ВШтате. Установка и обновление

Требования к серверу

Компонент	Требование
ОС	Linux с поддержкой PHP 8.3 или новее
PHP	8.3, 8.4 или 8.5 с расширениями: pdo_mysql или pdo_pgsql, mbstring, openssl, tokenizer, xml, ctype, json, fileinfo, gd, intl, zip, bcmath, curl, dom, session. Для входа через LDAP: ldap
База данных	MySQL 8.0 или новее с кодировкой utf8mb4, либо PostgreSQL 15 или новее, либо Postgres Pro
Веб-сервер	nginx с PHP-FPM или другой сервер с PHP
Ресурсы для 50 сотрудников	2 ядра, 2 ГБ памяти, 10 ГБ диска плюс место под вложения и резервные копии
Браузеры сотрудников	Актуальные Chrome, Яндекс Браузер, Firefox, Edge, Safari

Установка из архива проверена на PHP 8.3 с PHP-FPM, nginx и MySQL 8.0 в контейнерах Debian. Автоматические тесты проходят на PHP 8.4. Работу на отечественных ОС проверяйте перед внедрением: в штатных репозиториях ОС может не быть нужной версии PHP.

Установка

1. Создайте базу данных и пользователя. Для MySQL:

   ```
   CREATE DATABASE vshtate CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
   CREATE USER 'vshtate'@'localhost' IDENTIFIED BY 'придумайте-пароль';
   GRANT ALL PRIVILEGES ON vshtate.* TO 'vshtate'@'localhost';
   ```

   Для PostgreSQL или Postgres Pro:

   ```
   CREATE USER vshtate WITH PASSWORD 'придумайте-пароль';
   CREATE DATABASE vshtate OWNER vshtate ENCODING 'UTF8';
   ```

2. Распакуйте архив и проверьте его контрольную сумму:

   ```
   sha256sum -c vshtate-2.1.1.zip.sha256
   unzip vshtate-2.1.1.zip -d /var/www
   mv /var/www/vshtate-2.1.1 /var/www/vshtate
   ```

3. Выдайте веб-серверу права на запись:

```
cd /var/www/vshtate
chown -R www-data:www-data storage bootstrap/cache
touch .env && chown www-data:www-data .env && chmod 640 .env
```

4. Настройте nginx. Корень сайта должен указывать на папку `public`, а не на папку продукта: иначе `.env` и данные будут доступны из интернета.

```
server {
    listen 443 ssl;
    server_name hr.example.ru;
    root /var/www/vshtate/public;
    index index.php;

    ssl_certificate     /etc/ssl/hr.example.ru.crt;
    ssl_certificate_key /etc/ssl/hr.example.ru.key;

    client_max_body_size 25m;

    add_header X-Content-Type-Options nosniff always;
    add_header X-Frame-Options SAMEORIGIN always;
    add_header Referrer-Policy strict-origin-when-cross-origin always;
    add_header Strict-Transport-Security "max-age=31536000" always;

    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }

    location ~ \.php$ {
        include fastcgi_params;
        fastcgi_pass unix:/run/php/php8.4-fpm.sock;
        fastcgi_param SCRIPT_FILENAME $realpath_root$fastcgi_script_name;
        fastcgi_read_timeout 120s;
    }

    location ~ /\.(?!well-known) {
        deny all;
    }
}
```

   Заголовок `X-Frame-Options` и остальные можно менять под правила вашей компании.

5. Настройте PHP, чтобы проходили вложения до 20 МБ. В `php.ini` или настройках пула:

```
upload_max_filesize = 25M
post_max_size = 28M
memory_limit = 256M
max_execution_time = 120
```

6. Откройте адрес портала и пройдите мастер установки, он описан в следующем разделе. **Сразу завершите мастер:** пока он не пройден, открыть его может любой, кто знает адрес. На время установки ограничьте доступ к сайту, если он виден из интернета.
7. Добавьте задачу планировщика. Без неё не работают сроки хранения данных и резервные копии по расписанию:

```
crontab -u www-data -e
```

```
* * * * * cd /var/www/vshtate && php artisan schedule:run >> /dev/null 2>&1
```

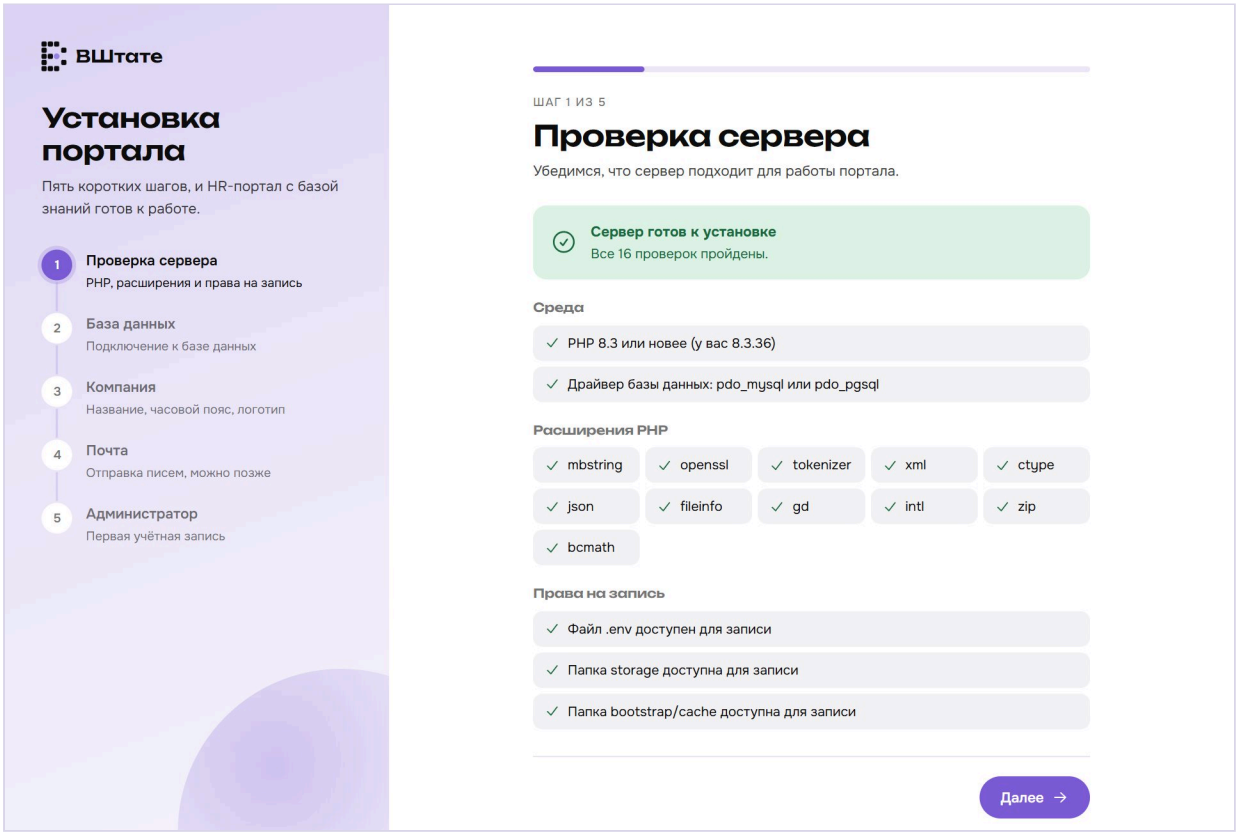
8. Откройте **Зона администратора** → **О системе** и проверьте раздел «Готовность сервера». Отметка «Планировщик запущен» появится в течение 10 минут.

Мастер установки

Мастер открывается сам, пока портал не установлен. Его адрес: `https://адрес-портала/install`. Шаги идут по порядку, вернуться к предыдущему можно кнопкой **Назад**.

Шаг 1. Проверка сервера

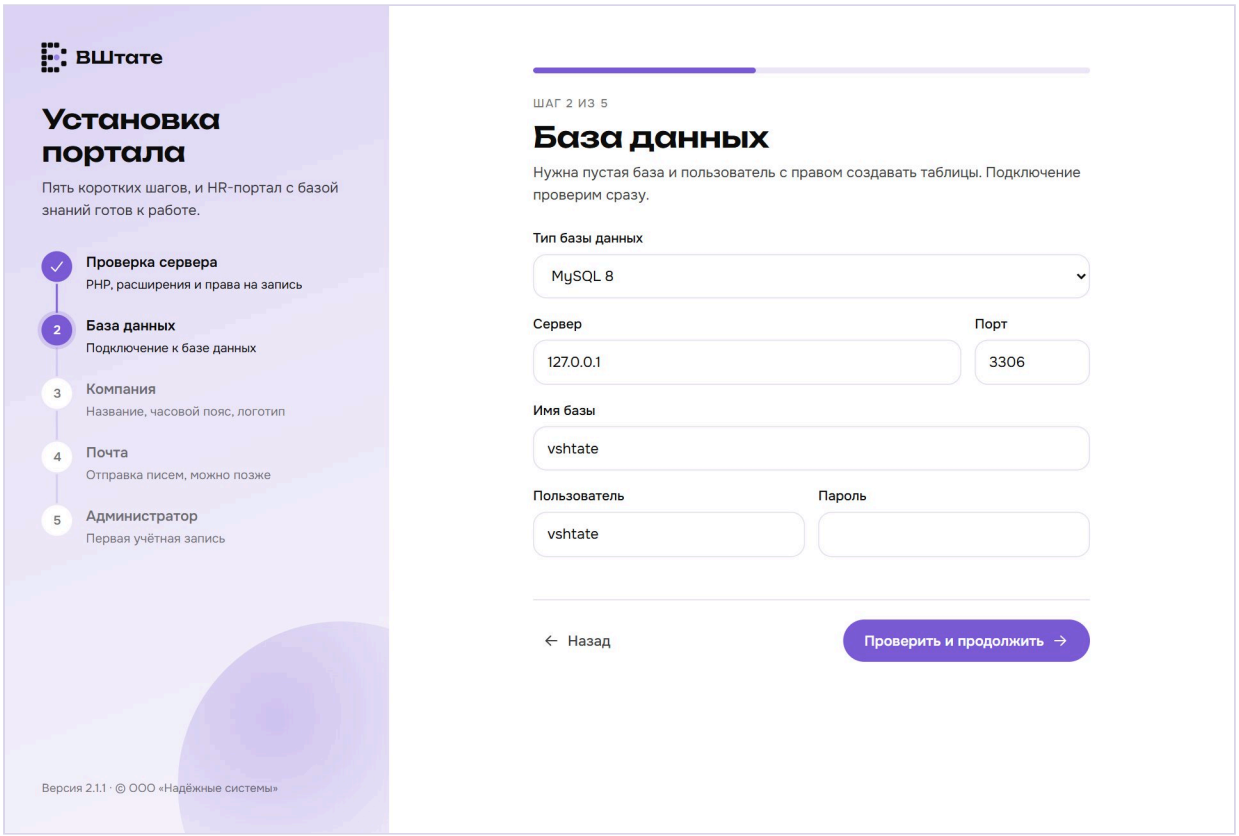
Мастер проверяет версию PHP, драйвер базы данных, расширения PHP и права на запись. Если всё в порядке, появится надпись «Сервер готов к установке»: нажмите **Далее**. Если что-то не так, неподходящие пункты будут отмечены. Исправьте их и нажмите **Проверить снова**.



Шаг 2. База данных

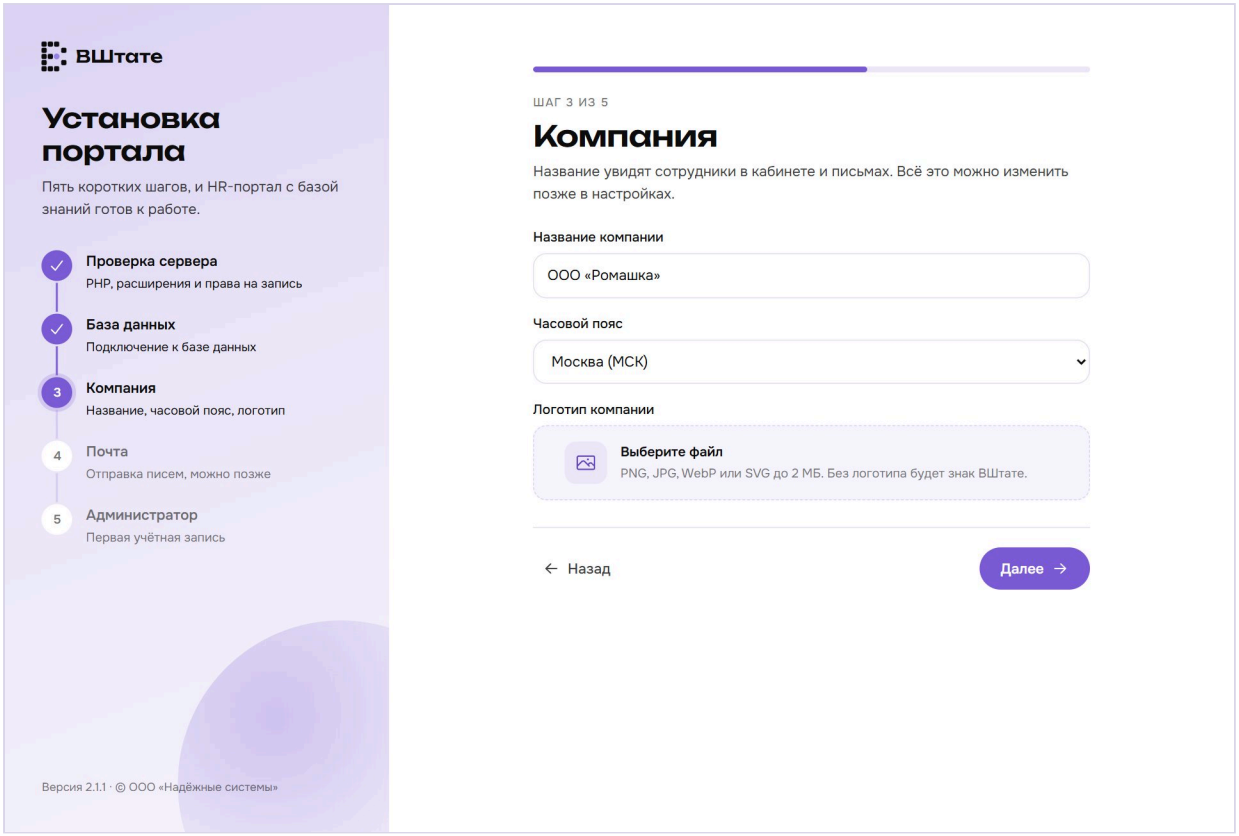
Поле	Что указать
Тип базы данных	MySQL 8 либо PostgreSQL или Postgres Pro. Порт подставится сам
Сервер	Адрес сервера базы, обычно `127.0.0.1`
Порт	`3306` для MySQL, `5432` для PostgreSQL
Имя базы	Имя пустой базы из шага 1 установки
Пользователь и пароль	Пользователь с правом создавать таблицы

Нажмите **Проверить и продолжить**: мастер сразу проверит подключение. После ошибки поле пароля очищается, введите пароль снова.



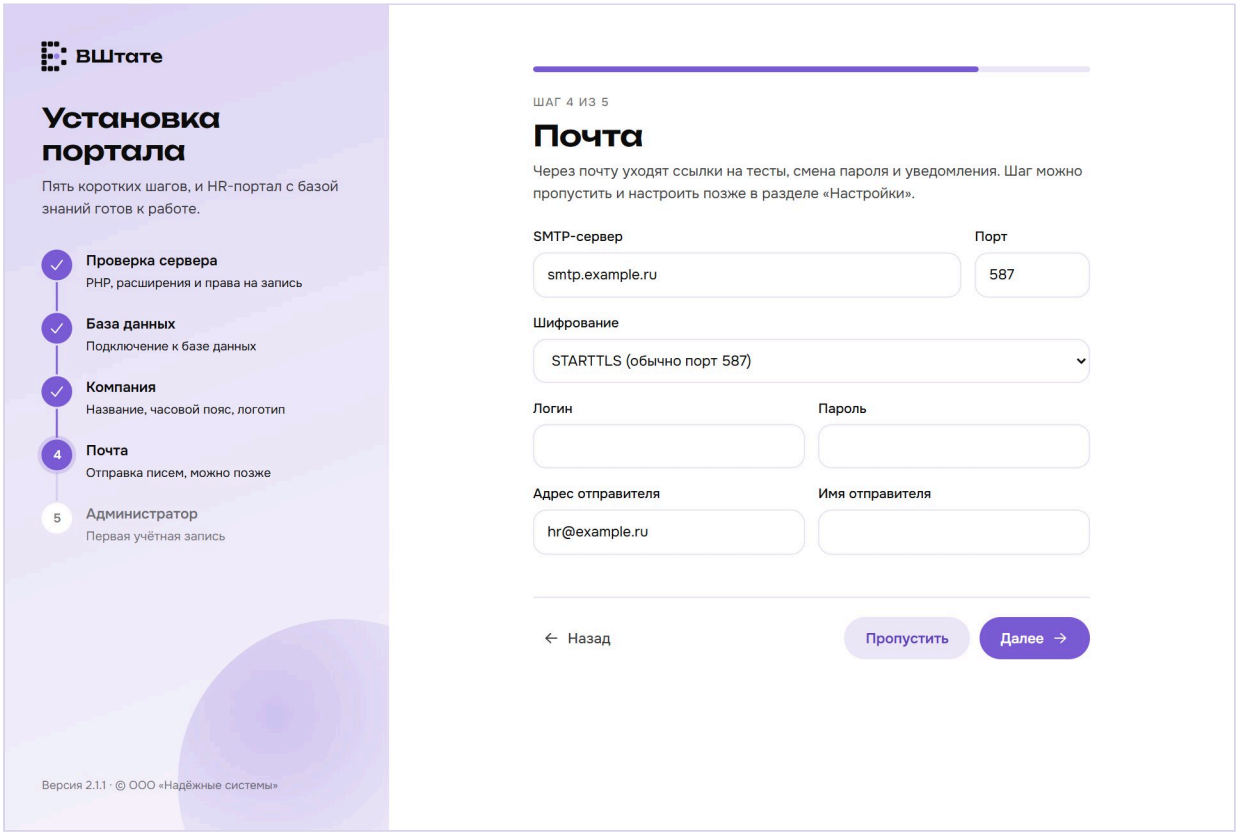
Шаг 3. Компания

Укажите название компании с формой организации, например ООО «Ромашка»: оно попадёт в кабинет, письма и тексты согласий. Выберите часовой пояс и при желании загрузите логотип (PNG, JPG, WebP или SVG до 2 МБ). Всё это можно изменить позже в разделе **Настройки**.



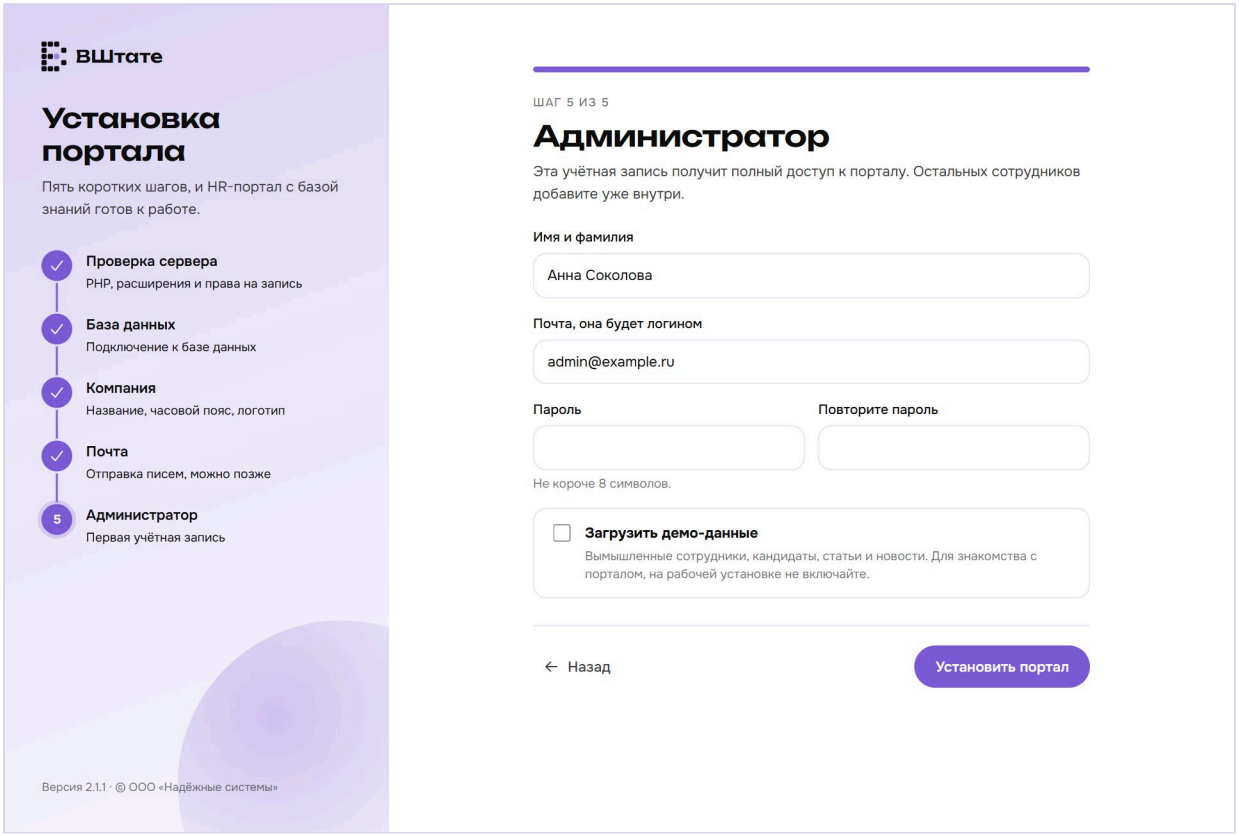
Шаг 4. Почта

Укажите SMTP-сервер, порт, шифрование, логин, пароль и адрес отправителя. Почта нужна для ссылок на тесты, смены пароля и уведомлений. Шаг можно пропустить кнопкой **Пропустить** и настроить почту позже в разделе **Настройки**.



Шаг 5. Администратор

Укажите имя и фамилию, почту и пароль не короче 8 символов: эта учётная запись получит полный доступ к порталу. Демо-данные на рабочем портале не включайте. Нажмите **Установить портал**: создание таблиц занимает до минуты, после чего откроется страница входа.



Вход через корпоративный каталог

Настройки → Вход через корпоративный каталог. Поддерживаются Active Directory, FreeIPA и OpenLDAP. Нужно расширение PHP ldap. Для Active Directory подойдёт фильтр `(&(objectClass=user)(mail=%s))`. Кнопка «Сохранить и проверить LDAP» проверяет подключение.

Обратный прокси

Если перед порталом стоит балансировщик или другой прокси, укажите его адреса в `.env`:

```
TRUSTED_PROXIES=10.0.0.5,10.0.0.6
```

Без этого в журналах и сигналах тестов будет адрес прокси, а портал может не определить HTTPS. Не указывайте `*`, если сервер доступен не только через прокси: тогда адрес сможет подделать любой посетитель.

Почта

Настраивается в мастере или в разделе **Настройки**, там же есть отправка тестового письма. Через почту уходят ссылки на тесты, смена пароля, коды входа и уведомления. Вход с кодом включайте только после проверки почты. Если вход заблокирован:

```
php artisan hr:2fa-off
```

Резервные копии

Включите копии по расписанию в разделе **Безопасность**. Архивы создаются ночью в `storage/app/backups`. Настройте их копирование на другой сервер.

Храните файл `.env` отдельно от архивов. В нём находится ключ `APP_KEY`, без которого зашифрованные данные не прочитать. Потеря ключа означает потерю этих данных.

Создать копию вручную:

```
php artisan hr:backup /надёжное/место/backup.zip
```

Восстановить на новом сервере: установите ту же версию продукта, верните прежний `APP_KEY` в `.env` и выполните:

```
php artisan migrate --force
php artisan hr:restore /надёжное/место/backup.zip
```

Смена ключа шифрования

Сначала сделайте резервную копию. Все сотрудники выйдут из портала. Старые копии будут читаться только со старым ключом.

```
php artisan hr:rotate-key
```

Обновление

1. Сделайте резервную копию и сохраните `.env`.
2. Включите режим обслуживания:

   ```
   php artisan down
   ```

3. Распакуйте новый архив поверх старой папки. Файл `.env` и папка `storage/app` в архиве отсутствуют и не перезаписываются. Удалите старую папку `vendor` перед распаковкой, чтобы не осталось лишних файлов.
4. Примените изменения и включите портал:

```
php artisan migrate --force
php artisan optimize:clear
php artisan up
```

5. Проверьте права из шага 3 установки и страницу **О системе**.

Удаление демо-данных

Демо-данные предлагает только мастер установки, их не следует включать на рабочем портале: в них есть учётные записи с известным паролем. Если они загружены случайно, переустановите портал на чистую базу.

Если что-то не работает

Признак	Что проверить
Ошибка 500	`storage/logs/laravel.log`, права на `storage` и `bootstrap/cache`
Файл не загружается	Лимиты PHP и `client_max_body_size` из шагов 4 и 5
Письма не приходят	Раздел «Настройки», тестовое письмо, журнал
Нет отметки планировщика	Задача cron, запуск от того же пользователя, что и веб-сервер
После переноса данные нечитаемы	`APP_KEY` в `.env` должен совпадать с прежним