

ГРАВИТИНОАСУР

ИНСТРУКЦИЯ ПО УСТАНОВКЕ ПО

Листов 8

2024

Мобильная версия.

Заходим в каталог Rustore <https://www.rustore.ru/>*

В поисковую строку вводим аббревиатуру «АСУР» и нажимаем поиск.

Из предложенных вариантов выбираем следующий «АСУР - система управления работами» (рисунок 1).

Также мобильную версию приложения можно скачать с Rustore напрямую по ссылке: <https://www.rustore.ru/catalog/app/com.gravitino?ysclid=m06rywa1zy600475514>.

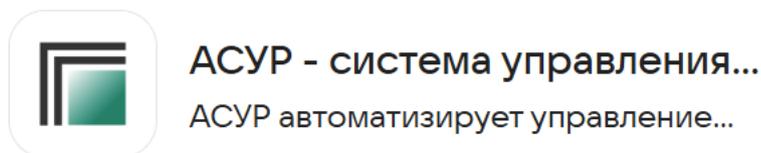


Рисунок 1 – Внешний вид приложения

Далее нажимаем кнопку установить с помощью Rustore и дожидаемся установки приложения на телефон.

После установки приложения будет предложено войти под существующим аккаунтом.

Чтобы войти в приложение введите пароль по умолчанию– 12345678. Для того, чтобы в последующем у каждого был свой индивидуальный пароль нужно ввести свою почту и пароль 12345678 и нажать «Войти». После этого сразу потребуется сменить пароль, для этого выберите надежный пароль и установите его.

*Если на телефоне требуется установка приложения Rustore следуйте инструкции на сайте «Инструкция по установке RuStore» (<https://www.rustore.ru/instruction>).

Веб-версия

Версия файла доступная для скачивания и установки находится по ссылке: <https://disk.yandex.ru/d/laiSgSjleoWBBw>.

Инструкция по установке Docker и настройке контейнера.

1. Установка Docker

1. Установка Docker на Windows

Шаг 1: Загрузка Docker Desktop

- Перейдите на официальный сайт Docker (<https://www.docker.com/products/docker-desktop/>).

- Нажмите кнопку "Download for Windows" и загрузите установочный файл.

Шаг 2: Установка Docker Desktop

1. Запустите скачанный установочный файл.
2. После завершения установки перезагрузите компьютер, если потребуется (рисунок 2).

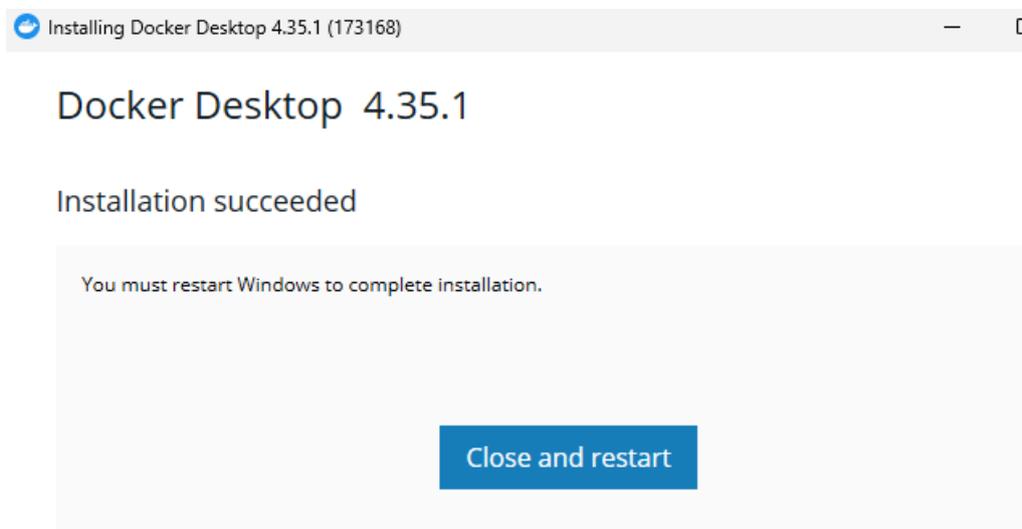


Рисунок 2 – Пример интерфейса после завершения установки

3. Запускаем Docker Desktop и принимаем соглашение (рисунок 3).

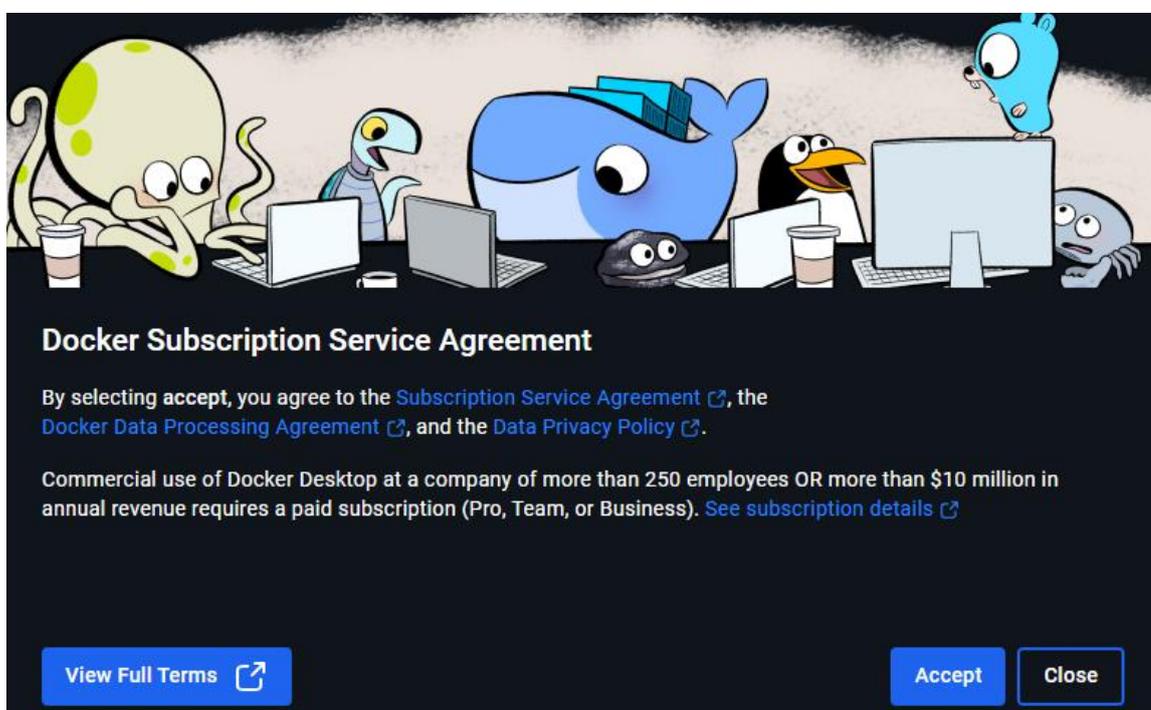


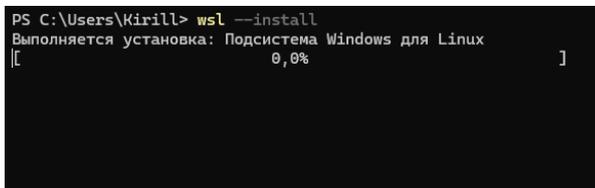
Рисунок 3 – Интерфейс принятия соглашения

Шаг 3: Настройка WSL 2

- Убедитесь, что включена поддержка Windows Subsystem for Linux 2 (WSL 2):

1. Откройте PowerShell с правами администратора.
2. Выполните команду:

```
wsl --install
```



```
PS C:\Users\Kirill> wsl --install
Выполняется установка: Подсистема Windows для Linux
[ 0,0% ]
```

3. Установите необходимую дистрибутиву Linux (по умолчанию Ubuntu):

```
wsl --set-default-version 2
```

Шаг 4: Запуск Docker Desktop

1. Запустите Docker Desktop.
2. Проверьте, работает ли Docker:
 - Откройте терминал (PowerShell) и выполните:

```
docker --version
```

- Вы должны увидеть установленную версию Docker.

2. Установка Docker на Linux

Шаг 1: Обновление пакетов

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

Шаг 2: Установка зависимостей

```
sudo apt install -y apt-transport-https ca-certificates curl software-properties-common
```

Шаг 3: Добавление Docker-репозитория

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
```

```
echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Шаг 4: Установка Docker

```
sudo apt update  
sudo apt install -y docker-ce docker-ce-cli containerd.io
```

Шаг 5: Проверка работы Docker

Проверьте установленную версию:

```
docker --version
```

Убедитесь, что служба Docker запущена:

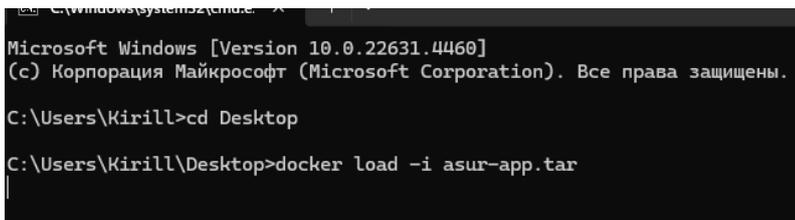
```
sudo systemctl start docker  
sudo systemctl enable docker
```

II. Развёртывание из файла (.tar)

Шаг 1: Импорт Docker-образа

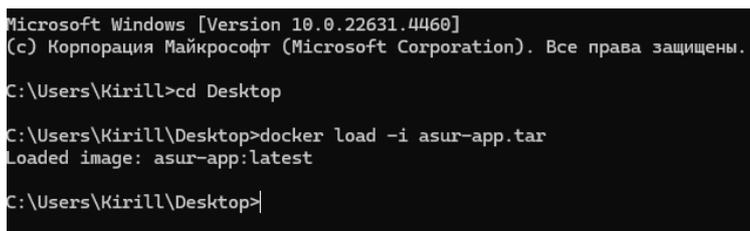
Переданный файл образа необходимо разместить в директории и выполнить команду:

```
docker load -i asur-app.tar
```



```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 10.0.22631.4460]  
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.  
C:\Users\Kirill>cd Desktop  
C:\Users\Kirill\Desktop>docker load -i asur-app.tar
```

Ожидаем распаковки контейнера:



```
Microsoft Windows [Version 10.0.22631.4460]  
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.  
C:\Users\Kirill>cd Desktop  
C:\Users\Kirill\Desktop>docker load -i asur-app.tar  
Loaded image: asur-app:latest  
C:\Users\Kirill\Desktop>
```

В Docker Desktop, в разделе Images можем увидеть контейнер asur-app (рисунок 4).

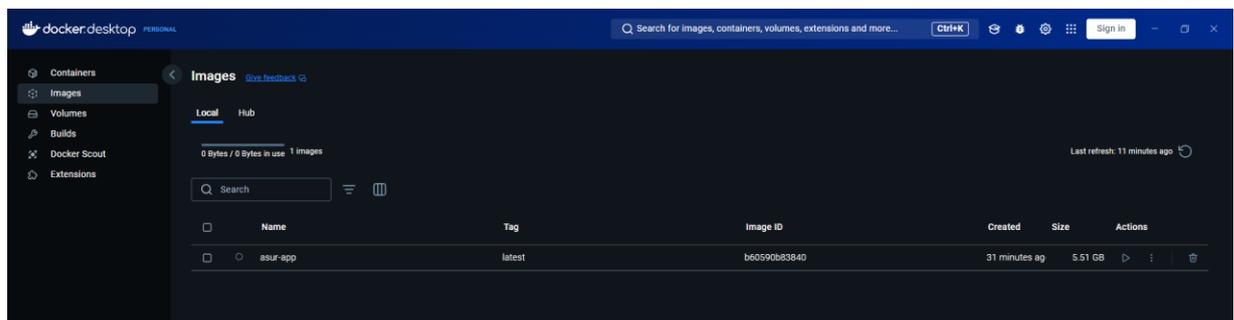


Рисунок 4 – Расположение контейнера asur-app

Шаг 2: Запуск контейнера

Запустить контейнер можно через терминал, либо через программу Docker Desktop

Для запуска через терминал выполните команду:

```
docker run -p 3001:3001 -p 3002:3002 asur-app
```

Для запуска через программу переходим во вкладку "Images", находим наш контейнер и нажимаем на кнопку "Run" (рисунок 5).

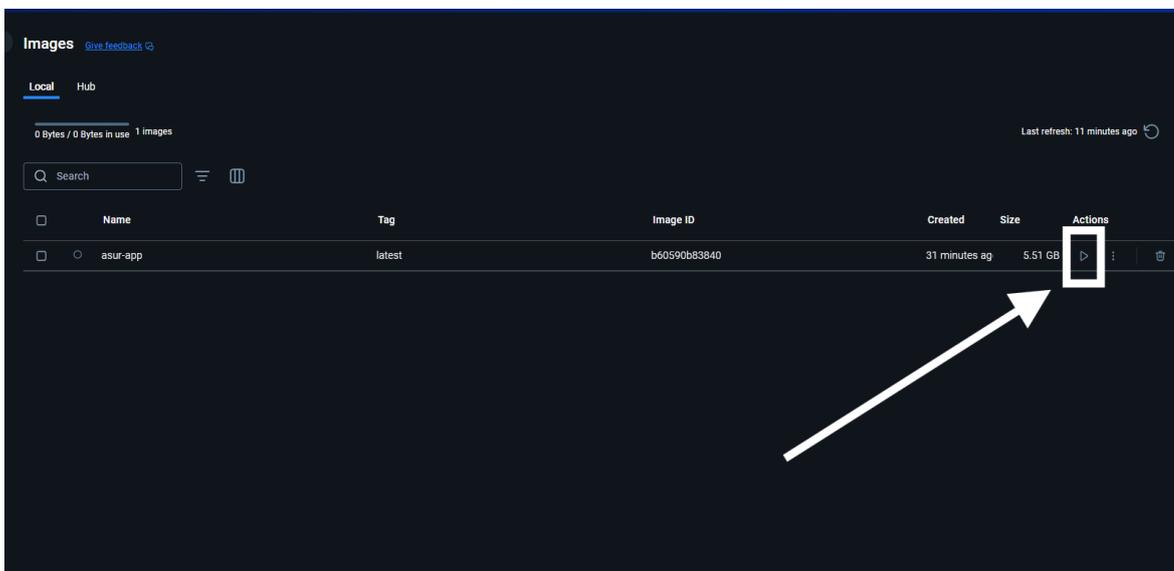


Рисунок 5 – Интерфейс запуска через программу

В настройках оставляем все по умолчанию (рисунок 6,7).

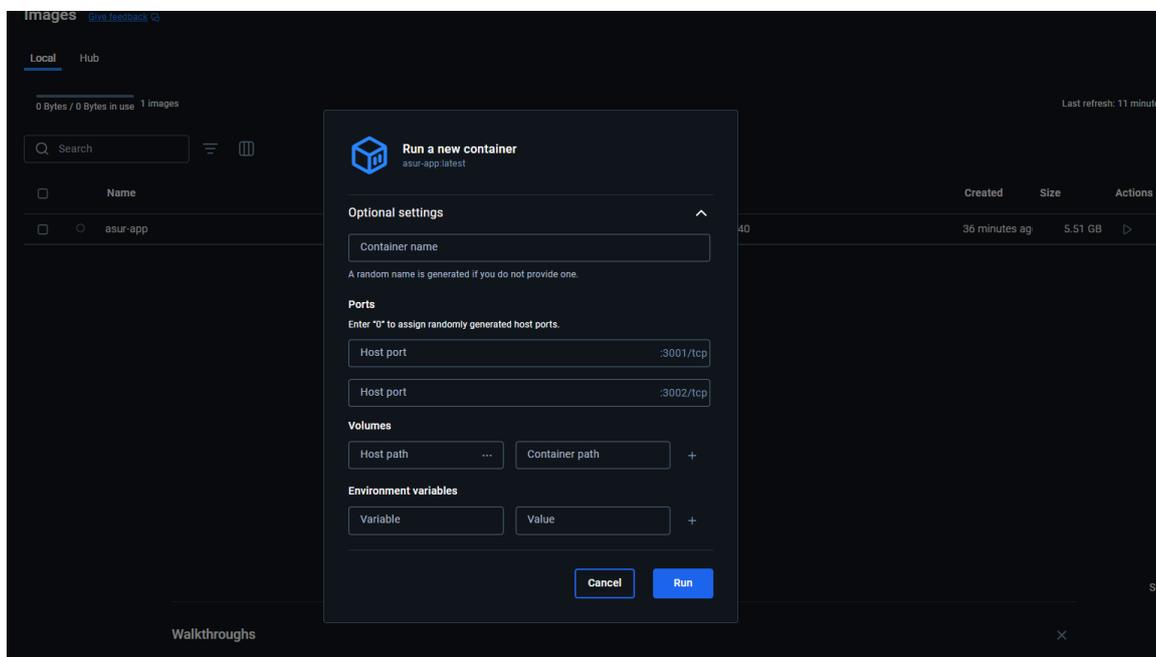


Рисунок 6 – Интерфейс настройки

```
Containers / laughing_clarke
laughing_clarke
f9ea205a571a asur-app:latest
STATUS Running (0 seconds ago)
Logs Inspect Bind mounts Exec Files Stats
2024-11-24 17:10:02 == 20240917114815-update-order-status: migrating =====
2024-11-24 17:10:02 == 20240917114815-update-order-status: migrated (0.007s)
2024-11-24 17:10:02 == 20240923875325-update-order-status: migrating =====
2024-11-24 17:10:02 == 20240923875325-update-order-status: migrated (0.007s)
2024-11-24 17:10:02 == 20240924873320-add-role-permissions: migrating =====
2024-11-24 17:10:02 == 20240924873320-add-role-permissions: migrated (0.006s)
2024-11-24 17:10:02 == 20240924873321-update-order-status: migrating =====
2024-11-24 17:10:02 == 20240924873321-update-order-status: migrated (0.007s)
2024-11-24 17:10:02 == 20240925135748-add-role-permissions: migrating =====
2024-11-24 17:10:02 == 20240925135748-add-role-permissions: migrated (0.007s)
2024-11-24 17:10:02 == 20241023884541-seed-passports: migrating =====
2024-11-24 17:10:02 == 20241023884541-seed-passports: migrated (0.008s)
2024-11-24 17:10:02 == 20241024142686-create-passport-permissions: migrating =====
2024-11-24 17:10:02 == 20241024142686-create-passport-permissions: migrated (0.008s)
2024-11-24 17:10:02 == 20241112143888-seed-new-category: migrating =====
2024-11-24 17:10:02 == 20241112143888-seed-new-category: migrated (0.006s)
2024-11-24 17:10:02 == 20241114091947-seed-permissions: migrating =====
2024-11-24 17:10:02 == 20241114091947-seed-permissions: migrated (0.007s)
2024-11-24 17:10:02 > gravitino-asu-apt@0.0.1 start
2024-11-24 17:10:02 > nest start
2024-11-24 17:10:02 > srm@0.0.0 dev
2024-11-24 17:10:02 > vite --mode development --port 3001 --open
2024-11-24 17:10:03 VITE v5.4.8 ready in 156 ms
2024-11-24 17:10:03 → Local: http://localhost:3001/
2024-11-24 17:10:03 → Network: http://172.17.0.2:3001/
2024-11-24 17:10:03 Error: spawn xdg-open ENOENT
2024-11-24 17:10:03 at ChildProcess.handle.onexit (node:internal/child_process:284:19)
2024-11-24 17:10:03 at onerrorNT (node:internal/child_process:477:10)
2024-11-24 17:10:03 at process.processTicksAndRejections (node:internal/process/task_queues:82:21)
2024-11-24 17:10:03 warn - The 'warn-' and 'max-' variants are not supported with a 'screens' configuration containing objects.
RAM 8.75 GB CPU 66.89% Disk 1019.46 GB avail of 1081.10 GB
Terminal v4.35.1
```

Рисунок 7 – Процесс запуска

После запуска необходимо подождать некоторое время для запуска контейнера. Затем переходим по адресу <http://localhost:3001> и входим в аккаунт (рисунок 8).

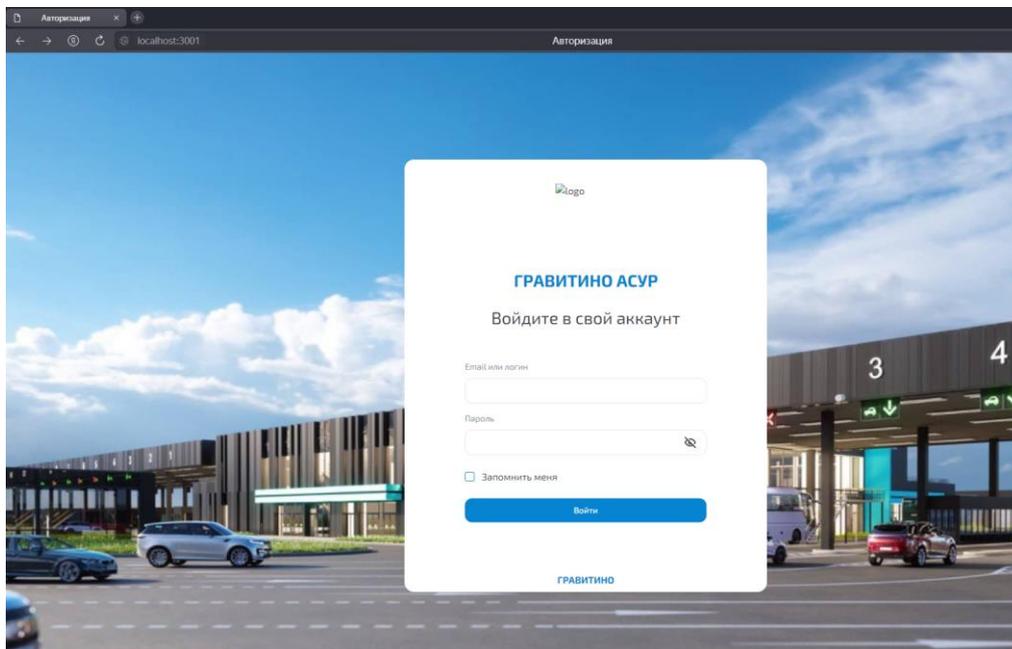


Рисунок 8 – Главная страница

Чтобы войти введите пароль по умолчанию– 12345678. Для того, чтобы в последующем у каждого был свой индивидуальный пароль нужно ввести свою почту и пароль 12345678 и нажать «Войти». После этого сразу потребуется сменить пароль, для этого выберите надежный пароль и установите его.

III. Команды Docker

1. Остановка контейнеров:

```
docker stop <container_id>
```

2. Удаление контейнеров:

```
docker rm <container_id>
```

3. Просмотр работающих контейнеров:

```
docker ps
```

4. Просмотр всех контейнеров:

```
docker ps -a
```

5. Удаление образов:

```
docker rmi <image_id>
```

Порядок проверки работоспособности

Работоспособность системы не требует от пользователя никакой дополнительной проверки.

Процессы самодиагностики, контроля и мониторинга информационной безопасности в системе выполняются полностью в автоматическом режиме. Диагностирование системы осуществляется с помощью встроенных средств диагностики технических средств, предусмотренных производителем.