frontend/.env и собирает production-версию командой npm run build. Результат размещается в /opt/flowforge/Frontend/build.

Ключ Яндекс Карт включается в клиентскую сборку только при выборе этой интеграции. Для изменения ключа после установки потребуется обновить Frontend/.env и повторно собрать клиентскую часть.

```
sudo -u flowforge npm --prefix /opt/flowforge/Frontend run build
```

1.8. Настройка сервера приложений (Gunicorn)

Инсталлятор создаёт модуль systemd /etc/systemd/system/gunicorn-flowforge.service, включает его в автозапуск и запускает после подготовки приложения. Gunicorn принимает соединения только на 127.0.0.1:8000; внешний доступ к приложению выполняется через nginx.

```
sudo systemctl status gunicorn-flowforge.service
sudo journalctl -u gunicorn-flowforge.service -n 100 --no-pager
```

Служба flowforge-ttm-sync.service включается и запускается только при включённой интеграции TTM RTK. При выключенной интеграции служба останавливается и исключается из автозапуска.

1.9. Настройка веб-сервера (nginx) и TLS

Инсталлятор формирует отдельный сайт /etc/nginx/sites-available/flowforge.conf, создаёт ссылку в sites-enabled, проверяет конфигурацию командой nginx -t и перезагружает nginx. HTTP-запросы на порт 80 перенаправляются на HTTPS, а приложение обслуживается на порту 443.

```
sudo nginx -t
sudo systemctl status nginx.service
```

Конфигурация содержит маршруты только для Flowforge, его API, статических и медиафайлов. Она не создаёт location или upstream для Zabbix. При совместном размещении Zabbix должен слушать другой порт и иметь отдельную конфигурацию доступа.

Режимы TLS

Режим	Порядок настройки
existing	Укажите абсолютные пути к полному сертификату и закрытому ключу. Инсталлятор проверит наличие файлов и передаст пути nginx.
self-signed	Инсталлятор создаст сертификат RSA 3072 сроком 825 дней в /etc/flowforge/tls. Клиентским устройствам потребуется доверять этому сертификату вручную.

Внимание. TLS обязателен. Режим без HTTPS промышленным инсталлятором не поддерживается.

HSTS

HSTS добавляет браузеру требование обращаться к экземпляру только по HTTPS. По умолчанию параметр выключен. Включайте его только после проверки сертификата, которому доверяют все рабочие станции; для временного самоподписанного сертификата HSTS включать не следует.

1.10. Настройка межсетевого экрана

Install.sh не изменяет UFW, nftables или внешние межсетевые экраны. После установки разрешите входящие соединения на TCP 443 от требуемых сетей, TCP 80

для перенаправления на HTTPS и административный SSH-доступ в соответствии с политикой. Порт 8000 не должен быть доступен извне.

```
sudo ufw status
sudo ss -ltnp '( sport = :80 or sport = :443 or sport = :8000 )'
```

Исходящие соединения разрешаются только к репозиториям, внешней PostgreSQL и включённым интеграциям. Если Zabbix расположен на другом сервере, проверьте доступ от Flowforge к указанному JSON-RPC endpoint.

2. Эксплуатация ПО

2.1. Запуск и проверка работоспособности

После установки выполните штатную проверку:

```
cd ~/flowforge-release
sudo bash ./Install.sh check
```

Команда проверяет платформу, наличие файлов окружения и клиентской сборки, конфигурацию nginx, состояние служб, настройки Django, отсутствие неприменённых миграций, наличие активного суперпользователя и срок действия TLS-сертификата. В завершение выполняется локальный HTTPS-запрос к экземпляру.

Проверка	Ожидаемый результат
nginx.service	active
gunicorn-flowforge.service	active
flowforge-ttm-sync.service	active только при включённой TTM RTK; иначе disabled/inactive
https://<адрес>/	Открывается форма входа Flowforge без ошибки сервера
Суперпользователь	Активен и имеет прикладную роль MAINSTAFF

Войдите под созданной административной учётной записью, проверьте основные справочники и настройте их значения с необходимыми требованиями до начала эксплуатации.

2.2. Обновление программного обеспечения

Перед обновлением создайте резервную копию базы данных, медиафайлов, файлов окружения и каталога /etc/flowforge. Распакуйте новый релиз в отдельный каталог и запустите update из его корня:

```
cd ~/flowforge-release-new
sudo bash ./Install.sh update
sudo bash ./Install.sh check
```

Обновление синхронизирует исходный код, переустанавливает зависимости, применяет миграции, обновляет базовые справочники без перезаписи существующих значений, пересобирает клиентскую часть и перезапускает службы. Backend/.env, Frontend/.env и каталог media сохраняются.

Внимание. Не используйте команду install для обновления и не удаляйте текущий каталог /opt/flowforge до успешного завершения проверки.

2.3. Резервное копирование

Периодичность и срок хранения резервных копий определяются соответствующим регламентом. Для локальной PostgreSQL можно использовать следующий пример, предварительно проверив имя базы и прикладной роли:

```
sudo install -d -o postgres -g postgres -m 0700 /var/backups/flowforge
sudo -u postgres pg_dump -Fc -d flowforge -f /var/backups/flowforge/database.dump
sudo tar -C /opt/flowforge/Backend -czf /var/backups/flowforge/media.tar.gz media
sudo install -m 0600 /opt/flowforge/Backend/.env /var/backups/flowforge/backend.env
sudo install -m 0600 /opt/flowforge/Frontend/.env /var/backups/flowforge/frontend.env
sudo tar -C /etc -czf /var/backups/flowforge/etc-flowforge.tar.gz flowforge
```

Для внешней PostgreSQL используйте штатные средства резервного копирования владельца СУБД. Храните копии файлов окружения и закрытого TLS-ключа в защищённом хранилище с ограниченным доступом. Регулярно проверяйте возможность восстановления на отдельном контуре.

2.4. Восстановление

Перед восстановлением зафиксируйте адрес экземпляра, режим PostgreSQL и состав резервной копии. Остановите прикладные службы и убедитесь, что выбран правильный целевой сервер и база данных:

```
sudo systemctl stop flowforge-ttm-sync.service
sudo systemctl stop gunicorn-flowforge.service
```

Восстановите базу данных средствами PostgreSQL, затем каталог media, Backend/.env, Frontend/.env и /etc/flowforge. Права на файлы окружения должны оставаться 0640, владелец — flowforge, группа — www-data. После восстановления примените миграции и выполните проверку:

```
sudo -u flowforge /opt/flowforge/Backend/venv/bin/python /opt/flowforge/Backend/manage.py
migrate --noinput
sudo systemctl start gunicorn-flowforge.service
sudo systemctl start flowforge-ttm-sync.service
sudo bash ./Install.sh check
```

Примечание. Службу flowforge-ttm-sync.service запускайте только при включённой интеграции TTM RTK. Восстановление базы с удалением или заменой существующих данных должно выполняться по утверждённому регламенту.

2.5. Диагностика

При ошибке установки или эксплуатации последовательно проверьте состояние служб и журналы:

```
sudo bash ./Install.sh check
sudo systemctl status nginx.service gunicorn-flowforge.service
sudo journalctl -u gunicorn-flowforge.service -n 200 --no-pager
sudo journalctl -u flowforge-ttm-sync.service -n 200 --no-pager
sudo tail -n 200 /var/log/nginx/error.log
```

Симптом	Что проверить
502 Bad Gateway	Состояние gunicorn-flowforge.service, журнал службы, прослушивание 127.0.0.1:8000
Ошибка подключения к БД	DB_HOST, DB_PORT, DB_NAME, DB_USER в Backend/.env, маршрут, pg_hba.conf и права роли
Ошибка сертификата	Соответствие SERVER_NAME, срок действия, цепочку доверия и пути к сертификату и ключу
Не работает интеграция	Флаг включения, URL, реквизиты, сетевой доступ и ответ внешнего сервиса
Не загружается интерфейс	Наличие /opt/flowforge/Frontend/build/index.html, права файлов и журнал nginx

Информация по использованию ПО «Flowforge» содержится в руководстве пользователя.