

Модульная интегрированная

SCADA КРУГ-2000TM

WEB-КОНТРОЛЬTM

Версия 4.4

Администрирование

© НПФ «КРУГ», 1992-2023. Все права защищены.

Никакая часть настоящего издания ни в каких целях не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотографирование, магнитную запись или иные средства копирования или сохранения информации, без письменного разрешения владельцев авторских прав.

Все упомянутые в данном издании товарные знаки и зарегистрированные товарные знаки принадлежат своим законным владельцам.

НПФ «КРУГ»

РОССИЯ, 440028, г. Пенза, ул. Германа Титова 1

Тел. +7 (8412) 49-97-75, 49-94-14, 48-34-80,

E-mail: krug@krug2000.ru

E-mail: support@krug2000.ru

<http://www.krug2000.ru>



СОДЕРЖАНИЕ

ОБЩИЕ СВЕДЕНИЯ	2
1. УСТАНОВКА WEB-КОНТРОЛЬ.....	3
1.1 Системные требования	3
1.2 Установка электронного ключа защиты	3
1.3 Порядок установки серверной части Web-Контроль.....	4
1.3.1 Установка на выделенную (виртуальную) ПЭВМ	4
1.3.2 Установка сервера Web-Контроль на ПЭВМ Windows-10.....	11
1.3.3 Установка сервера Web-Контроль на ПЭВМ Windows Server 2019	18
2. АДМИНИСТРИРОВАНИЕ «WEB-КОНТРОЛЬ»	26
2.1 Задачи администрирования.....	26
2.1.1 Администрирование сервера Web-Контроль.....	26
2.1.2 Администрирование SCADA серверов.....	26
2.2 Защита.....	27
2.2.1 Защита от несанкционированного доступа к информации	27
2.2.2 Защита от несанкционированного использования	27
2.3 Начало работы.....	27
2.4 Управление SCADA серверами	29
2.4.1 Создание нового SCADA сервера	30
2.4.2 Изменение параметров существующих SCADA серверов.....	31
2.4.3 Удаление SCADA сервера	32
2.4.4 Настройка прав доступа к SCADA серверам	33
2.5 Управление пользователями.....	37
2.5.1 Создание новых Пользователей.....	39
2.5.2 Изменение параметров существующих пользователей	40
2.5.3 Удаление Пользователя.....	44
2.6 Управление группами.....	45
2.6.1 Создание новых групп	46
2.6.2 Изменение параметров группы	47
2.6.3 Удаление группы.....	49
3. ОБНОВЛЕНИЕ WEB-КОНТРОЛЬ БЕЗ ПОТЕРИ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ.....	50
ПРИЛОЖЕНИЕ А. ОГРАНИЧЕНИЯ ПО WEB-КОНТРОЛЬ, СВЯЗАННЫЕ С ЭЛЕКТРОННЫМ КЛЮЧОМ ЗАЩИТЫ.....	54

ОБЩИЕ СВЕДЕНИЯ

Программное обеспечение Web-Контроль™ (далее Web-Контроль) предоставляет Пользователям возможности просмотра мнемосхем, печатных документов, протокола сообщений (роллинга) абонентов систем КРУГ-2000 с помощью стандартного программного обеспечения, используемого при работе в Internet/Intranet сетях.

Отличительные характеристики Web-Контроль версии 4.4:

- Использование векторного формата для отображения мнемосхем и печатных документов, что позволяет неограниченно использовать масштабирование и детализацию изображений.
- Отсутствие необходимости использовать на стороне клиента ПО Web-Контроль стороннего программного обеспечения (виртуальной машины Java, Java-расширений для браузера, обеспечивающих работу Java-апплетов)
- Разграничение прав доступа пользователей к компонентам ПО Web-Контроль (разрешение/запрещение доступа к отдельным источникам данных, просмотру мнемосхем, архивных документов и протокола сообщений).
- Гибкая система развертывания серверной части Web-Контроль: возможность использовать как существующие ПЭВМ, работающие под управлением ОС "Windows" или "Linux", так и специально выделенные для установки серверной части Web-Контроль аппаратные или виртуальные ПЭВМ.
- Отказ от необходимости настройки DCOM для получения протокола событий
- Поддержка мобильных клиентов (планшеты/смартфоны)

Web-Контроль версии 4.4 совместим с системой SCADA КРУГ-2000 версии 4.4.

Web-Контроль включает в себя серверную (сервер) и клиентскую (клиент) части.

Администрирование *выполняется сразу после установки Web-Контроль* и включает следующие основные этапы:

- Редактирование списка серверов SCADA
- Создание Групп Безопасности
- Создание Пользователей.

1. УСТАНОВКА WEB-КОНТРОЛЬ

1.1 Системные требования

Сервер Web-Контроль

Для установки серверной части Web-контроль необходимо обеспечить работу контейнеров **Docker** (<https://www.docker.com/>) под управлением ПО **Docker-compose** (<https://github.com/docker/compose>). Установка Docker и Docker-compose возможна на ПЭВМ, работающих под управлением ОС “Linux”, а также под управлением ОС “Windows 10”, “Windows-server 2019” при наличии поддержки аппаратной виртуализации, либо с использованием виртуальной машины (например, VirtualBox) на любой ПЭВМ с ОС семейства “Windows”. В последнем случае необходимо иметь возможность предоставить для работы виртуальной машины 1Gb оперативной памяти.

Клиент Web-Контроль

- Требования к программному обеспечению.
На компьютере должно быть установлено следующее программное обеспечение:
 - Современный браузер (исключая Internet Explorer) с включённой поддержкой cookies.

1.2 Установка электронного ключа защиты

Web-Контроль при своей работе использует электронный ключ защиты Rainbow Technologies – **Sentinel SuperPro**. Электронный ключ защиты – это устройство, которое применяется для защиты программ и данных от незаконного использования. Полноценная работа с ПО Web-Контроль возможна только тогда, когда ключ подключен к компьютеру, на котором установлена серверная часть Web-Контроль, либо обеспечен сетевой доступ сервера Web-Контроль к компьютеру, на который установлен электронный ключ и сетевой менеджер лицензий Sentinel SuperPro.

Инсталлятор драйвера электронного ключа находится на фирменном диске в папке \КРУГ2000\Sentinel.

В случае отсутствия данного файла на диске следует обратиться в службу технической поддержки – support@krug2000.ru. Также инсталлятор драйвера электронного ключа можно найти на сайте SafeNet, Inc. – <http://www.safenet-inc.com>.



ВНИМАНИЕ!!!

Драйвер электронного ключа защиты устанавливается автоматически инсталлятором SCADA КРУГ-2000.



ВНИМАНИЕ!!!

Гарантируется правильная работа SCADA КРУГ-2000 только с драйвером Sentinel из состава дистрибутива SCADA.

Более подробно установка электронного ключа защиты описана в книге «Введение в КРУГ-2000» в разделе «Подготовка к работе SCADA КРУГ-2000».

1.3 Порядок установки серверной части Web-Контроль

1.3.1 Установка на выделенную (виртуальную) ПЭВМ

Наиболее простой вариант установки серверной части Web-Контроль - использование преднастроенного дистрибутива на основе ОС Linux, который может быть развернут на выделенной, либо виртуальной ПЭВМ. Образ установочного диска - файл WebControl.iso необходимо скопировать на выбранный для установки загрузочный носитель:

- в случае использования USB Flash диска - можно воспользоваться утилитой Win32 Disk Imager, или любым другим доступным способом скопировать образ загрузочного диска на USB Flash диск;
- в случае использования для загрузки DVD-привода - записать образ установочного диска на DVD-R оптический диск;
- в случае установки сервера на виртуальную машину - выбрать файл WebControl.iso в качестве образа виртуального загрузочного диска;

Выполните загрузку с подготовленного носителя (рисунок 1.1):

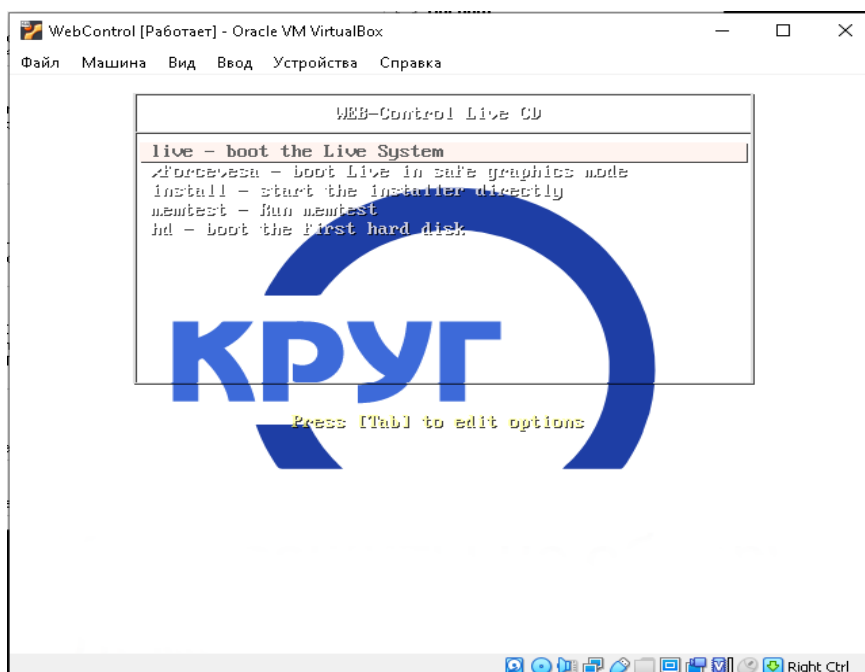


Рисунок 1.1 – Страница выбора варианта загрузки

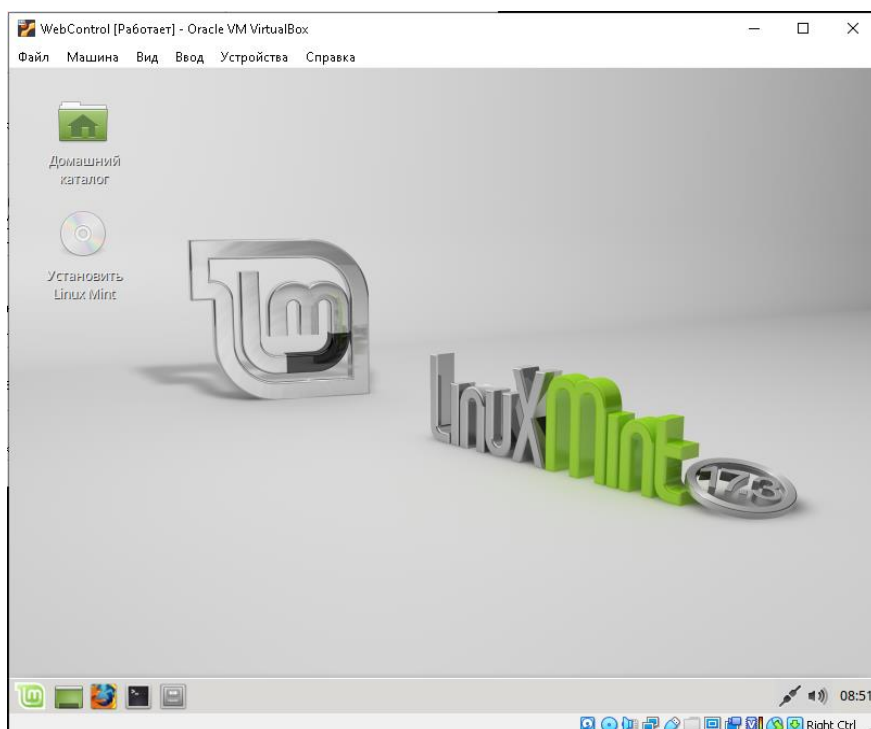


Рисунок 1.2 – Рабочий стол после загрузки установочного образа системы.

Запустите программу установки, используя соответствующую пиктограмму на рабочем столе (рисунок 1.2), выберите язык (русский) для установки сервера WebControl (рисунок 1.3):

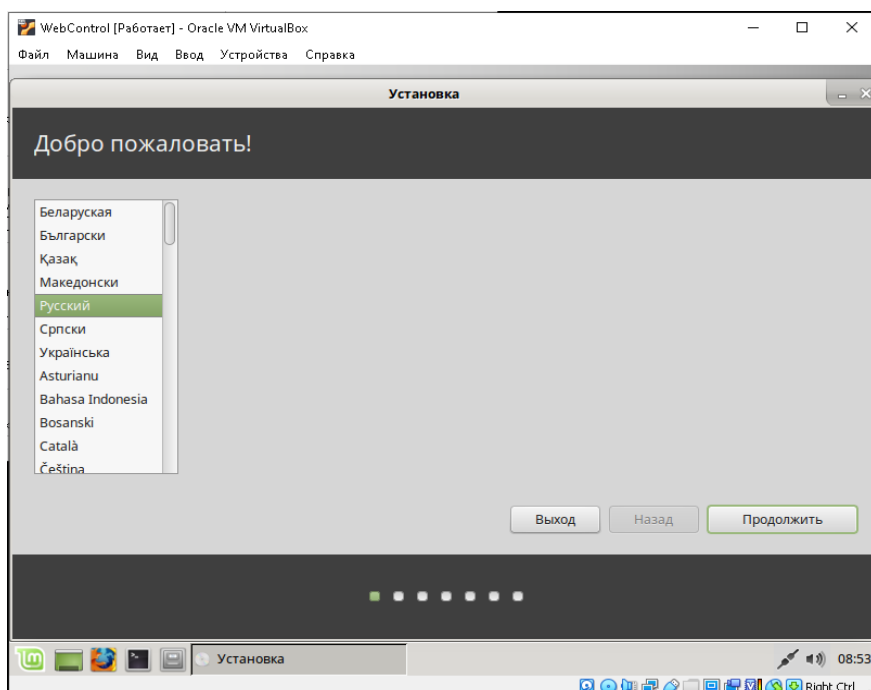


Рисунок 1.3 – Выбор языка установки.

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

Продолжите установку. Выберите вариант использования локального диска (рисунок 1.4):

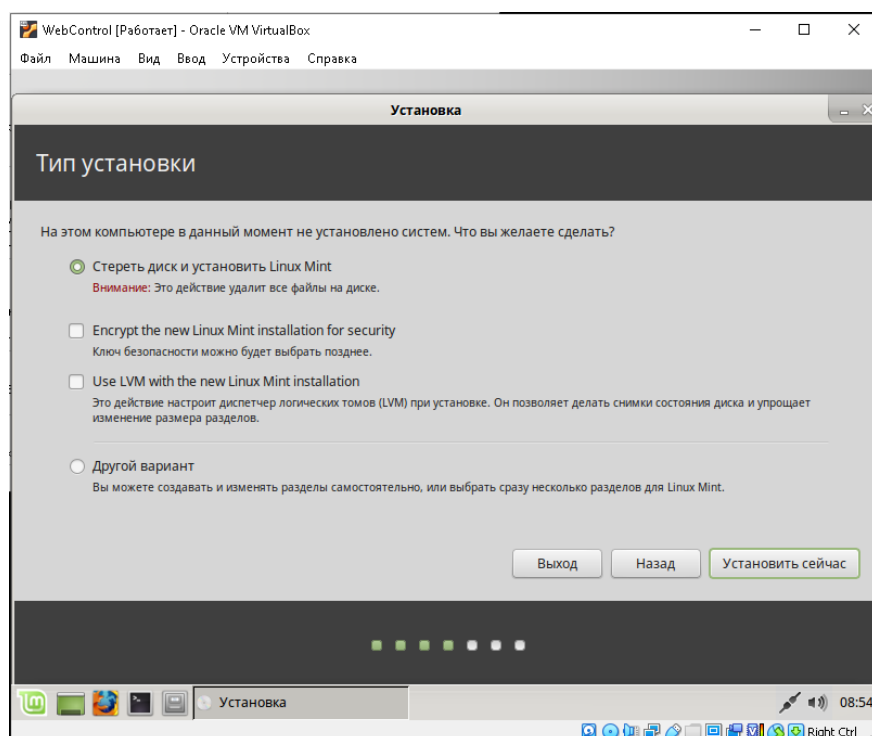


Рисунок 1.4 – Выбор варианта использования диска.

Продолжите установку. Выберите часовой пояс:

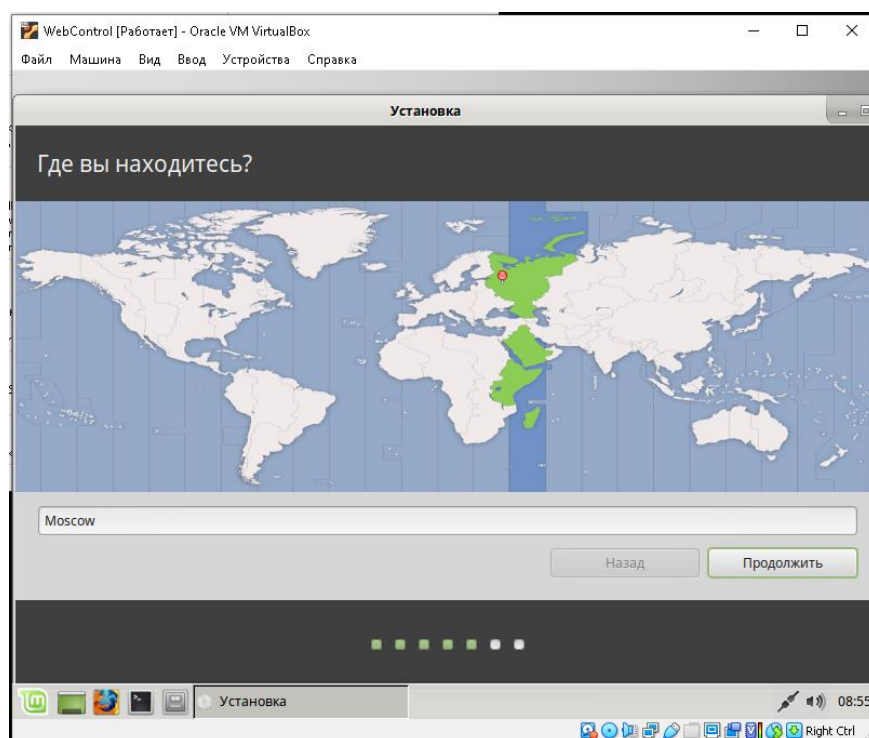


Рисунок 1.5 – Выбор часового пояса.

Продолжите установку. Подтвердите использование русской раскладки клавиатуры:

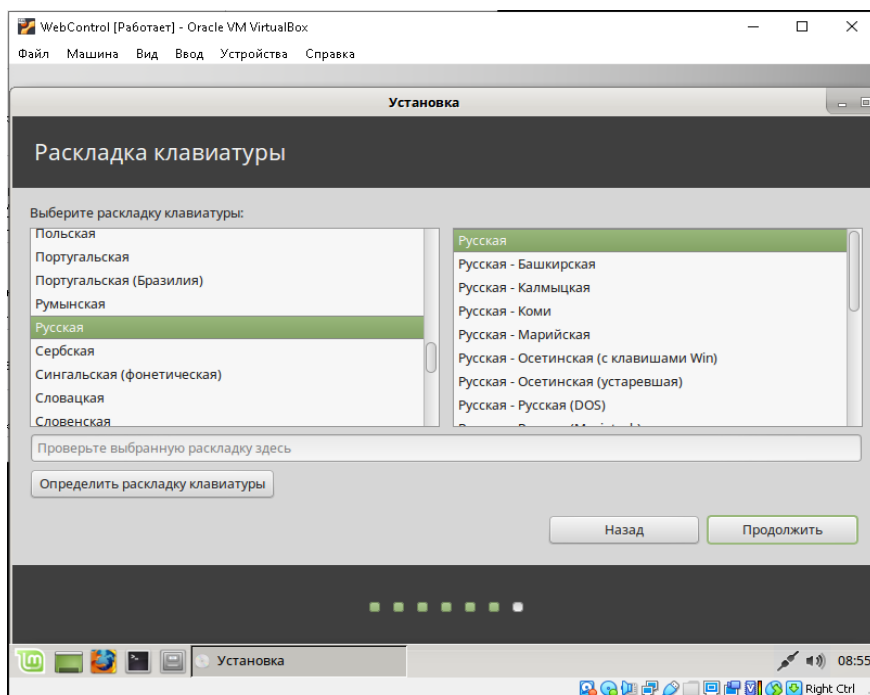


Рисунок 1.6 – Выбор раскладки клавиатуры.

Продолжите установку. Укажите параметры учетной записи пользователя, имя компьютера и параметры входа в систему (рисунок 1.7):

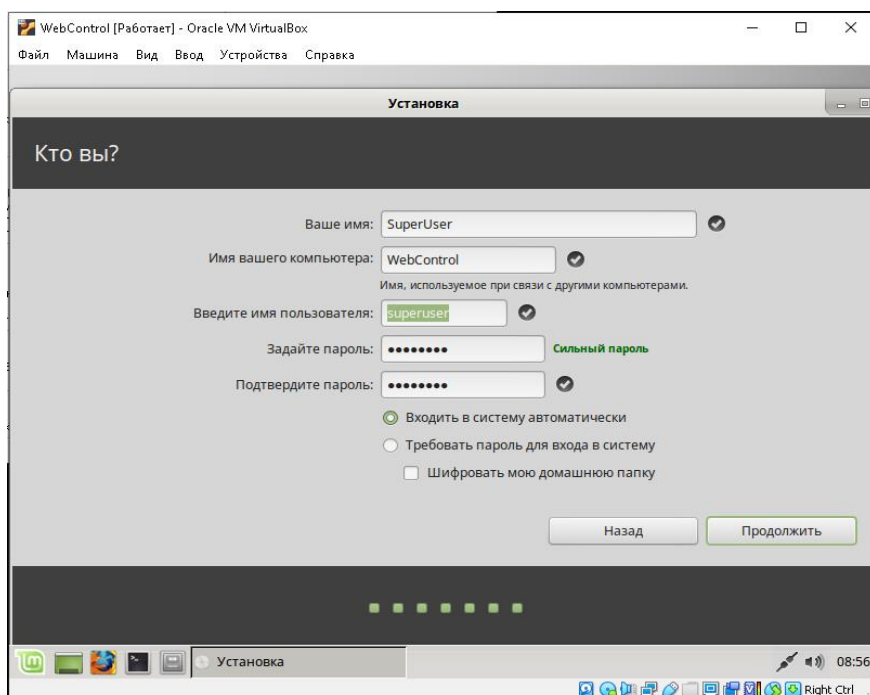


Рисунок 1.7 – Создание учетной записи пользователя.

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

Нажмите «Продолжить» и дождитесь окончания установки (рисунок 1.8, рисунок 1.9):

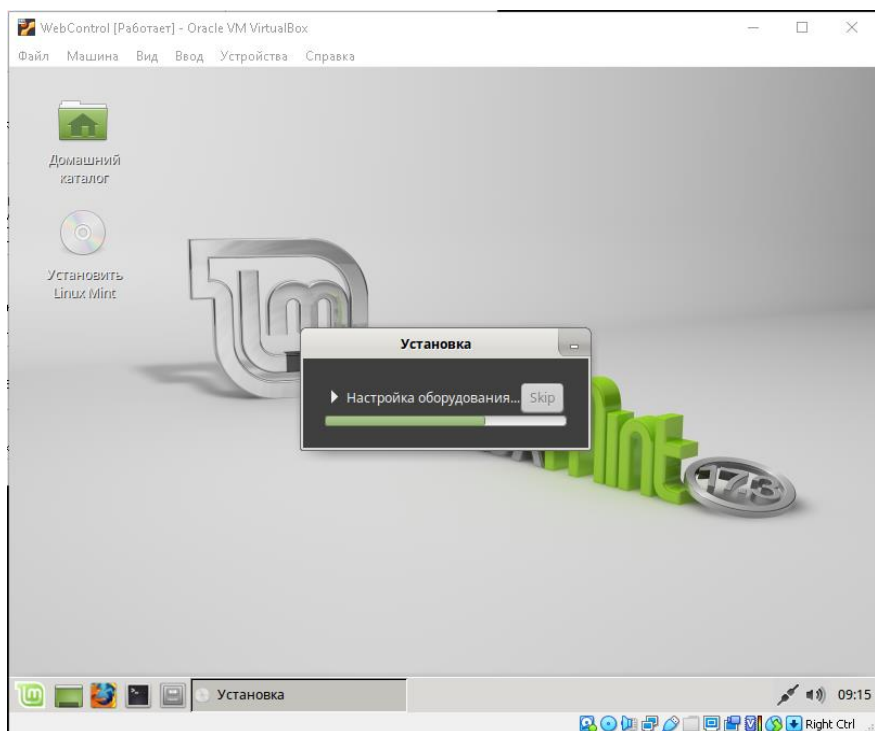


Рисунок 1.8 – Установка.

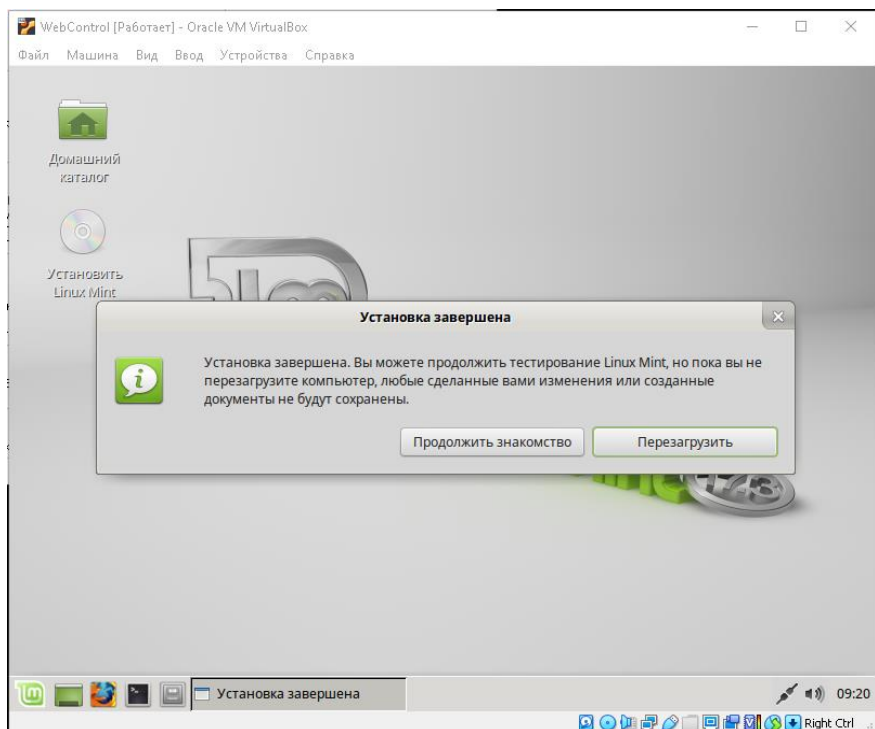


Рисунок 1.9 – Окончание установки.

После перезагрузки настройте (если необходимо) параметры доступа к сети (рисунок 1.10, рисунок 1.11):

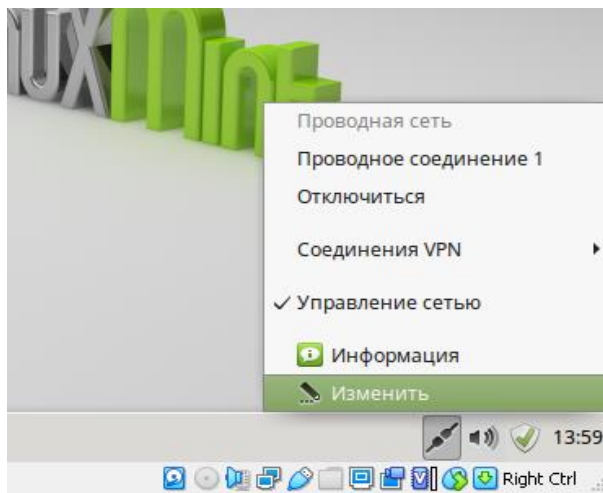


Рисунок 1.10 – Изменение сетевых настроек.

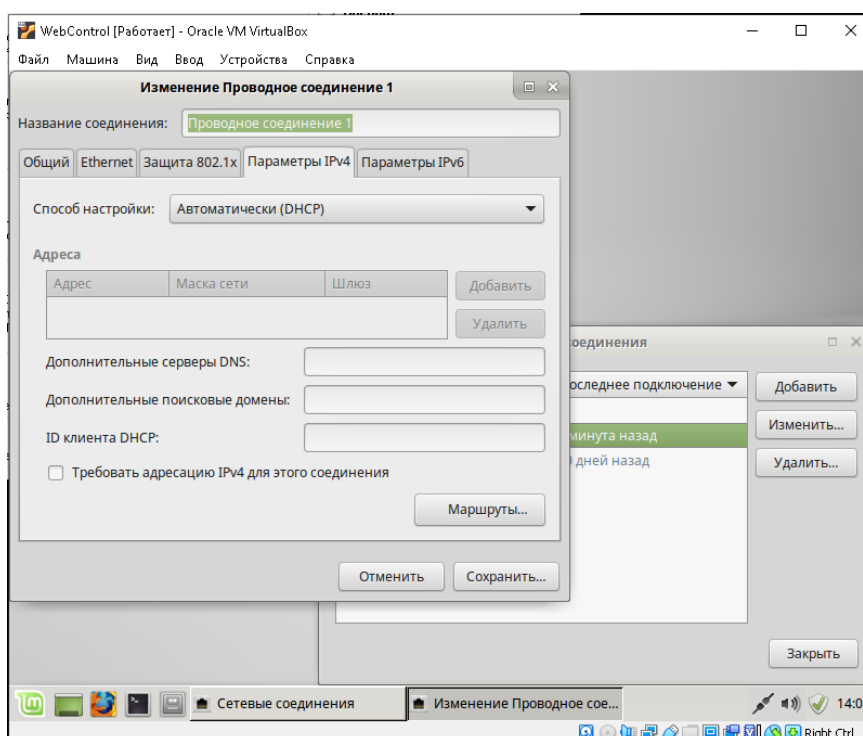


Рисунок 1.11 – Настройка параметров сетевого соединения.

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

В случае использования виртуальной машины необходимо заранее настроить свойства виртуального сетевого интерфейса и “проброс” сетевого порта 8080 (рисунок 1.12):

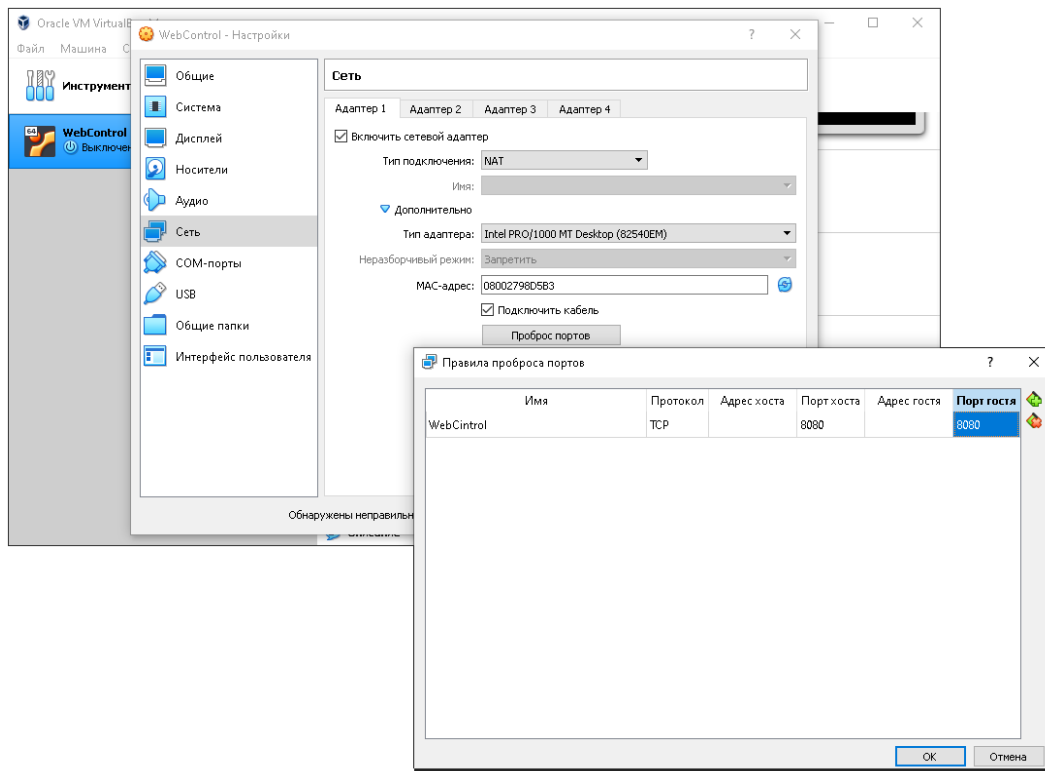


Рисунок 1.12 – Сетевые настройки виртуальной машины.

Для автоматического старта виртуальной машины можно создать и добавить в автозагрузку пакетный файл **WebControl.bat**, содержащий команду запуска. Для этого выполните следующие действия:

1. Кликните правой кнопкой мыши в любом свободном месте рабочего стола и выберите пункт «Создать» → «Текстовый документ». Укажите имя документа (**WebControl**) и нажмите Enter.
2. Откройте файл для редактирования и запишите туда команду:

```
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" startvm WebControl --type headless
```

где **WebControl** - имя виртуальной машины (применимо для VirtualBox).

3. В меню «Файл» выберите пункт «Сохранить как...», измените тип файла на «Все файлы», при необходимости отредактируйте имя файла, после него поставьте точку и добавьте расширение **bat**. Нажмите «Сохранить».
4. Вызовите окно «Выполнить» выбрав соответствующий пункт в контекстном меню кнопки «Пуск» или сочетанием клавиш **Win+R**), введите команду **shell:startup** и нажмите OK.
5. В открывшееся окно автозагрузки перетащите файл **WebControl.bat**.

После перезагрузки сервер Web-Контроль готов к работе. Доступ к панели администрирования можно получить, открыв в браузере страницу с адресом вида:

<http://192.168.0.248:8080/admin/>

где 192.168.0.248 - адрес ПЭВМ, на которой установлен сервер Web-Контроль (либо адрес ПЭВМ, где развернута виртуальная машина с сервером Web-Контроль).

Для авторизации используется учетная запись с именем **admin** и паролем **admin**.

1.3.2 Установка сервера Web-Контроль на ПЭВМ Windows-10

Для установки сервера Web-Контроль на компьютер с операционной системой Windows-10 необходимо предварительно установить и настроить ПО **Docker Desktop**. Это возможно при соблюдении следующих требований к оборудованию:

- 64-битный процессор с преобразованием адресов второго уровня (SLAT);
- Системная оперативная память 4 ГБ или более;
- Поддержка аппаратной виртуализации на уровне BIOS должна быть включена в настройках BIOS;
- установлена 64-разрядная версия Windows 10: Pro, Enterprise или Education (сборка 16299 или новее)

Перед установкой ПО Docker Desktop необходимо подключить компоненты Windows Hyper-V:

1. Щелкните правой кнопкой мыши по кнопке Windows и в появившемся меню выберите пункт «Найти».
2. В строке поиска введите «компонент» и в результатах поиска выберите «Включение или отключение компонентов Windows» (рисунок 1.13).
3. Отметьте пункт «Hyper-V» и подтвердите нажатием кнопки «Ок» (рисунок 1.14)

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

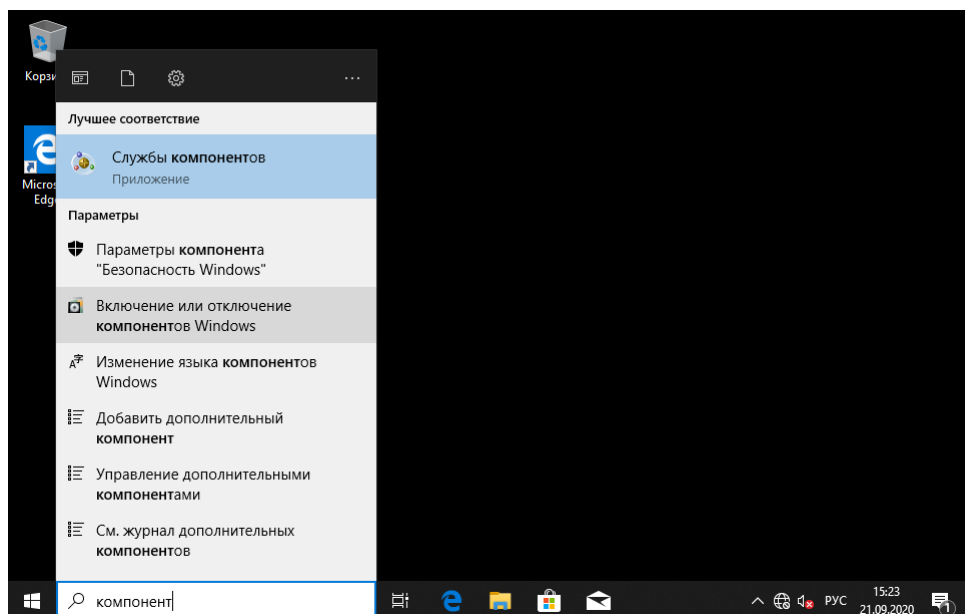


Рисунок 1.13 – Запуск оснастки «Компоненты Windows».

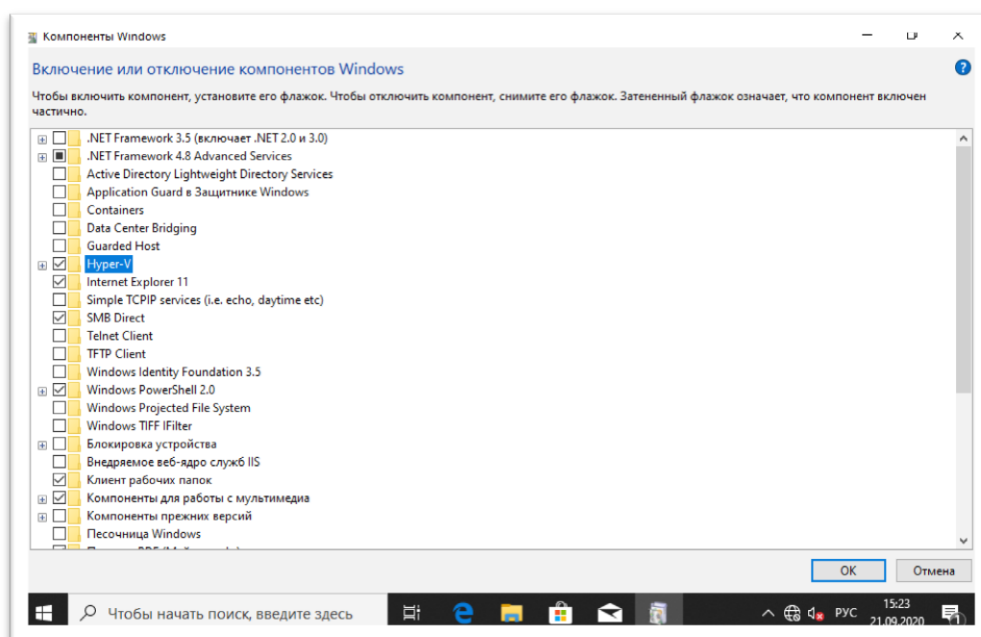


Рисунок 1.14 – Подключение компонента виртуализации.

После применения изменений потребуется перезагрузка операционной системы.

Для установки ПО «Docker Desktop» скачайте инсталлятор с сайта <https://www.docker.com> и запустите **Docker Desktop Installer.exe**.

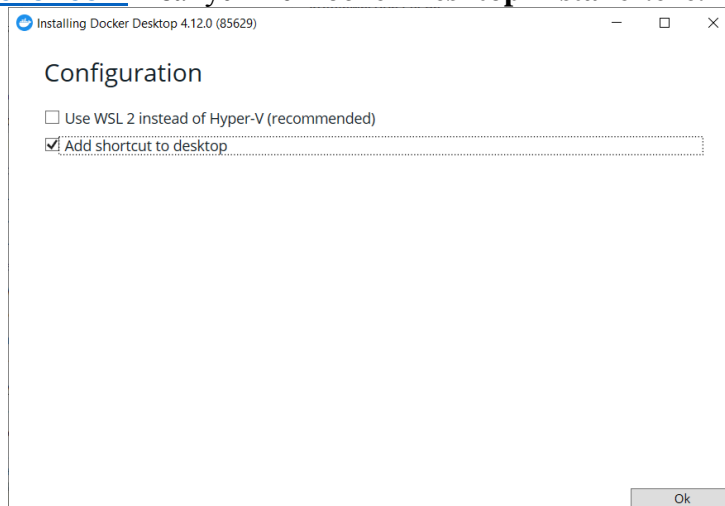


Рисунок 1.15 – Установка Docker Desktop.

После установки ПО «Docker Desktop» потребуется повторный вход в систему для применения разрешений, назначенных учетной записи пользователя.

Для установки сервера Web-Контроль нужно создать каталог, в который затем распаковать из архива **WebControl.tgz** необходимую структуру файлов и папок WEB-приложения. Распаковать архив можно, например, открыв от имени администратора классическую командную строку и выполнив в ней следующую команду:

```
tar -xvzf E:\web-control_install\WebControl.tgz -C E:\web-control
```

где - **E:\web-control_install\WebControl.tgz** – путь к архиву,
E:\web-control – путь к целевой папке.

ВНИМАНИЕ: Оболочки командной строки используют пробел для разделения команд и аргументов. Поэтому, если в пути имеется файл или папка, содержащие в своем названии пробел, то весь путь необходимо заключить в двойные кавычки. Например, `tar -xvzf "E:\web-control_install\WebControl 4.4.4.tgz" -C "E:\web control"`

Перед началом работы необходимо запустить Docker Desktop. Для этого выполните поиск Docker и выберите Docker Desktop в результатах поиска, либо используйте ярлык, созданный на рабочем столе. Для автоматического запуска Docker Desktop при включении или перезагрузке ПК необходимо в настройках Docker Desktop на вкладке General поставить галочку напротив пункта «Start Docker Desktop when you log in», а затем нажать кнопку «Apply and restart».

Дальнейшие действия необходимо производить в командной оболочке PowerShell, запущенной из каталога проекта.

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

Для этого откройте в проводнике Windows папку проекта, распакованную из архива **WebControl.tgz**, (в корне папки должен находиться файл **docker-compose.yml**) и кликните в окне проводника правой кнопкой мыши при зажатой клавише Shift. В открывшемся контекстном меню выберите - "Открыть окно PowerShell здесь" (рисунок 1.16).

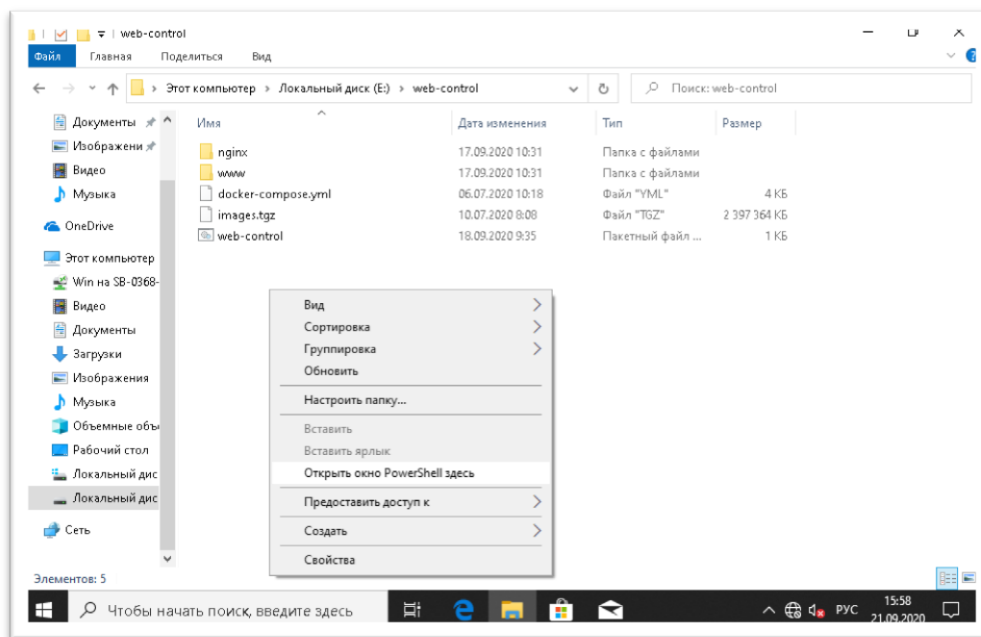
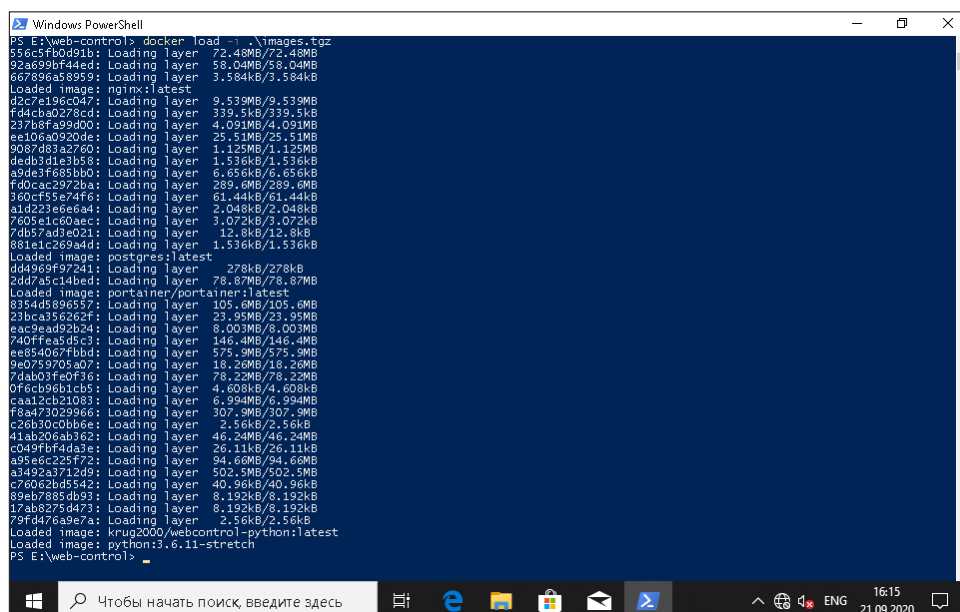


Рисунок 1.16 – Запуск командной оболочки PowerShell.

В командной оболочке PowerShell выполните команду:

```
docker load -i images.tgz
```



При этом будет выполнена загрузка необходимых Docker-образов из архива (рисунок 1.17).

Рисунок 1.17 – Развертывание Docker-образов из архива.

После выполнения этих шагов WEB-приложение готово к запуску командой:

docker-compose up -d

При этом необходимо в ответ на запрос разрешить совместное использование раздела жесткого диска и подтвердить это вводом пароля текущего пользователя (рисунок 1.18).

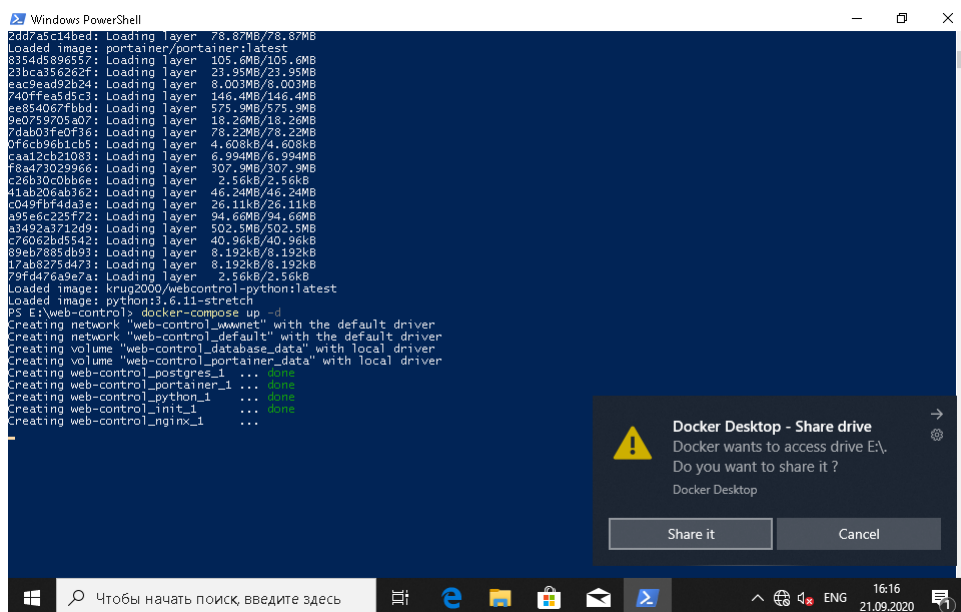
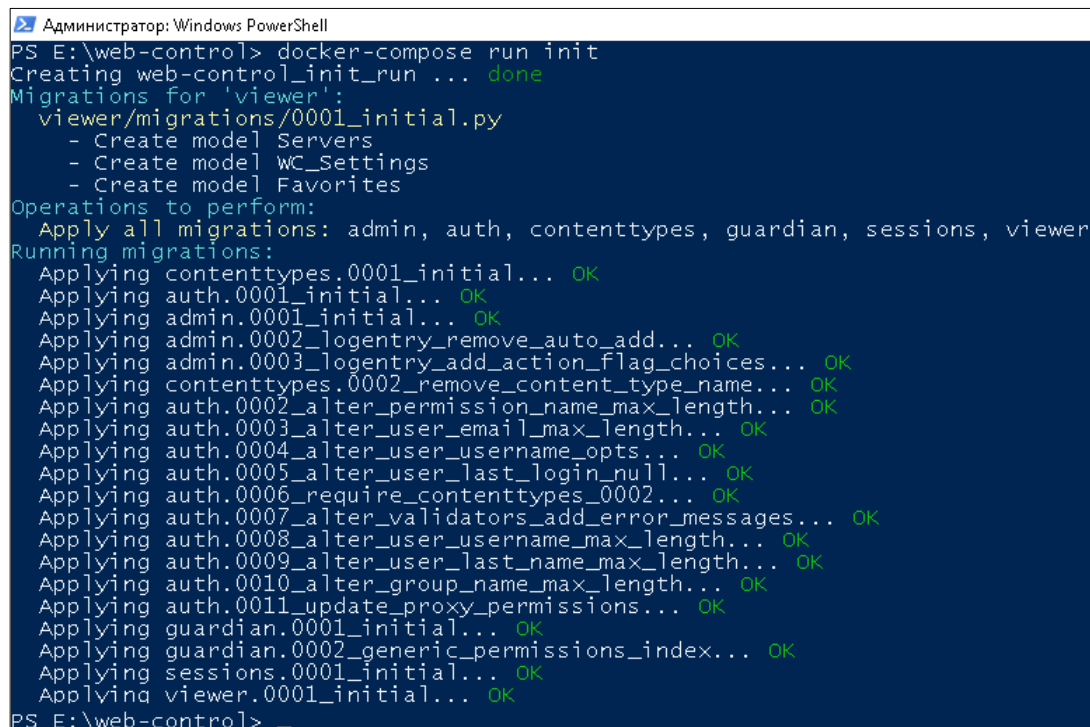


Рисунок 1.18 – Первый запуск приложения Web-Контроль

После первого запуска приложения выполните начальную инициализацию базы данных приложения командой (рисунок 1.19):

docker-compose run init

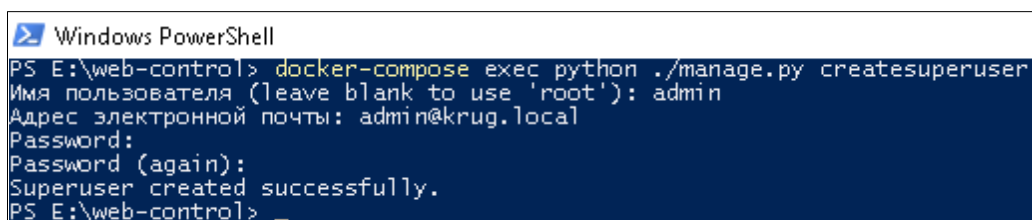


```
Администратор: Windows PowerShell
PS E:\web-control> docker-compose run init
Creating web-control_init_run ... done
Migrations for 'viewer':
  viewer/migrations/0001_initial.py
    - Create model Servers
    - Create model WC_Settings
    - Create model Favorites
Operations to perform:
  Apply all migrations: admin, auth, contenttypes, guardian, sessions, viewer
Running migrations:
  Applying contenttypes.0001_initial... OK
  Applying auth.0001_initial... OK
  Applying admin.0001_initial... OK
  Applying admin.0002_logentry_remove_auto_add... OK
  Applying admin.0003_logentry_add_action_flag_choices... OK
  Applying contenttypes.0002_remove_content_type_name... OK
  Applying auth.0002_alter_permission_name_max_length... OK
  Applying auth.0003_alter_user_email_max_length... OK
  Applying auth.0004_alter_user_username_opts... OK
  Applying auth.0005_alter_user_last_login_null... OK
  Applying auth.0006_require_contenttypes_0002... OK
  Applying auth.0007_alter_validators_add_error_messages... OK
  Applying auth.0008_alter_user_username_max_length... OK
  Applying auth.0009_alter_user_last_name_max_length... OK
  Applying auth.0010_alter_group_name_max_length... OK
  Applying auth.0011_update_proxy_permissions... OK
  Applying guardian.0001_initial... OK
  Applying guardian.0002_generic_permissions_index... OK
  Applying sessions.0001_initial... OK
  Applying viewer.0001_initial... OK
PS E:\web-control>
```

Рисунок 1.19 – Инициализация базы данных.

Для выполнения задач администрирования необходимо создать учетную запись администратора. Для этого выполните команду (рисунок 1.20):

```
docker-compose exec python ./manage.py createsuperuser
```



```
Windows PowerShell
PS E:\web-control> docker-compose exec python ./manage.py createsuperuser
Имя пользователя (leave blank to use 'root'): admin
Адрес электронной почты: admin@krug.local
Password:
Password (again):
Superuser created successfully.
PS E:\web-control>
```

В ответ на запрос укажите имя учетной записи (например, **admin**) и пароль.

Рисунок 1.20 – Создание учетной записи администратора.

После выполненных настроек доступ к панели администрирования можно получить, открыв в браузере страницу с адресом вида:

<http://192.168.0.248:8080/admin/>

где 192.168.0.248 - адрес ПЭВМ, на которой установлен сервер Web-Контроль. Для авторизации используется созданная ранее учетная запись администратора.

После перезапуска ПЭВМ сервер Web-Контроль автоматически стартует после запуска ПО **Docker Desktop**.

Для доступа к панели администрирования с удаленных компьютеров необходимо создать правило брандмауэра для входящих подключений, разрешающее доступ к порту 8080 (рисунок 1.21):

1. Откройте окно «Монитор брандмауэра...» (через поиск).
2. В левой части окна выберите «Правило для входящих подключений», затем кликните правой кнопкой мыши по выбранному пункту и в появившемся меню выберите «Создать правило...»
3. Выберите: Тип правила – для порта; Протокол и порты – Протокол TCP, Определенные протоколы и порты, порт 8080 (рисунок 1.21).

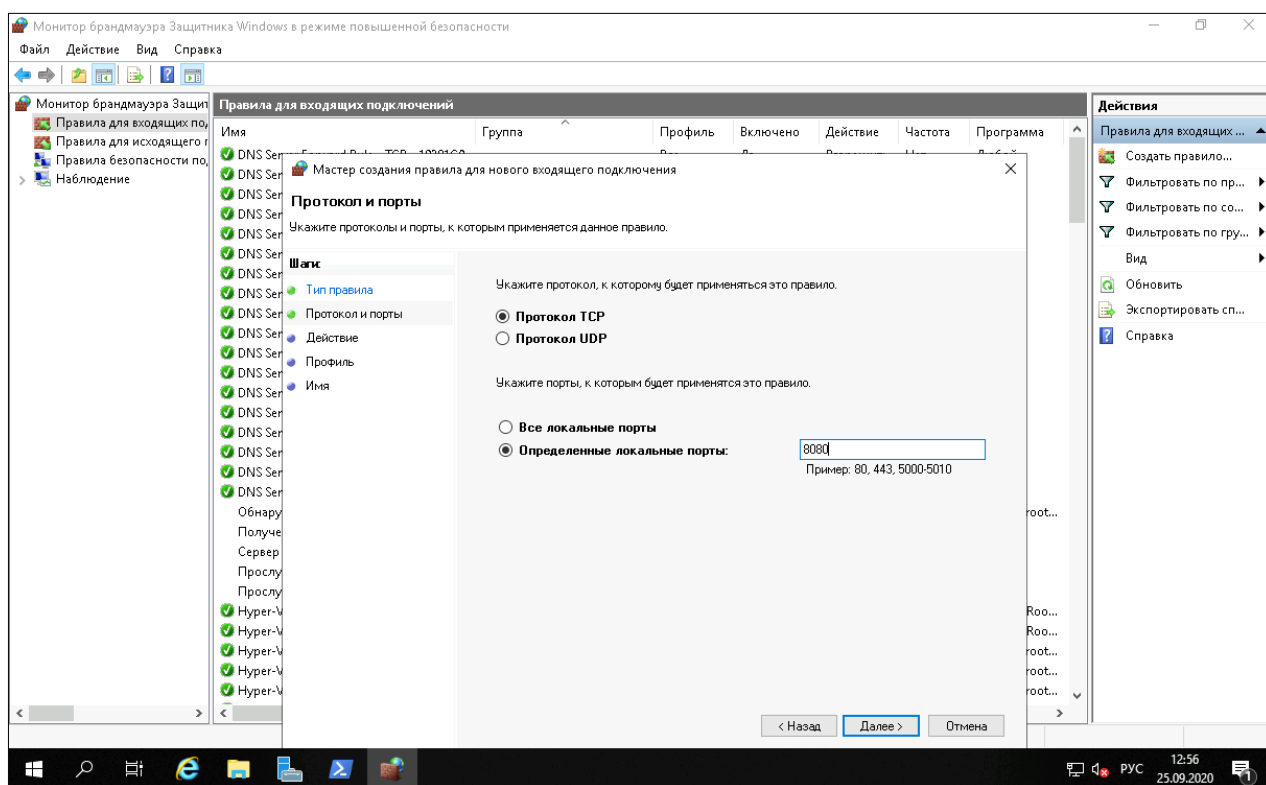


Рисунок 1.21 – Создание правила брандмауэра.

Для остановки сервера Web-Контроль необходимо в командной оболочке PowerShell, запущенной в каталоге WEB-приложения, выполнить команду:

docker-compose down

 **ВНИМАНИЕ!!!**

Выполнять команду запуска/остановки приложения нужно в папке, где присутствует файл docker-compose.yml

1.3.3 Установка сервера Web-Контроль на ПЭВМ Windows Server 2019

Для установки сервера Web-Контроль на компьютер с операционной системой Windows Server-2019 необходимо предварительно установить и настроить сервис Docker для работы с контейнерами Linux.

Перед установкой и настройкой сервиса Docker необходимо включить функции Hyper-V и Windows-контейнера. Для этого откройте оболочку PowerShell от имени администратора (кликните правой кнопкой по кнопке «Пуск» и выберите пункт «Windows PowerShell (администратор)») и выполните в ней следующие команды (рисунок 1.22):

```
Install-WindowsFeature -Name Hyper-V,Containers -IncludeAllSubFeature  
-IncludeManagementTools
```

После чего перезагрузите систему.

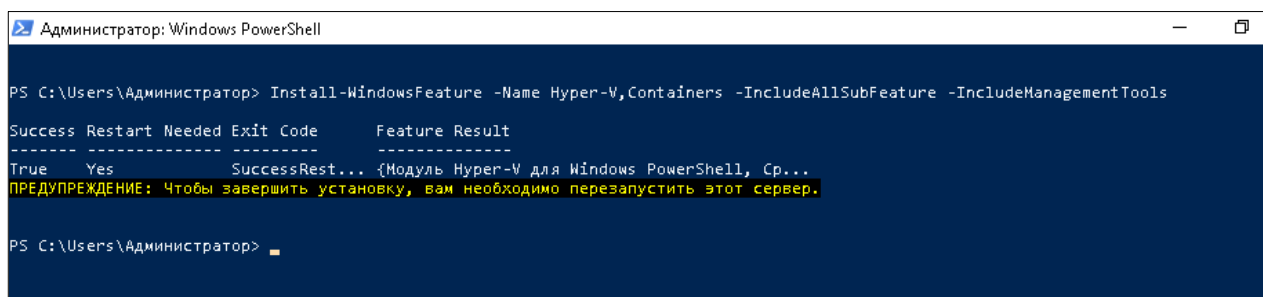


Рисунок 1.22 – Включение функций Hyper-V и Containers.

Следующим шагом необходимо установить поставщика пакетов, содержащего последнюю версию Docker. Для этого выполняются команды (рисунок 1.23):

```
Install-Module DockerMSFTProvider
```

```
Import-Module -Name DockerMSFTProvider -Force
```

```
Import-Packageprovider -Name DockerMSFTProvider -Force
```

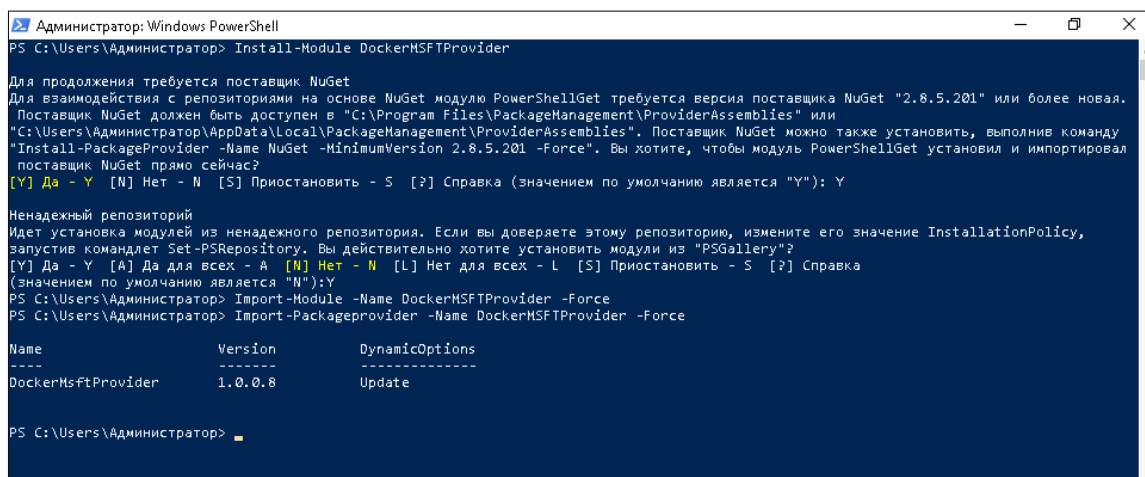


Рисунок 1.23 – Установка поставщика Docker.

Следующие команды устанавливают сервис Docker (рисунок 1.24):

```
Install-Package -Name Docker -Source DockerDefault
```

и включают поддержку контейнеров Linux (рисунок 1.24):

```
[Environment]::SetEnvironmentVariable("LCOW_SUPPORTED", "1", "Machine")
```

```
Start-service Docker
```

```
$configfile = @"
{
    "experimental": true
}
"@
```

```
$configfile | Out-File -FilePath
C:\ProgramData\docker\config\daemon.json -Encoding ascii -Force
```

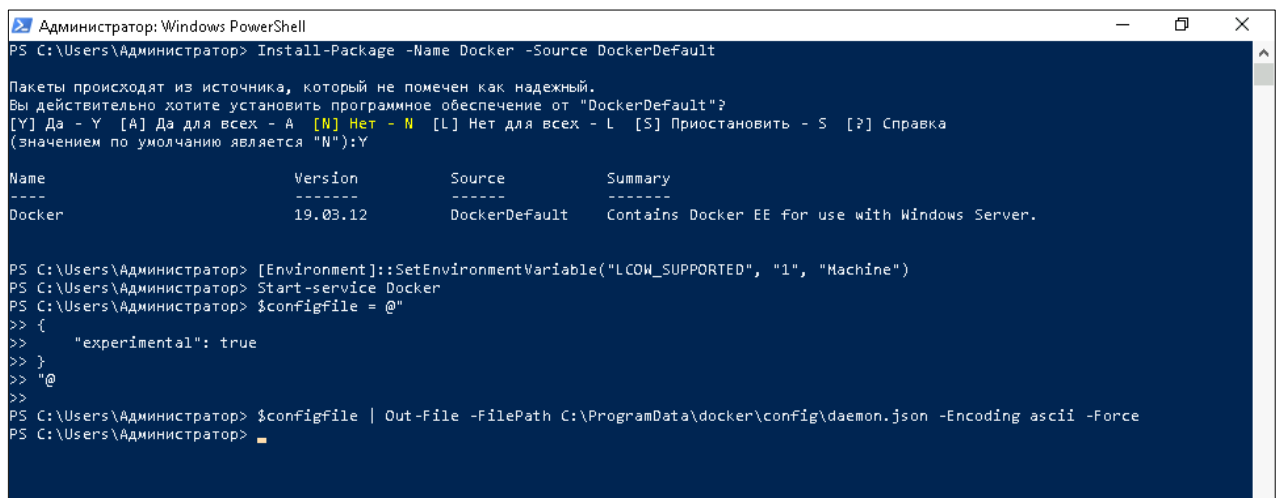


Рисунок 1.24 – Установка сервиса Docker с поддержкой контейнеров Linux.

Развертываем LCOW для запуска ядра Linux с помощью следующих команд (рисунок 1.25):

```
Invoke-WebRequest -Uri
"https://github.com/linuxkit/lcow/releases/download/v4.14.35-
v0.3.9/release.zip" -UseBasicParsing -OutFile release.zip
```

```
Expand-Archive release.zip -DestinationPath "$Env:ProgramFiles\Linux
Containers\."
```

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

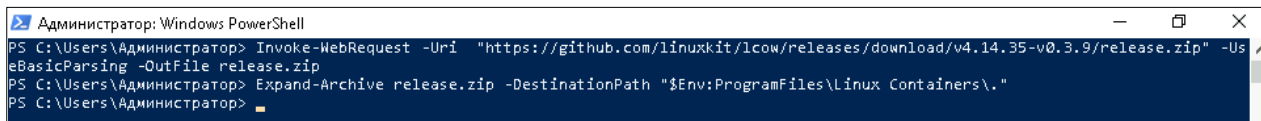


Рисунок 1.25 – Импорт ядра системы Linux.

В заключении установите ПО Docker-compose актуальной версии. Для этого выполните команды (рисунок 1.26):

```
$dockerComposeVersion = "1.27.3"
```

Invoke-WebRequest

```
"https://github.com/docker/compose/releases/download/$dockerComposeVersion/docker-compose-Windows-x86_64.exe" -UseBasicParsing -OutFile $Env:ProgramFiles\docker\docker-compose.exe
```

ВНИМАНИЕ: если при выполнении последней команды возникла ошибка («Invoke-WebRequest : Запрос был прерван: Соединение было неожиданно закрыто.»), то с помощью поиска найдите актуальную версию **Docker-compose** (<https://github.com/docker/compose/releases>), в предыдущей команде (`$dockerComposeVersion = "1.27.3"`) замените номер версии на актуальный, скопируйте ссылку на файл `docker-compose-windows-x86_64.exe` и вставьте новую ссылку в последнюю команду (`Invoke-WebRequest "<ссылка на скачивание файла>" -UseBasicParsing -OutFile $Env:ProgramFiles\docker\docker-compose.exe`)

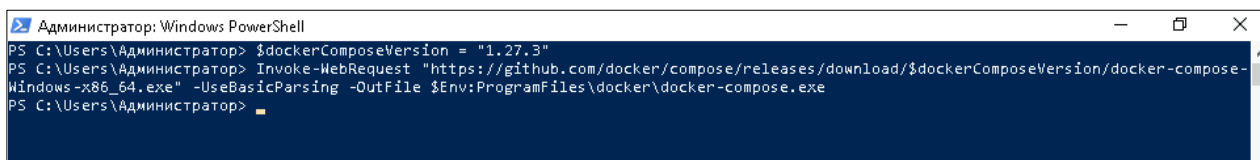


Рисунок 1.26 – Установка Docker-compose.

После этого перезагрузите систему

Для установки сервера Web-Контроль необходимо создать каталог, в который будет распакована из архива **WebControl.tgz** необходимая структура файлов и папок WEB-приложения. Для распаковывания архива выполните следующую команду в командной оболочке PowerShell:

```
tar -xvzf E:\web-control_install\WebControl.tgz -C E:\web-control
```

где - `E:\web-control_install\WebControl.tgz` – путь к архиву,
 `E:\web-control` – путь к целевой папке.

Дальнейшие действия необходимо производить в командной оболочке PowerShell, запущенной от имени администратора из каталога проекта. Для этого откройте оболочку PowerShell от имени администратора (кликните правой кнопкой по кнопке «Пуск» и

выберите пункт «Windows PowerShell (администратор)» и перейдите в каталог, в котором располагается необходимая структура файлов и папок WEB-приложения, выполнив команду:

```
cd E:\web-control
```

где - **E:\web-control** – путь к папке, в корне которой находится файл **docker-compose.yml**.

В командной оболочке PowerShell выполните команду:

```
docker load -i images.tgz
```

При этом будет выполнена загрузка необходимых Docker-образов из архива (рисунок 1.27).

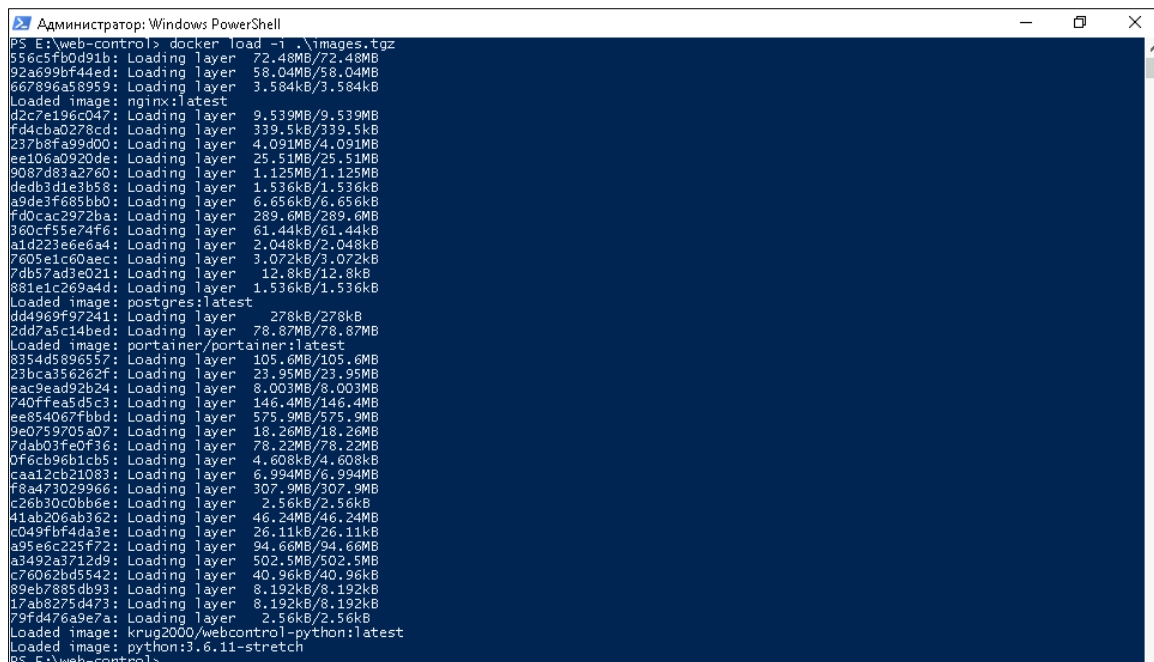


Рисунок 1.27 – Развертывание Docker-образов из архива.

Для обеспечения функционирования приложения необходимо предоставить полные права доступа для системной учетной записи «СЛУЖБА» на папку хранения баз данных Docker:

C:\ProgramData\docker\volumes

(Замечание: Иногда папка *ProgramData* может быть скрыта. Чтобы её увидеть, в Проводнике перейдите на вкладку «Вид» и проставьте галочку напротив пункта «Скрытые элементы».)

Перейдите к указанной папке, откройте окно свойств, кликнув правой клавишей мыши по нужной папке и выбрав в списке «Свойства». Откройте вкладку «Безопасность» и в список

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

групп и пользователей добавьте системную учетную запись «СЛУЖБА» и предоставьте ей полные права доступа (рисунок 1.28).

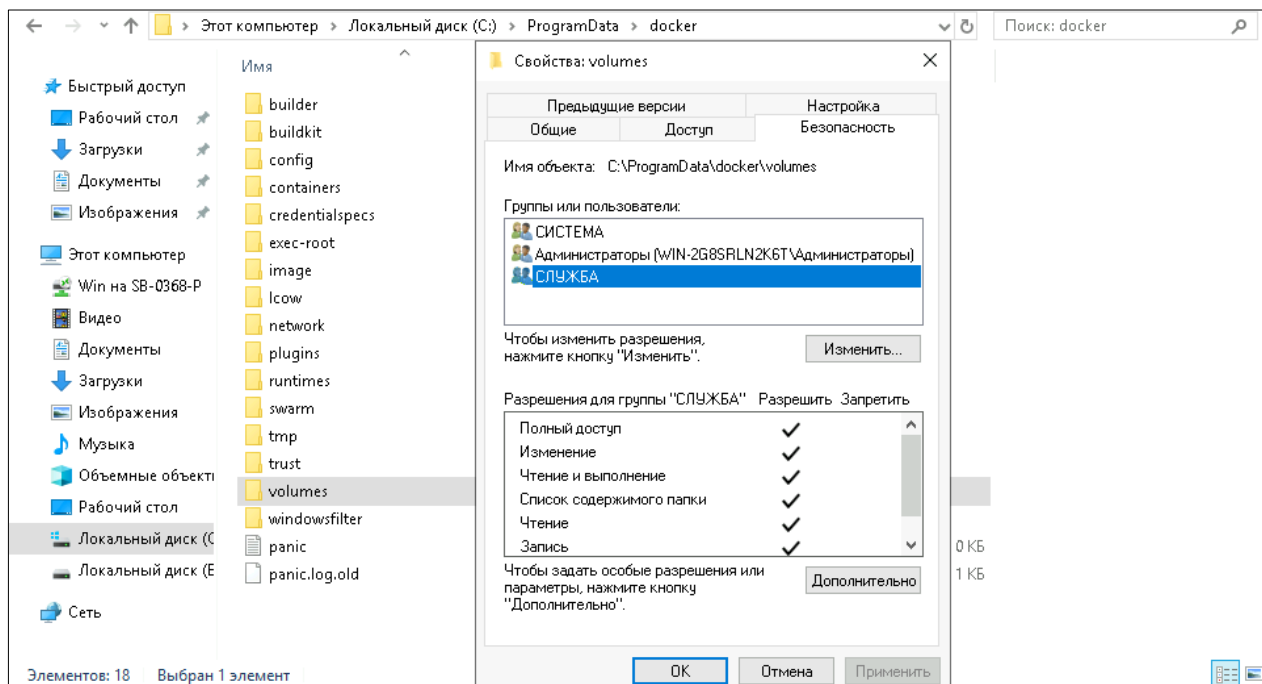


Рисунок 1.28 – Назначение прав доступа для системной учетной записи «СЛУЖБА».

Для предоставления прав на работу с Docker текущему пользователю выполните следующие действия:

1. Создайте группы безопасности Docker и Docker-users (Диспетчер серверов → Средства → Пользователи и компьютеры Active Directory → кликните правой кнопкой мыши по «Users» и выберите в меню «Создать» → «Группа») и включите в эти группы учетную запись текущего пользователя.
2. Добавьте правило "group": "Docker" в конфигурацию docker: для этого отредактируйте файл C:\ProgramData\docker\config\daemon.json. Указанный файл должен содержать следующие строки:

```
{  
  "experimental": true,  
  "group": "Docker"  
}
```

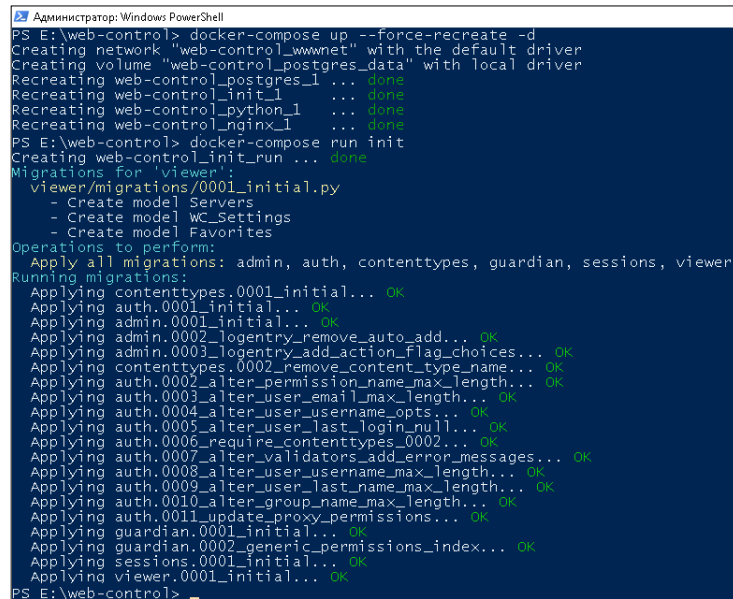
Выполните перезагрузку.

После выполнения этих шагов WEB-приложение готово к запуску командой:

```
docker-compose up --force-recreate -d
```


После первого запуска приложения необходимо выполнить начальную инициализацию базы данных приложения командой (рисунок 1.29):

docker-compose run init



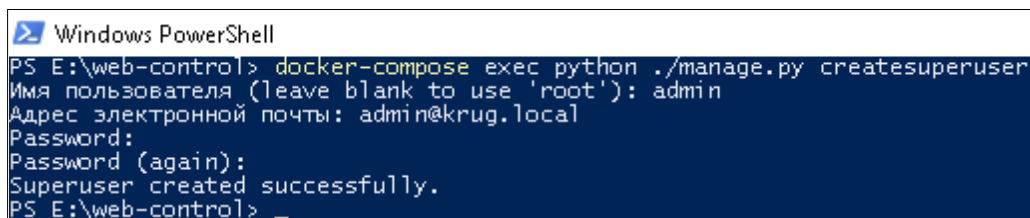
```

PS E:\web-control> docker-compose up --force-recreate -d
Creating network "web-control_wwwnet" with the default driver
Creating volume "web-control_postgres_data" with local driver
Recreating web-control_postgres_1 ... done
Recreating web-control_init_1 ... done
Recreating web-control_python_1 ... done
Recreating web-control_nginx_1 ... done
PS E:\web-control> docker-compose run init
Creating web-control_init_run ... done
Migrations for 'viewer':
  viewer/migrations/0001_initial.py
    - Create model Servers
    - Create model WC_Settings
    - Create model Favorites
Operations to perform:
  Apply all migrations: admin, auth, contenttypes, guardian, sessions, viewer
Running migrations:
  Applying contenttypes.0001_initial... OK
  Applying auth.0001_initial... OK
  Applying admin.0001_initial... OK
  Applying admin.0002_logentry_remove_auto_add... OK
  Applying admin.0003_logentry_add_action_flag_choices... OK
  Applying contenttypes.0002_remove_content_type_name... OK
  Applying auth.0002_alter_permission_name_max_length... OK
  Applying auth.0003_alter_user_email_max_length... OK
  Applying auth.0004_alter_user_username_opts... OK
  Applying auth.0005_alter_user_last_login_null... OK
  Applying auth.0006_require_contenttypes_0002... OK
  Applying auth.0007_alter_validators_add_error_messages... OK
  Applying auth.0008_alter_user_username_max_length... OK
  Applying auth.0009_alter_user_last_name_max_length... OK
  Applying auth.0010_alter_group_name_max_length... OK
  Applying auth.0011_update_proxy_permissions... OK
  Applying guardian.0001_initial... OK
  Applying guardian.0002_generic_permissions_index... OK
  Applying sessions.0001_initial... OK
  Applying viewer.0001_initial... OK
PS E:\web-control>
  
```

Рисунок 1.29 – Инициализация базы данных.

Для выполнения задач администрирования необходимо создать учетную запись администратора. Для этого выполните следующую команду (рисунок 1.30):

docker-compose exec python ./manage.py createsuperuser



```

Windows PowerShell
PS E:\web-control> docker-compose exec python ./manage.py createsuperuser
Имя пользователя (leave blank to use 'root'): admin
Адрес электронной почты: admin@krug.local
Password:
Password (again):
Superuser created successfully.
PS E:\web-control>
  
```

Рисунок 1.30 – Создание учетной записи администратора.

В ответ на запрос укажите имя учетной записи (например, **admin**) и пароль.

Доступ к панели администрирования можно получить, открыв в браузере страницу с адресом вида:

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

<http://192.168.0.248:8080/admin/>

где 192.168.0.248 - адрес ПЭВМ, на которой установлен сервер Web-Контроль. Для авторизации используется созданная ранее учетная запись администратора.

Для доступа к панели администрирования с удаленных компьютеров необходимо создать правило брандмауэра для входящих подключений, разрешающее доступ к порту 8080:

1. Откройте окно «Монитор брандмауэра...» (через поиск).
2. В левой части окна выберите «Правило для входящих подключений», затем кликните правой кнопкой мыши по выбранному пункту и в появившемся меню выберите «Создать правило...»
3. Выберите: Тип правила – для порта; Протокол и порты – Протокол TCP, Определенные протоколы и порты, порт 8080 (рисунок 1.31).

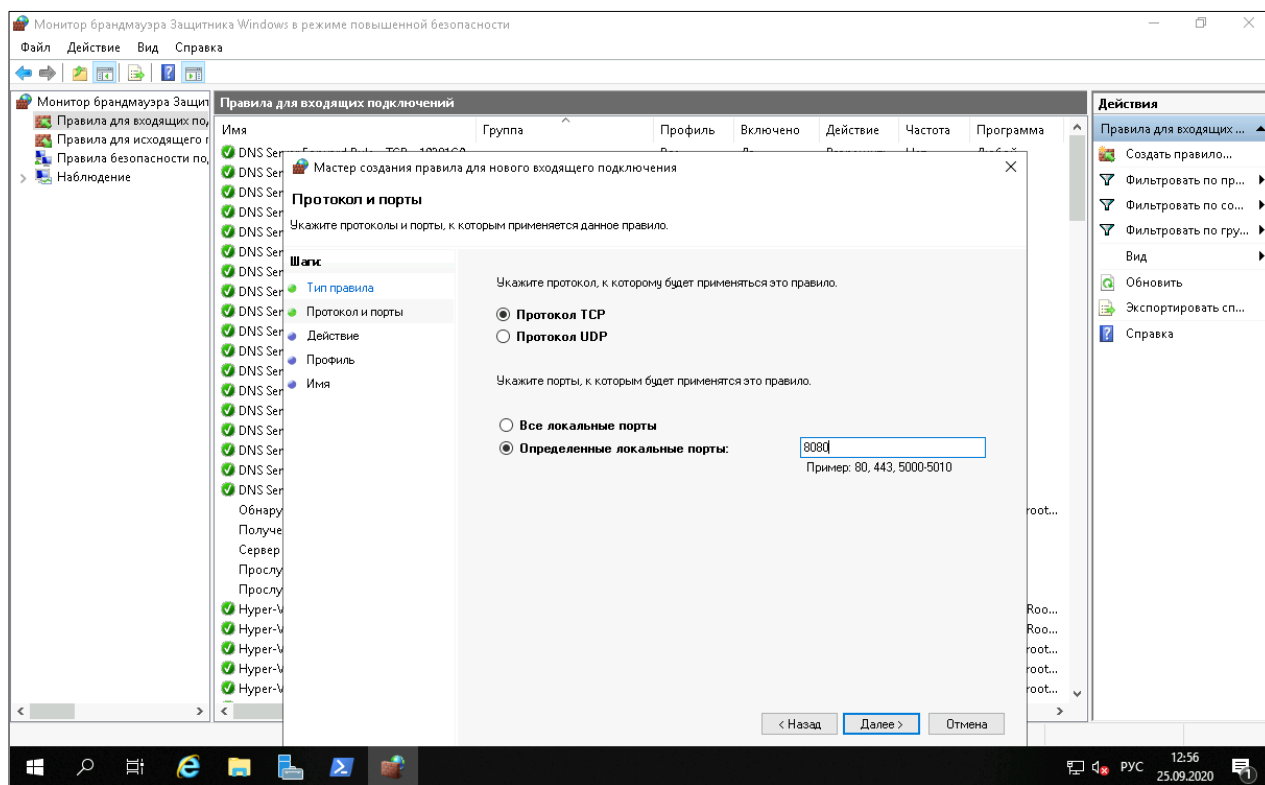


Рисунок 1.31 – Настройка правил брандмауэра.

Для автоматического старта приложения при загрузке операционной системы необходимо создать в папке приложения скрипт web-control.bat и добавить ссылку на скрипт в автозагрузку. Для этого выполните следующие действия:

1. В проводнике Windows откройте папку приложения Web-Control, кликните правой кнопкой мыши в любом свободном месте папки и выберите пункт «Создать» → «Текстовый документ». Укажите имя документа (WebControl) и нажмите Enter.
2. Откройте файл для редактирования и запишите туда команду:

```
docker-compose -f %~dp0%docker-compose.yml up --force-recreate -d
```

3. В меню «Файл» выберите пункт «Сохранить как...», измените тип файла на «Все файлы», при необходимости отредактируйте имя файла, после него поставьте точку и добавьте расширение `.bat`. Нажмите «Сохранить».
4. Для добавления в автозагрузку ссылки на скрипт запустите редактор реестра, нажав сочетание клавиш `Win+R` и введя `regedit`. Откройте ветку `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` и создайте в ней строковый параметр (Правка → Создать → Строковый параметр). Введите имя нового значения, нажмите `Enter`, после чего нажмите правой кнопкой на этой строке и выберите пункт «Изменить». В поле «Значение» введите полный путь к созданному файлу со скриптом, например, `E:\web-control\WebControl.bat`

При следующем запуске операционной системы приложение будет запущено автоматически.

2. АДМИНИСТРИРОВАНИЕ «WEB-КОНТРОЛЬ»

2.1 Задачи администрирования

2.1.1 Администрирование сервера Web-Контроль

Администрирование сервера Web-Контроль включает в себя:

- Занесение информации о SCADA серверах в АСУТП
- Управление Пользователями
- Управление Группами

Для выполнения администрирования сервера предназначена оснастка «**Управление Web-Контроль**» консоли управления.

2.1.2 Администрирование SCADA серверов

При использовании в качестве источников данных программного обеспечения Станции оператора системы КРУГ-2000, необходимо принимать во внимание, что возможно возникновение несовместимости Web-Контроль с ПО сторонних производителей, которое использует устаревший брокер объектных запросов NEO фирмы Sun Microsystems или его протоколы обмена данными. Это ПО может конфликтовать с Графическим интерфейсом КРУГ-2000. При этом будет невозможна работа модулей «**Мнемосхемы**» и «**Печатные документы**» Web-Контроль с данной Станцией оператора как с источником данных. Решением проблемы является обновление стороннего ПО или замена на аналогичное.

2.2 Защита

2.2.1 Защита от несанкционированного доступа к информации

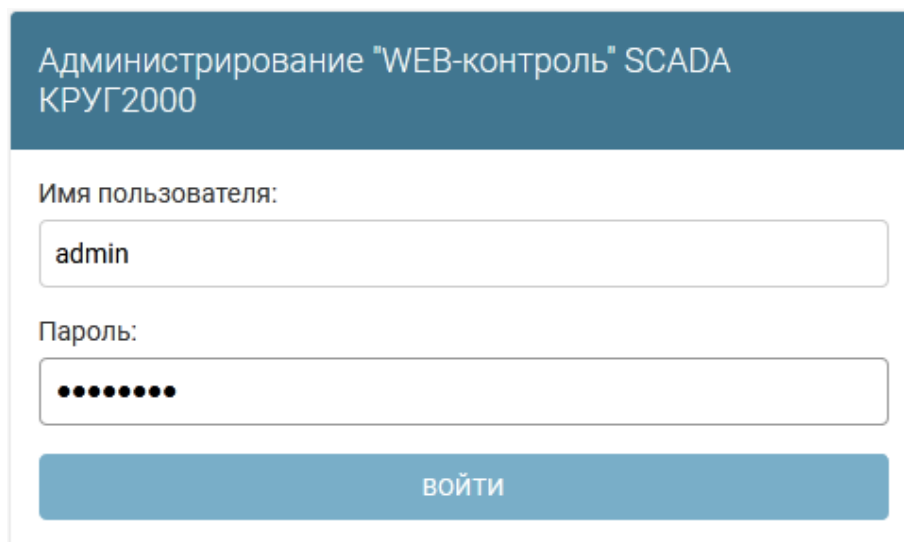
Защита информации в Web-Контроле основана на разграничении доступа к данным на основе учетных записей пользователей, защищенных паролями. Разрешения на доступ к данным в явном виде указываются при администрировании учетных записей пользователей, групп безопасности и источников данных.

2.2.2 Защита от несанкционированного использования

Для защиты от несанкционированного использования Web-Контроль используется электронный ключ. Ограничения, связанные с ним, описаны [в приложении А](#).

2.3 Начало работы

Для работы с административной панелью приложения Web-Контроль в адресной строке браузера введите адрес сервера Web-Контроль и добавьте **/admin/** (например, <http://192.168.10.230:8080/admin/>, где 192.168.10.230 - IP-адрес веб-сервера, на котором развёрнута служба Web-Контроль). На странице появится окно аутентификации панели администрирования Web-Контроль. (рисунок 2.1)



Администрирование "WEB-контроль" SCADA
КРУГ2000

Имя пользователя:
admin

Пароль:
●●●●●●●●

ВОЙТИ

Рисунок 2.1 – Окно аутентификации администратора

В окне необходимо ввести логин и пароль административной учетной записи.

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

В случае успешной идентификации откроется страница **Администрирование «Web-Контроль» SCADA КРУГ2000** (рисунок 2.2).

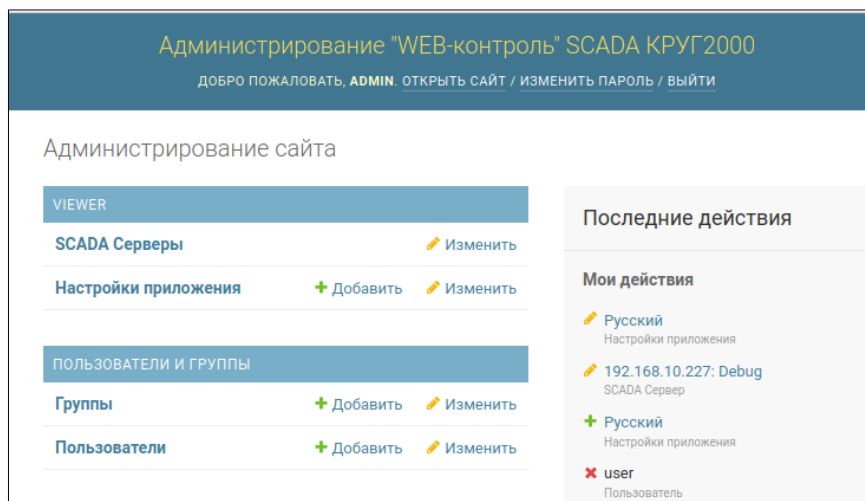


Рисунок 2.2 – Страница администрирования WEB-контроль

Для полноценной работы сервера WEB-контроль необходимо обеспечить сетевой доступ к ПЭВМ с установленным аппаратным ключом защиты. Сетевой адрес этой ПЭВМ («Сервер защиты») необходимо указать в «Настройках приложения» (рисунок 2.3):

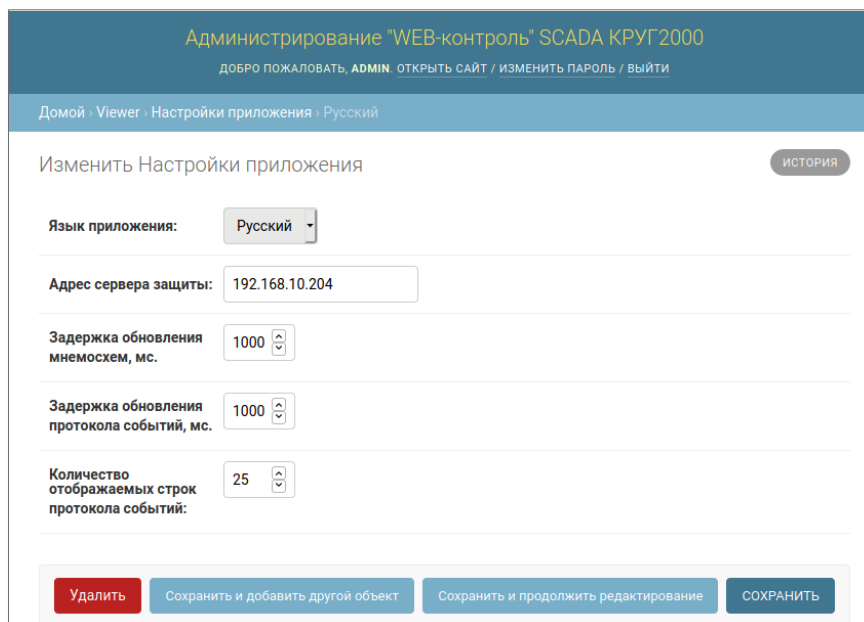


Рисунок 2.3 – Настройки приложения WEB-контроль

2.4 Управление SCADA серверами

SCADA сервер представляют собой приложение, работающее на компьютере в сети АСУТП, и способное поставлять информацию для модулей Web-Контроль.

Для управления источниками данных щелкните на **SCADA Серверы**. Браузер откроет страницу со списком SCADA-серверов (рисунок 2.4).

Управление источниками данных включает:

- Создание новых SCADA серверов
- Изменение параметров существующих SCADA серверов
- Удаление SCADA серверов
- Настройка прав доступа к SCADA серверам

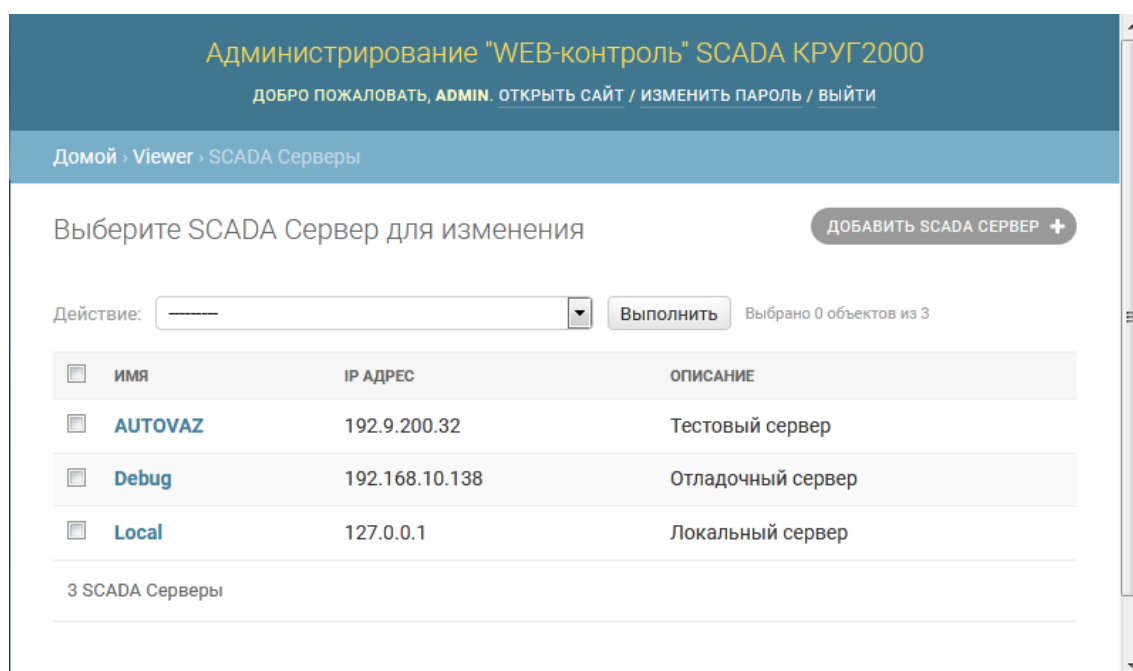


Рисунок 2.4 – Список источников данных

2.4.1 Создание нового SCADA сервера

Для добавления нового SCADA-сервера нажмите кнопку **«Добавить SCADA сервер»**. Откроется страница (рисунок 2.5), содержащая следующие поля:

- **Имя** – имя SCADA сервера (отображается в списке SCADA серверов у клиента). Имя должно быть уникально среди SCADA серверов. Имя источника данных может состоять только из русских и латинских букв, цифр и пробелов. Остальные символы в имени недопустимы
- **IP-адрес** – адрес компьютера- SCADA сервера
- **Описание** - описание SCADA сервера.

Введите необходимые параметры в указанные поля и нажмите одну из нижерасположенных кнопок:

- **Сохранить и добавить другой объект** – происходит создание SCADA-сервера и открытие новой формы для создания следующего SCADA-сервера
- **Сохранить и продолжить редактирование** – происходит создание SCADA-сервера без перехода на новую страницу
- **Сохранить** – происходит создание SCADA-сервера и переход к списку SCADA-серверов.

SCADA сервер создан, и появится в списке SCADA серверов.

The screenshot shows the administration interface for 'WEB-контроль' SCADA KPYG2000. At the top, there is a header with the title 'Администрирование "WEB-контроль" SCADA КРУГ2000' and a navigation bar with links: 'ДОБРО ПОЖАЛОВАТЬ, ADMIN', 'ОТКРЫТЬ САЙТ', 'ИЗМЕНИТЬ ПАРОЛЬ', and 'ВЫЙТИ'. Below the header is a breadcrumb trail: 'Домой > Viewer > SCADA Серверы > Добавить SCADA Сервер'. The main content area is titled 'Добавить SCADA Сервер' and contains three input fields: 'Имя:' (Name), 'IP адрес:' (IP address), and 'Описание:' (Description). The 'Имя:' field has a small vertical line indicating it is required. At the bottom of the form, there are three buttons: 'Сохранить и добавить другой объект' (Save and add another object), 'Сохранить и продолжить редактирование' (Save and continue editing), and 'СОХРАНИТЬ' (Save).

Рисунок 2.5 – Создание SCADA сервера – ввод имени, IP-адреса и описания

2.4.2 Изменение параметров существующих SCADA серверов

Для изменения свойств SCADA сервера щелкните на имени источника данных в списке; откроется страница управления SCADA сервером (рисунок 2.6).

Для SCADA сервера следует задать:

- **Имя** – отображается в списке источников данных на клиенте. Должно быть уникально среди SCADA сервера
- **IP-адрес** – адрес компьютера, который служит SCADA сервера для модулей
- **Описание** – описание SCADA сервера

Администрирование "WEB-контроль" SCADA КРУГ 2000
ДОБРО ПОЖАЛОВАТЬ, ADMIN. ОТКРЫТЬ САЙТ / ИЗМЕНИТЬ ПАРОЛЬ / ВЫЙТИ

Домой > Viewer > SCADA Серверы > 192.168.10.138: Debug

Изменить SCADA Сервер ПРАВА НА ОБЪЕКТ ИСТОРИЯ

Имя:

IP адрес:

Описание:

Удалить Сохранить и добавить другой объект Сохранить и продолжить редактирование СОХРАНИТЬ

Рисунок 2.6 – Параметры SCADA сервера

После редактирования параметров нажмите одну из нижерасположенных кнопок:

- **Сохранить и добавить другой объект** – происходит сохранение внесенных изменений и открытие формы создания нового SCADA-сервера;
- **Сохранить и продолжить редактирование** – происходит сохранение внесенных изменений без перехода на другую страницу;
- **Сохранить** – происходит сохранение внесенных изменений и переход к списку SCADA-серверов.

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

Для просмотра информации о произведенных изменениях параметров SCADA сервера нажмите на кнопку «История». На открывшейся странице выводятся данные о дате и времени, имени пользователя и выполненном этим пользователем действии в отношении выбранного SCADA-сервера (рисунок 2.7).

ДАТА И ВРЕМЯ	ПОЛЬЗОВАТЕЛЬ	ДЕЙСТВИЕ
20 февраля 2020 г. 12:53	admin	Добавлено.
21 апреля 2020 г. 12:11	admin	Изменено Описание.
21 апреля 2020 г. 12:13	admin	Изменено Имя.

Рисунок 2.7 - История изменений SCADA-сервера

2.4.3 Удаление SCADA сервера

Удалить SCADA Сервер можно на странице просмотра списка SCADA Серверов и на странице редактирования SCADA Серверов.

На странице просмотра списка SCADA Серверов для удаления SCADA Сервера выполните следующие действия (рисунок 2.8):

1. выделите в списке, поставив флаг в соответствующей строке, один или несколько подлежащих удалению SCADA-серверов,
2. в выпадающем списке поля **Действие** выберите «Удалить выбранные Серверы»,
3. нажмите на кнопку «**Выполнить**», расположенную справа от поля **Действие**.

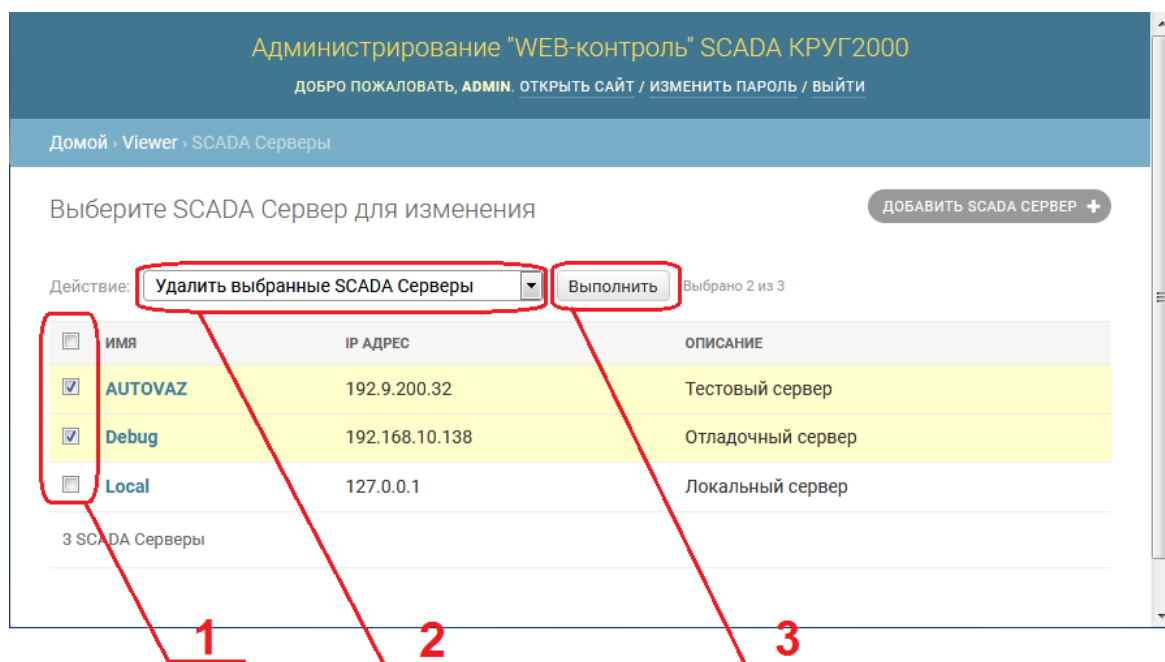


Рисунок 2.8 - Удаление SCADA-сервера на странице просмотра списка SCADA Серверов

Удаление SCADA-сервера возможно на странице редактирования его параметров. Для этого в списке SCADA-серверов (Домой>Viewer>SCADA серверы) кликните по имени подлежащего удалению SCADA-сервера, и на открывшейся странице нажмите на кнопку «Удалить».

2.4.4 Настройка прав доступа к SCADA серверам

Настройка прав доступа к SCADA серверам возможна следующими путями:

1. Для Пользователя/Группы назначение прав доступа к одному или нескольким серверам,
2. Для конкретного SCADA сервера назначение прав доступа Пользователям/Группам.

1. Для настройки прав доступа пользователя или группы к SCADA-серверу в списке SCADA серверов (Домой>Viewer>SCADA Серверы) выделите, поставив флаг в соответствующей строке, один или несколько SCADA-серверов, в выпадающем списке поля **Действие** выберите либо «**Настроить разрешения для пользователя**», либо «**Настроить разрешения для группы**» и нажмите на кнопку **Выполнить**.

При выборе действия «**Настроить разрешения для пользователя**» откроется страница (рисунок 2.9), которая позволит настроить следующие права для пользователя:

- Доступ к серверу
- Просмотр мнемосхем
- Просмотр печатных документов
- Просмотр протокола событий

Ниже отображается список серверов, к которым будут предоставлены права доступа для Пользователя/Группы.

Администрирование "WEB-контроль" SCADA КРУГ 2000

Домой > Настройка прав доступа к серверам

Настройка прав доступа к серверам

Пользователь:

Доступ к серверу:

- ☒ Не менять
- ☐ Разрешить
- ☐ Запретить

Просмотр мнемосхем:

- ☒ Не менять
- ☐ Разрешить
- ☐ Запретить

Просмотр печатных документов:

- ☒ Не менять
- ☐ Разрешить
- ☐ Запретить

Просмотр протокола событий:

- ☒ Не менять
- ☐ Разрешить
- ☐ Запретить

Права доступа будут предоставлены к следующим серверам:

- 192.9.200.32: AUTOVAZ Server
- 192.9.200.138: Virtual Scada

Сохранить

Рисунок 2.9 - Настройка прав доступа пользователя к серверам

Для настройки (или изменения) прав доступа в выпадающем списке поля **Пользователь** выберите имя пользователя, задайте значение для каждого права, выбрав один из вариантов:

- Не менять
- Разрешить
- Запретить

Затем нажмите кнопку «Сохранить». В результате происходит сохранение внесенных изменений и переход к списку SCADA-серверов.

Настройка прав доступа для Группы осуществляется аналогично настройке прав доступа для Пользователя.

Настроенные таким образом разрешения для доступа к SCADA серверу можно посмотреть в разделе «Права на объект» конкретного SCADA сервера (Домой>Viewer>SCADA Серверы>Имя SCADA сервера>Права на объект) (рисунок 2.10).

2. Для настройки прав доступа пользователя или группы на странице редактирования SCADA сервера (Домой>Viewer>SCADA Серверы>Имя SCADA сервера) нажмите кнопку «Права на объект». Откроется страница просмотра прав доступа пользователей и групп (рисунок 2.10).

Администрирование "WEB-контроль" SCADA КРУГ2000

ДОБРО ПОЖАЛОВАТЬ, ADMIN. ОТКРЫТЬ САЙТ / ИЗМЕНИТЬ ПАРОЛЬ / ВЫЙТИ

Домой · Viewer · SCADA Серверы · 192.9.200.32: AUTOVAZ · Права на объект

Права на объект

Пользователи

ПРАВА ПОЛЬЗОВАТЕЛЯ

ПОЛЬЗОВАТЕЛЬ	МОЖЕТ ПРОСМАТРИВАТЬ ПРОТОКОЛ СОБЫТИЙ	МОЖЕТ ПРОСМАТРИВАТЬ МНЕМΟΣХЕМЫ	МОЖЕТ ПРОСМАТРИВАТЬ ПЕЧАТНЫЕ ДОКУМЕНТЫ	ИМЕЕТ ДОСТУП К СЕРВЕРУ	ДЕЙСТВИЕ
user1	✓	✗	✗	✓	Редактировать
user2	✗	✓	✓	✓	Редактировать

User identification:
Enter a value compatible with User.USERNAME_FIELD

Управление пользователем

Группы

ГРУППОВЫЕ ПРАВА

ГРУППА	МОЖЕТ ПРОСМАТРИВАТЬ ПРОТОКОЛ СОБЫТИЙ	МОЖЕТ ПРОСМАТРИВАТЬ МНЕМΟΣХЕМЫ	МОЖЕТ ПРОСМАТРИВАТЬ ПЕЧАТНЫЕ ДОКУМЕНТЫ	ИМЕЕТ ДОСТУП К СЕРВЕРУ	ДЕЙСТВИЕ
Group:					

Управление группой


Рисунок 2.10 - Права на объект




На открывшейся странице отображаются права пользователя и групповые права:

- Может просматривать протокол событий
- Может просматривать мнемосхемы
- Может просматривать печатные документы
- Имеет доступ к серверу

Для предоставления Пользователю прав на объект введите в поле **User Identification** имя пользователя и нажмите кнопку «Управление пользователем». (если Пользователю уже предоставлены определенные права доступа, то для их изменения нажмите «Редактировать» в строке этого пользователя.)

На открывшейся странице (рисунок 2.11) предоставление прав доступа Пользователю к Объекту осуществляется следующим образом:

1. В списке «Доступные права» выделите необходимое право (выбранное право выделяется строкой синего цвета)
2. Добавьте выделенное право в список «Выбранные права» двойным щелчком мыши или с помощью кнопки  (добавить право), расположенной между списками выбранных и доступных прав.

Кнопка  (удалить право) используется для удаления права из списка «Выбранные права». Внизу списков с правами располагаются кнопки **Выбрать все**  и **Удалить все** , с помощью которых добавляются/удаляются все права в списке.

3. Нажмите кнопку «Сохранить».

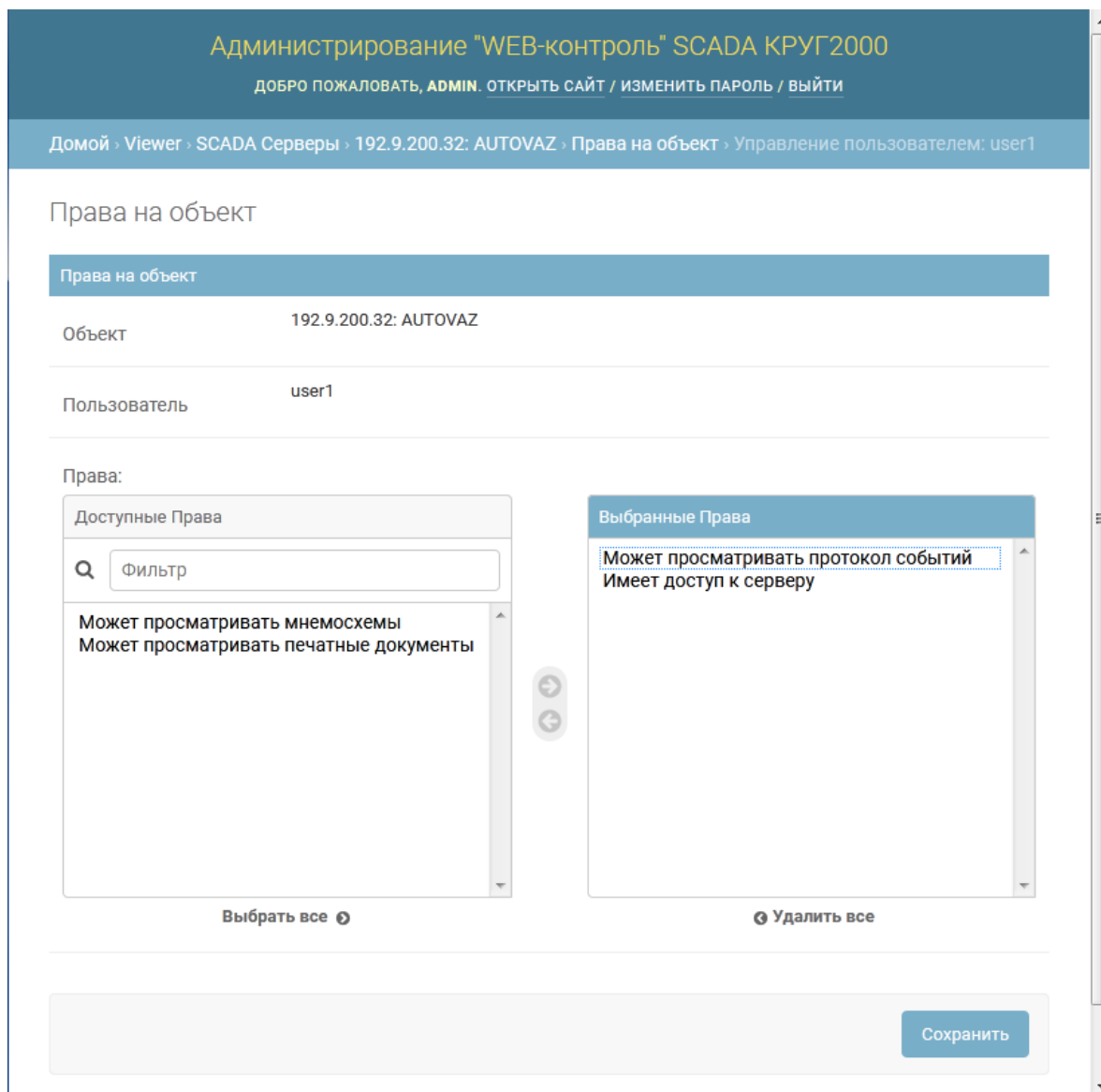


Рисунок 2.11 - Предоставление прав доступа Пользователю

Для предоставления Группе прав на объект введите в поле **Group** (рисунок 2.10) имя группы и нажмите кнопку «**Управление группой**». (Если Группе уже предоставлены определенные права доступа, то для их изменения нажмите «**Редактировать**» в строке этой группы.)

Предоставление/изменение прав доступа на объект Группе осуществляется аналогично предоставлению/изменению прав доступа Пользователю.



Индивидуальные права Пользователя, Группы и права на объект суммируются по принципу логического ИЛИ. Т.е. если индивидуальные права Пользователя или Группы разрешают доступ к определенным модулям, отсутствие разрешений в разделе «Права на объект» конкретного SCADA сервера не лишит Пользователя/Группу доступа к указанным модулям этого SCADA сервера.

**ВНИМАНИЕ!!!**

Для запрета доступа Пользователю к конкретному модулю необходимо отменить это право 1) в индивидуальных правах Пользователя, 2) в правах Группы, в которую включен Пользователь (или удалить Пользователя из этой Группы), 3) отменить разрешение для SCADA серверов.

2.5 Управление пользователями

Для доступа к данным АСУТП с помощью Web-Контроль необходимо создать учетные записи Пользователей, которые будут это делать. Каждого Пользователя можно включить в одну или несколько Групп, тогда Пользователь получит все права, указанные в каждой из Групп.

При установке Web-Контроль создается учетная запись администратора, от имени которой выполняются все последующие настройки (в случае развертывания преднастроенного дистрибутива на основе ОС Linux административная учетная запись — **admin** с паролем **admin**)

На странице просмотра Пользователей (рисунок 2.12) отображается список пользователей и информация о каждом из них, а именно:

- Имя пользователя,
- Адрес электронной почты,
- Имя,
- Фамилия,
- Статус персонала.

Для удобства работы со списком Пользователей предусмотрены фильтры, которые позволяют выводить пользователей для просмотра по следующим критериям:

- Статус персонала
- Статус суперпользователя
- Активный
- Принадлежность к группам

СРЕДСТВА ИНТЕГРАЦИИ В АСУТП

Управление пользователями включает:

- Создание новых Пользователей
- Изменение параметров существующих Пользователей
- Задание Пользователю нового пароля
- Удаление Пользователей.

Администрирование "WEB-контроль" SCADA
КРУГ2000

ДОБРО ПОЖАЛОВАТЬ, ADMIN. [ОТКРЫТЬ САЙТ](#) / [ИЗМЕНИТЬ ПАРОЛЬ](#) / [ВЫЙТИ](#)

Домой · Пользователи и группы · Пользователи

Выберите пользователь для изменения

ДОБАВИТЬ ПОЛЬЗОВАТЕЛЯ +

ФИЛЬТР

статус персонала

Все
Да
Нет

статус суперпользователя

Все
Да
Нет

активный

Все
Да
Нет

группы

Все
Доступ к серверам
Просмотр мнемосхем
Просмотр печатных документов
Просмотр протокола событий
-

	ИМЯ ПОЛЬЗОВАТЕЛЯ	АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ	ИМЯ	ФАМИЛИЯ	СТАТУС ПЕРСОНАЛА
<input type="checkbox"/>	admin	admin@krug.local			✓
<input type="checkbox"/>	user1				✗
<input type="checkbox"/>	user2				✗

3 пользователи

Рисунок 2.12 – Список пользователей

2.5.1 Создание новых Пользователей

Для создания нового Пользователя нажмите кнопку «Добавить пользователя» и на открывшейся странице (рисунок 2.13) введите необходимые данные:

- Имя пользователя
- Пароль
- Подтверждение пароля.

Процесс создания Пользователя завершается нажатием одной из кнопок:

- **Сохранить и добавить другой объект** – происходит создание Пользователя и открытие незаполненной формы для создания нового Пользователя,
- **Сохранить и продолжить редактирование** – происходит создание Пользователя без перехода на новую страницу,
- **Сохранить** – происходит создание Пользователя и переход к списку Пользователей.

The screenshot shows the administration interface for 'WEB-контроль' SCADA KPYG2000. The header includes the title and navigation links: 'ДОБРО ПОЖАЛОВАТЬ, ADMIN', 'ОТКРЫТЬ САЙТ', 'ИЗМЕНИТЬ ПАРОЛЬ', and 'ВЫЙТИ'. The breadcrumb trail is 'Домой > Пользователи и группы > Пользователи > Добавить пользователь'. The main heading is 'Добавить пользователь'. Below it, a message states: 'First, enter a username and password. Then, you'll be able to edit more user options.' The form contains three input fields: 'Имя пользователя:' (with a note: 'Обязательное поле. Не более 150 символов. Только буквы, цифры и символы @/./+/_'), 'Пароль:' (with multiple password strength rules in English and Russian), and 'Подтверждение пароля:' (with a note: 'Для подтверждения введите, пожалуйста, пароль ещё раз.'). At the bottom, there are three buttons: 'Сохранить и добавить другой объект', 'Сохранить и продолжить редактирование', and 'СОХРАНИТЬ'.

Рисунок 2.13 - Страница создания нового Пользователя

2.5.2 Изменение параметров существующих пользователей

Для изменения свойств Пользователя щелкните в списке Пользователей по имени нужного Пользователя. Открывшаяся страница управления Пользователями содержит следующие блоки для задания свойств Пользователя:

- Изменение пользователя
- Персональная информация
- Права
- Важные даты

В блоке **Изменение пользователя** можно изменить Имя пользователя и пароль (рисунок 2.14)

Рисунок 2.14 - Изменение имени пользователя и пароля

Для изменения пароля перейдите по ссылке и в открывшейся форме (рисунок 2.15) введите новый пароль, для подтверждения введите пароль еще раз и нажмите кнопку «**Изменить пароль**».

Рисунок 2.15 - Изменение пароля пользователя

Блок **Персональная информация** (рисунок 2.16) содержит следующие поля:

- Имя
- Фамилия
- Адрес электронной почты

Персональная информация

Имя: User

Фамилия: One

Адрес электронной почты: user1@krug.local

Рисунок 2.16 - Персональная информация о Пользователе

Блок **Права** (рисунок 2.17) позволяет задать для данного пользователя:

- статус (активный, статус персонала, статус суперпользователя),
- принадлежность к группам
- разрешения пользователя

Права

☒ Активный
Отметьте, если пользователь должен считаться активным. Уберите эту отметку вместо удаления учётной записи.

☐ Статус персонала
Отметьте, если пользователь может входить в административную часть сайта.

☐ Статус суперпользователя
Указывает, что пользователь имеет все права без явного их назначения.

Группы:

Доступные группы ?

Фильтр

Доступ к серверам
Просмотр протокола событий

Выбранные группы ?

Просмотр мнемосхем
Просмотр печатных документов

Удалить все

Выбрать все ?

Группы, к которым принадлежит данный пользователь. Пользователь получит все права, указанные в каждой из его/её групп. Удерживайте "Control" (или "Command" на Mac), чтобы выбрать несколько значений.

Разрешения пользователя:

Доступные разрешения ?

Фильтр

viewer | SCADA Сервер | Может просматривать протокол
viewer | SCADA Сервер | Может просматривать мнемосхе
viewer | SCADA Сервер | Может просматривать печатные
viewer | SCADA Сервер | Имеет доступ к серверу

Выбранные разрешения ?

Удалить все

Выбрать все ?

Рисунок 2.17 - Права пользователя



Ответственность за предоставление Пользователям доступа к различным модулям и SCADA серверам несет администратор Web-Контроль. Необходимо, по возможности, избегать предоставления избыточных прав доступа.

Изменение списка Групп, в которые включен Пользователь, и разрешений Пользователя осуществляется с помощью кнопок (выбрать), (удалить), расположенных между списками выбранных и доступных групп/разрешений или двойным щелчком мыши. С помощью кнопок добавляется/удаляется Группа/разрешение, выделенное строкой синего цвета.

Внизу списков располагаются кнопки **Выбрать все** и **Удалить все**, с помощью которых выбираются/удаляются все Группы/разрешения в списке.



Для запрета доступа Пользователю к конкретному модулю помимо удаления права доступа из списка выбранных разрешений необходимо отменить это право 1) в правах Группы, в которую включен Пользователь (или удалить Пользователя из этой Группы), 2) отменить разрешение для SCADA серверов, так как отмена разрешения для конкретного Пользователя не отменяет разрешений для Группы и SCADA серверов.

Блок **Важные даты** позволяет посмотреть дату и время регистрации Пользователя и последнего входа в систему (рисунок 2.18)

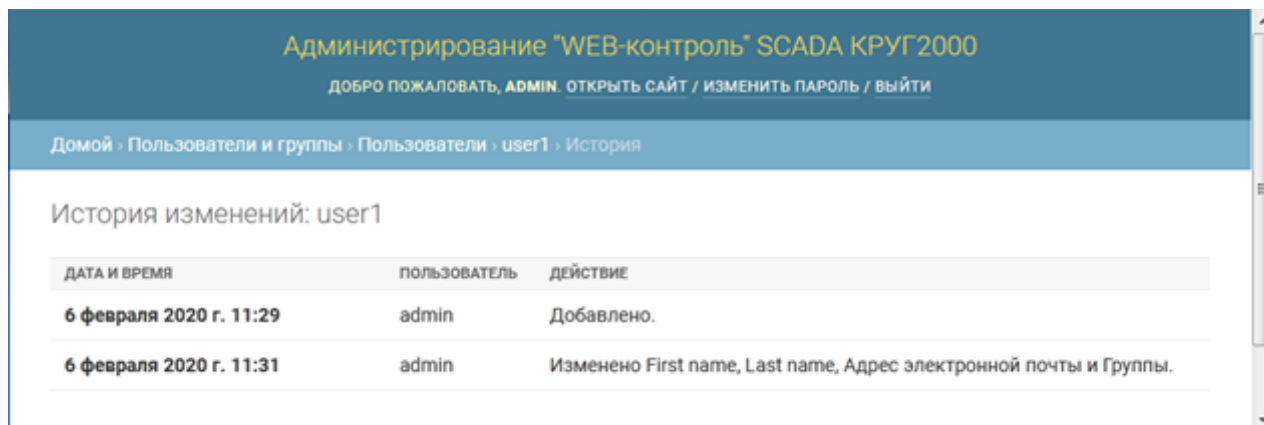
Важные даты	
Последний вход:	14 октября 2020 г. 15:48
Дата регистрации:	16 мая 2020 г. 23:23

Рисунок 2.18 - Важные даты

Для сохранения внесенных изменений в параметры Пользователя нажмите одну из кнопок, расположенных внизу страницы:

- **Сохранить и добавить другой объект** – происходит сохранение внесенных изменений и открытие незаполненной формы для создания нового Пользователя,
- **Сохранить и продолжить редактирование** – происходит сохранение внесенных изменений без перехода на новую страницу,
- **Сохранить** – происходит сохранение внесенных изменений и переход к списку Пользователей.

Для просмотра информации о произведенных изменениях в профиле Пользователя нажмите на кнопку «История». На открывшейся странице выводятся данные о дате и времени, имени Пользователя и внесенных указанным Пользователем изменений в профиль (рисунок 2.19).



Администрирование "WEB-контроль" SCADA КРУГ2000		
ДОБРО ПОЖАЛОВАТЬ, ADMIN. ОТКРЫТЬ САЙТ / ИЗМЕНИТЬ ПАРОЛЬ / ВЫЙТИ		
Домой · Пользователи и группы · Пользователи · user1 · История		
История изменений: user1		
ДАТА И ВРЕМЯ	ПОЛЬЗОВАТЕЛЬ	ДЕЙСТВИЕ
6 февраля 2020 г. 11:29	admin	Добавлено.
6 февраля 2020 г. 11:31	admin	Изменено First name, Last name, Адрес электронной почты и Группы.

Рисунок 2.19 – История изменений пользователя

2.5.3 Удаление Пользователя

Удалить Пользователя можно на странице просмотра списка Пользователей и на странице редактирования Пользователя.



При удалении всех учетных записей с правами администратора теряется доступ к панели управления Web-Контроль. Для восстановления учетной записи администратора необходимо выполнение административных действий в консоли серверной части WEB-контроля.

На странице просмотра списка Пользователей (рисунок 2.20) для удаления Пользователя выполните следующие действия:

1. выделите, поставив флаг в соответствующей строке, одного или нескольких подлежащих удалению Пользователей,
2. в выпадающем списке поля **Действие** выберите «Удалить выбранные пользователи»
3. нажмите на кнопку **«Выполнить»**, расположенную справа от поля **Действие**.

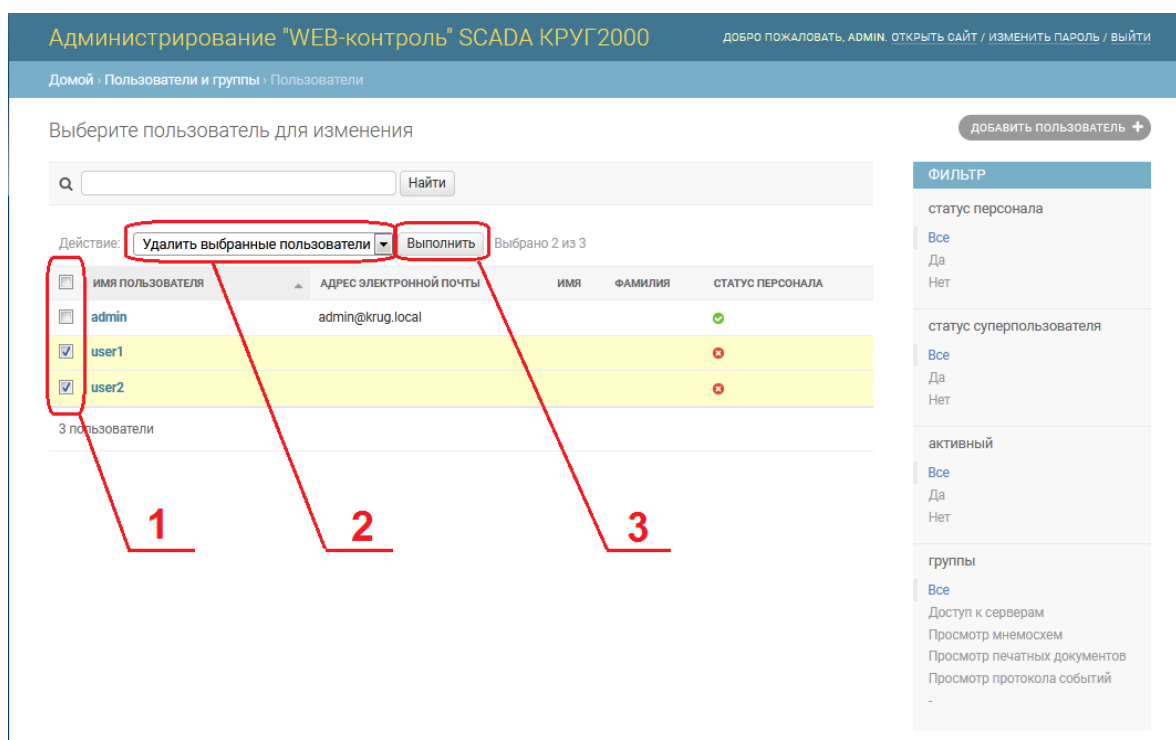


Рисунок 2.20 - Удаление Пользователя на странице просмотра списка Пользователей

Для удаления Пользователя на странице редактирования Пользователя (Домой>Пользователи и группы>Пользователи>Имя пользователя) нажмите на кнопку «Удалить», расположенную в левом нижнем углу страницы.

2.6 Управление группами

Группы используются для упрощения администрирования. Чтобы в индивидуальном порядке не назначать нескольким Пользователям одинаковые права, можно создать Группу, задать ей определенный набор прав, разрешающих доступ к модулям, SCADA серверам и управлению Web-Контроль, и затем включить в состав этой Группы требуемых Пользователей. При этом каждый Пользователь, входящий в Группу, унаследует все назначенные для данной Группы права.

Пользователя можно включить в состав одной или нескольких Групп.

Управление группами включает:

- Создание новых групп
- Изменение параметров существующих групп
- Удаление групп.

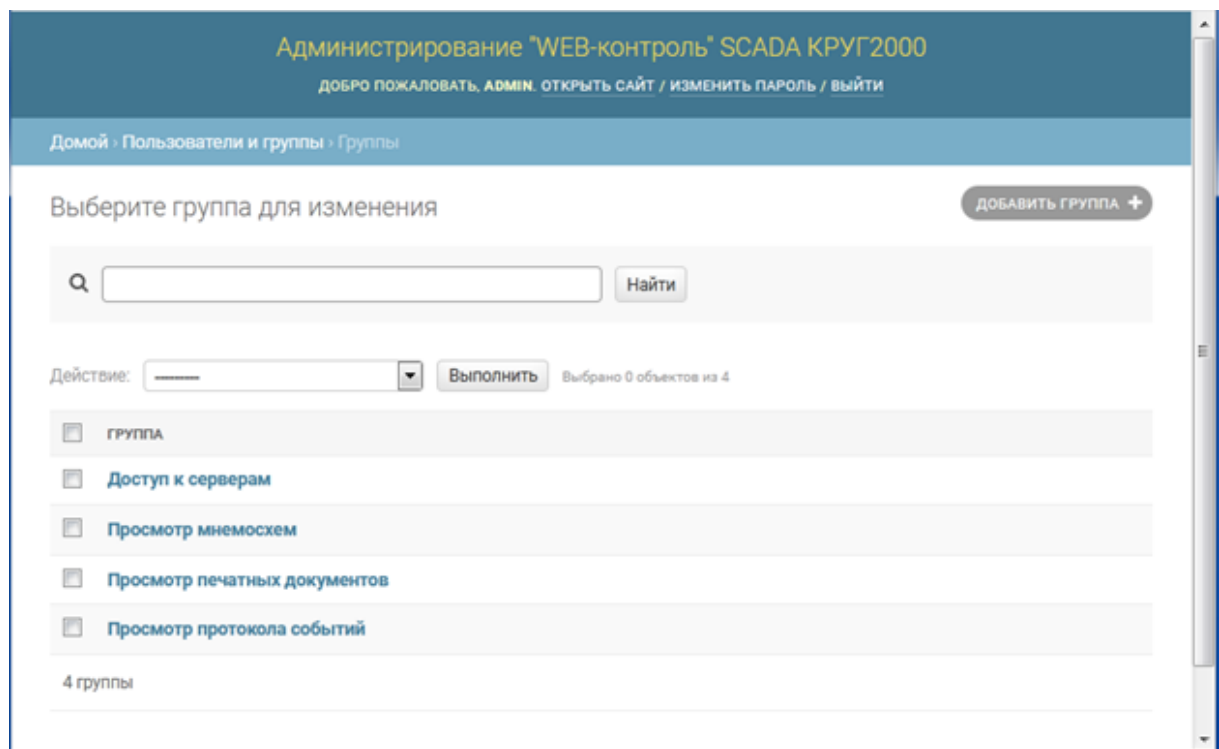




Рисунок 2.21 - Страница просмотра списка Групп



2.6.1 Создание новых групп

Для создания новой группы нажмите кнопку **«Добавить группу»** и на открывшейся странице (рисунок 2.22) введите необходимые данные:

- Имя – имя группы (должно быть уникально среди групп),
- Права

Блок управления правами разделен на две части – в левой части расположен список доступных прав, в правой части – выбранные права для создаваемой группы.

Формирование списка прав группы осуществляется с помощью кнопок  (добавить право),  (удалить право), расположенных между списками выбранных и доступных прав, или двойным щелчком мыши. С помощью данных кнопок добавляется/удаляется право, выделенное строкой синего цвета.

Внизу списков с правами располагаются кнопки **Выбрать все**  и  **Удалить все**, с помощью которых добавляются/удаляются все права в списке.

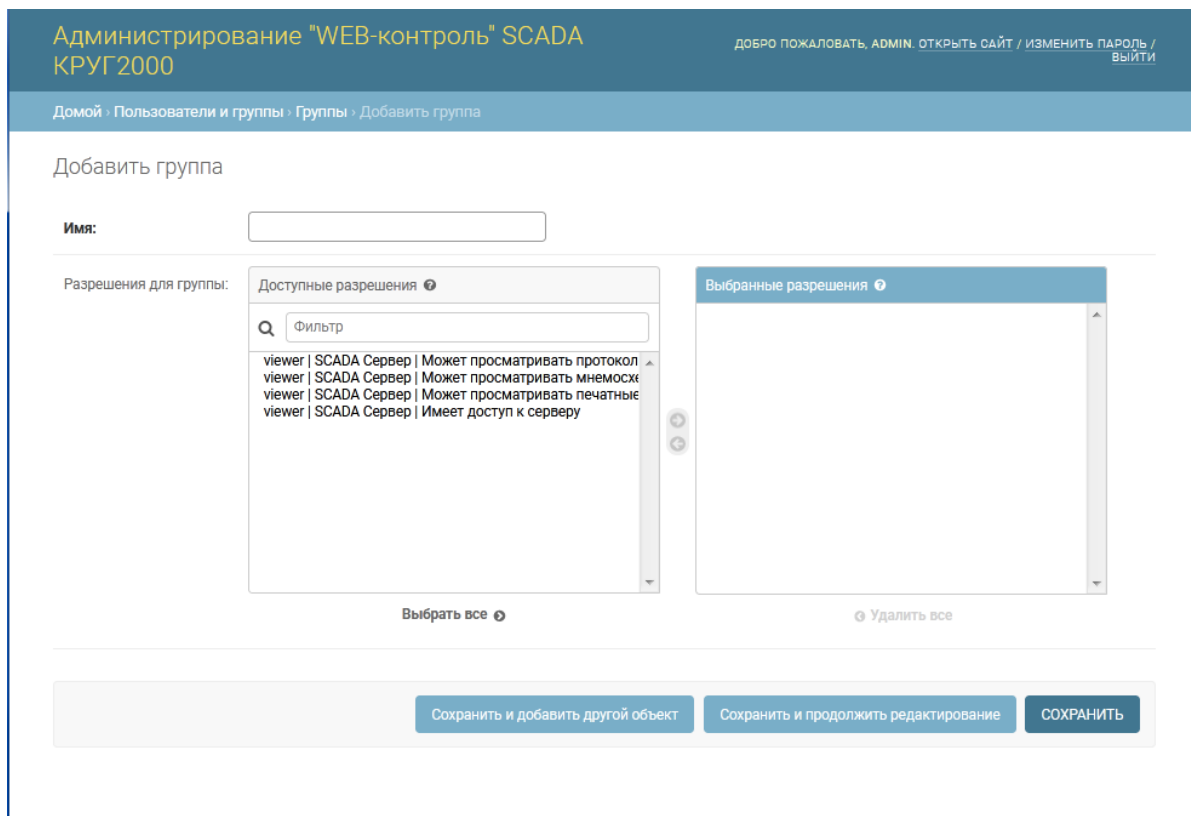


Рисунок 2.22 - Создание новой группы

Процесс создания Группы завершает нажатием одной из кнопок:



- **Сохранить и добавить другой объект** – происходит создание Группы и открытие новой формы для создания следующей Группы,
- **Сохранить и продолжить редактирование** – происходит создание Группы без перехода на новую страницу,
- **Сохранить** – происходит создание Группы и переход к списку Групп.



2.6.2 Изменение параметров группы

Для редактирования Группы на странице просмотра списка Групп (Домой>Пользователи и группы>Группы) кликните по имени нужной группы. На открывшейся странице (рисунок 2.23) доступны следующие действия:

- Изменение имени группы,
- Изменение прав группы,
- Удаление группы,
- Просмотр истории группы.

Для изменения имени группы в поле **Имя** введите новое имя группы.

Изменение списка прав группы осуществляется с помощью кнопок  (добавить право),  (удалить право), расположенных между списками выбранных и доступных прав, или двойным щелчком мыши. С помощью кнопок добавляется/удаляется право, выделенное строкой синего цвета.

Внизу списков с правами располагаются кнопки **Выбрать все**  и  **Удалить все**, с помощью которых добавляются/удаляются все права в списке.

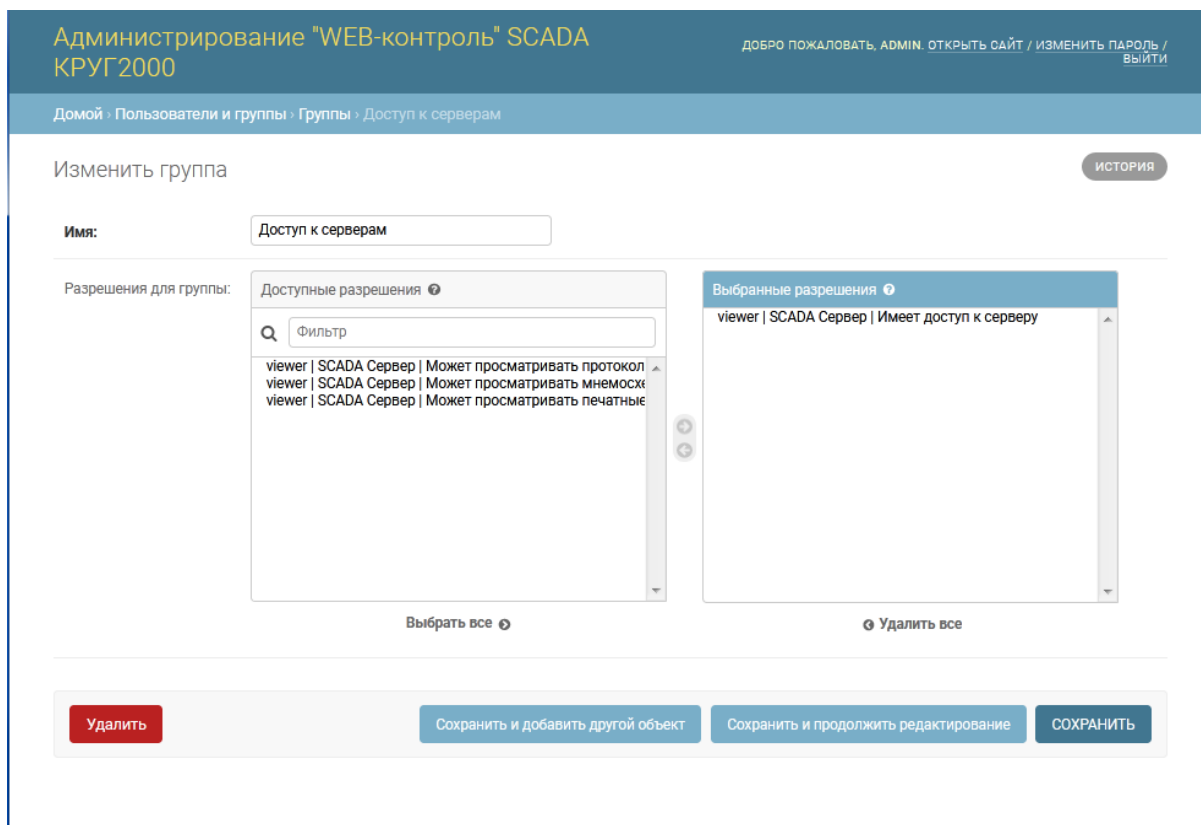


Рисунок 2.23 – Страница редактирования группы

После изменения параметров Группы нажмите одну из кнопок внизу страницы:

- **Сохранить и добавить другой объект** – происходит сохранение внесенных изменений и открытие незаполненной формы для создания новой Группы,
- **Сохранить и продолжить редактирование** – происходит сохранение внесенных изменений без перехода на новую страницу,
- **Сохранить** – происходит сохранение внесенных изменений и переход к списку Групп.

Для просмотра информации об изменениях параметров Группы нажмите на кнопку «История». На открывшейся странице отображается историю изменений Группы (рисунок 2.24):

- **Дата и время** – дата и время изменения Группы,
- **Пользователь** – имя Пользователя, выполнившего действие по изменению Группы,
- **Действие** – название действия, выполненного Пользователем.

Администрирование "WEB-контроль" SCADA КРУГ2000		
ДОБРО ПОЖАЛОВАТЬ, ADMIN. ОТКРЫТЬ САЙТ / ИЗМЕНИТЬ ПАРОЛЬ / ВЫЙТИ		
Домой · Пользователи и группы · Группы · Просмотр печатных документов · История		
История изменений: Просмотр печатных документов		
ДАТА И ВРЕМЯ	ПОЛЬЗОВАТЕЛЬ	ДЕЙСТВИЕ
6 февраля 2020 г. 11:27	admin	Добавлено.
6 февраля 2020 г. 11:27	admin	Изменено Права.

Рисунок 2.24 - Страница просмотра истории изменений группы

2.6.3 Удаление группы

Удалить группу можно на странице просмотра списка групп и на странице редактирования группы.

На странице просмотра списка Групп (Домой>Пользователи и группы>Группы) (рисунок 2.24) для удаления группы выполните следующие действия:

1. выделите, поставив флаг в соответствующей строке, одну или несколько подлежащих удалению Групп,
2. в выпадающем списке поля **Действие** выберите «Удалить выбранные группы»
3. нажмите на кнопку **«Выполнить»**, расположенную справа от поля **Действие**.

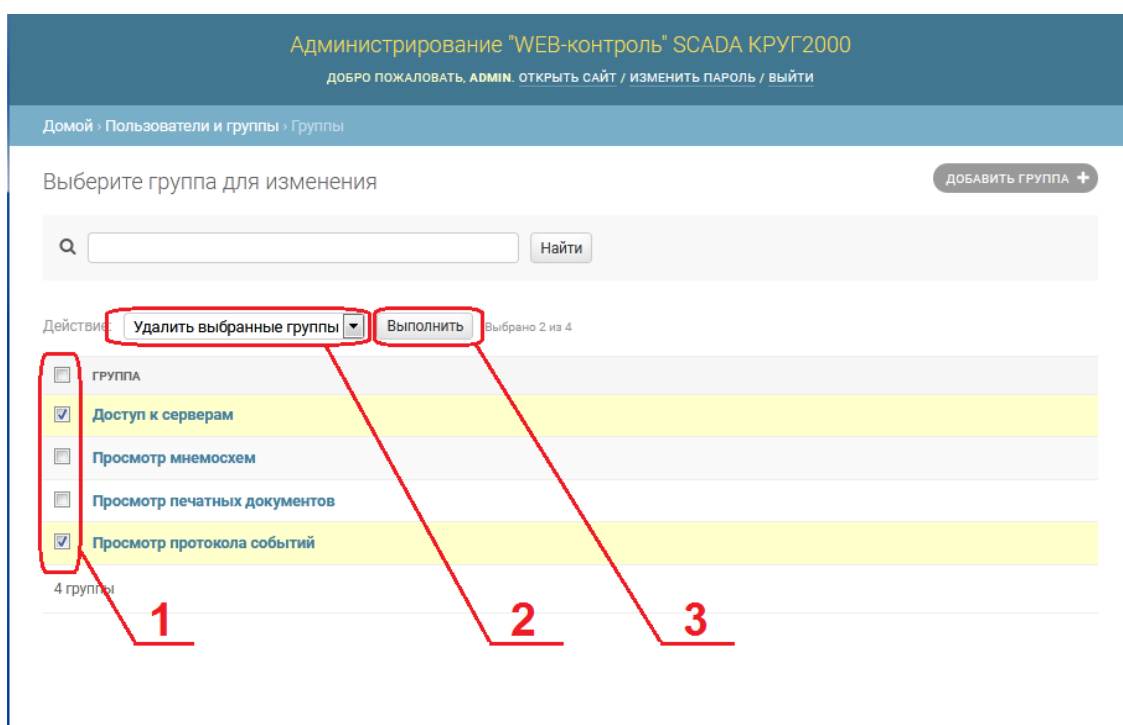


Рисунок 2.24 - Удаление группы на странице просмотра списка групп

Для удаления группы на странице редактирования группы (Домой>Пользователи и группы>Группы>Имя группы) нажмите на кнопку **«Удалить»**.

3. ОБНОВЛЕНИЕ WEB-КОНТРОЛЬ БЕЗ ПОТЕРИ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ

1. На существующий («старый») установленный WK более ранней версии (4.4.X) необходимо скопировать новый docker файл python-image.tgz в любую папку, например, /tmp (рисунок 3.1).

Механизм копирования осуществляется через подключаемую к ПК флешку с копируемым файлом (USB подключение предварительно настраивается в виртуальной машине) или через создание общей папки в настройках виртуальной машины с подключением в Linux образа диска диска Дополнительной гостевой ОС (см. [Как подключить общую папку в Virtualbox | 2DOMAINS.RU](#) ✓, нужно знать пароль пользователя в Linux).

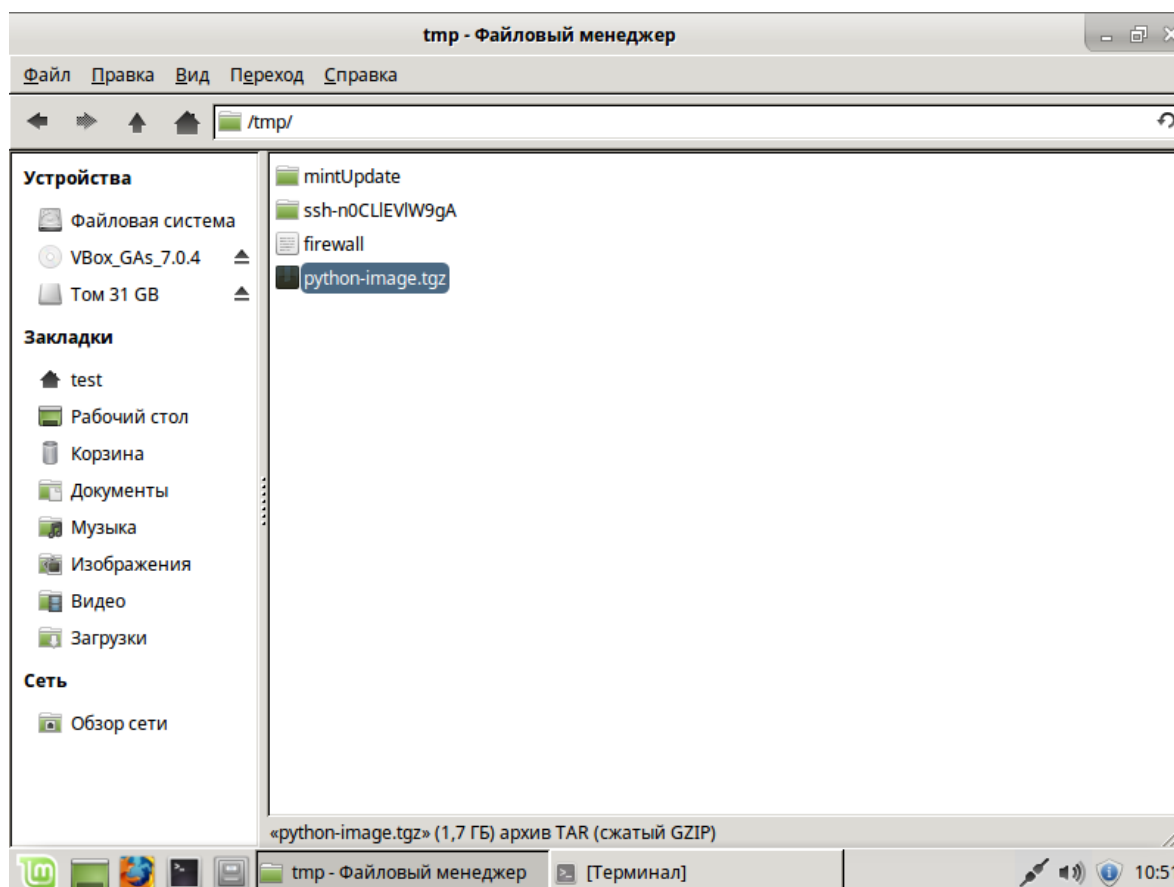
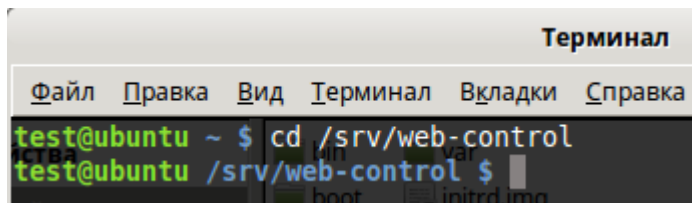


Рисунок 3.1

Все дальнейшие действия производятся в терминале.

2. Необходимо перейти в папку с установленным WK (рисунок 3.2):

cd /srv/web-control

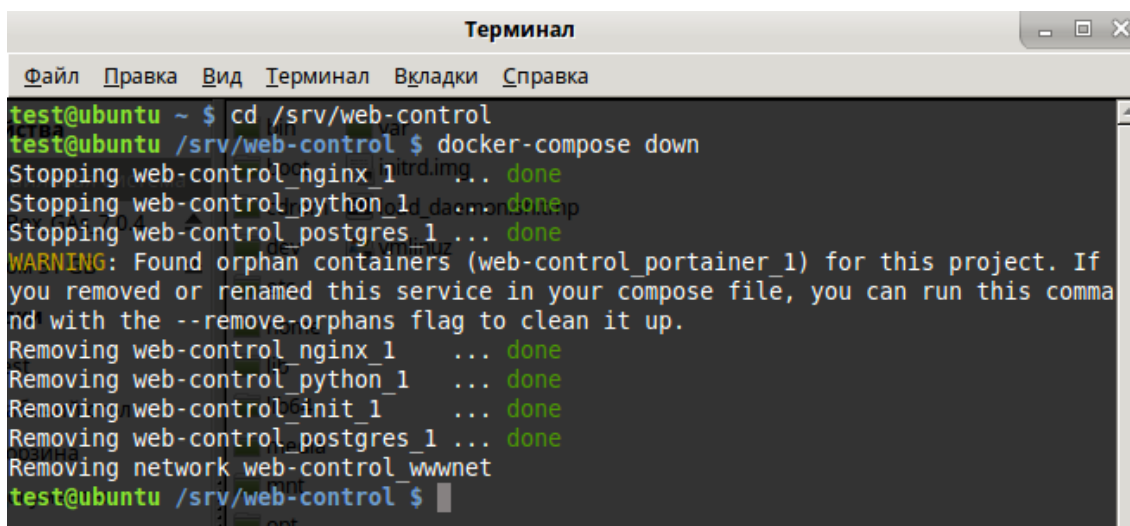


```
Терминал
Файл Правка Вид Терминал Вкладки Справка
test@ubuntu ~ $ cd /srv/web-control
test@ubuntu /srv/web-control $
```

Рисунок 3.2

3. Остановить сервер WC следующей командой (рисунок 3.3):

docker-compose down



```
Терминал
Файл Правка Вид Терминал Вкладки Справка
test@ubuntu ~ $ cd /srv/web-control
test@ubuntu /srv/web-control $ docker-compose down
Stopping web-control_nginx_1 ... done
Stopping web-control_python_1 ... done
Stopping web-control_postgres_1 ... done
WARNING: Found orphan containers (web-control_portainer_1) for this project. If
you removed or renamed this service in your compose file, you can run this comma
nd with the --remove-orphans flag to clean it up.
Removing web-control_nginx_1 ... done
Removing web-control_python_1 ... done
Removing web-control_init_1 ... done
Removing web-control_postgres_1 ... done
Removing network web-control_wwwnet
test@ubuntu /srv/web-control $
```

Рисунок 3.3 – Остановка сервера Web-контроль

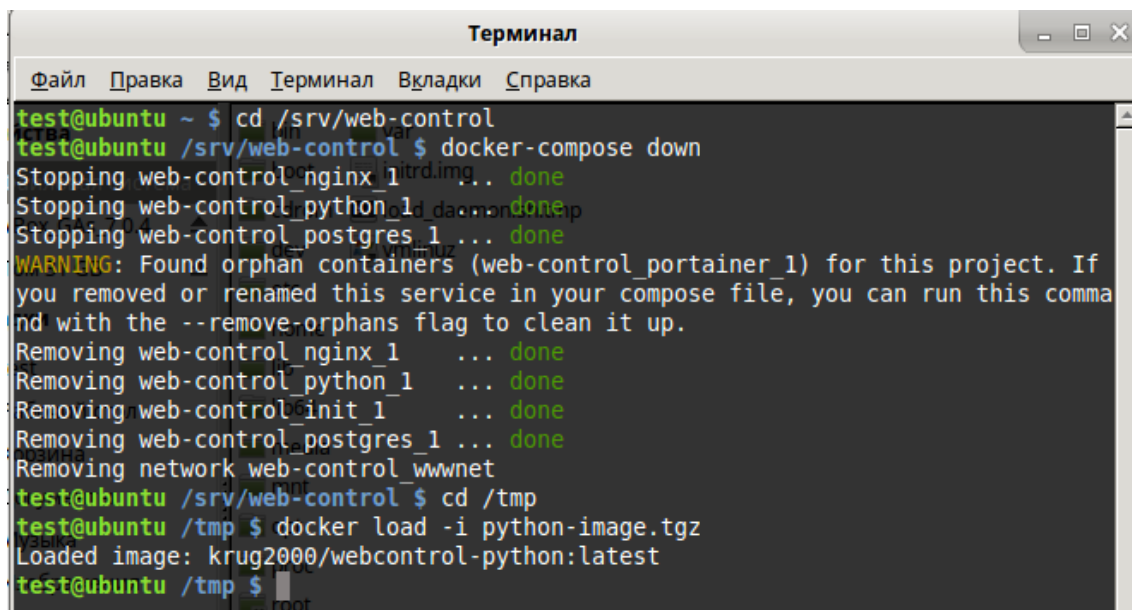
4. Перейти в папку со скопированным образом docker-файла python-image.tgz (папка /tmp):

cd /tmp

5. Загрузить новый образ docker-файла:

docker load -i python-image.tgz

Загрузка может происходить с задержкой и на экране при этом может не происходить никаких действий.



```
Терминал
Файл  Правка  Вид  Терминал  Вкладки  Справка
test@ubuntu ~ $ cd /srv/web-control
test@ubuntu /srv/web-control $ docker-compose down
Stopping web-control_nginx_1 ... done
Stopping web-control_python_1 ... done
Stopping web-control_postgres_1 ... done
WARNING: Found orphan containers (web-control_portainer_1) for this project. If
you removed or renamed this service in your compose file, you can run this comma
nd with the --remove-orphans flag to clean it up.
Removing web-control_nginx_1 ... done
Removing web-control_python_1 ... done
Removing web-control_init_1 ... done
Removing web-control_postgres_1 ... done
Removing network web-control_wwwnet
test@ubuntu /srv/web-control $ cd /tmp
test@ubuntu /tmp $ docker load -i python-image.tgz
Loaded image: krug2000/webcontrol-python:latest
test@ubuntu /tmp $
```

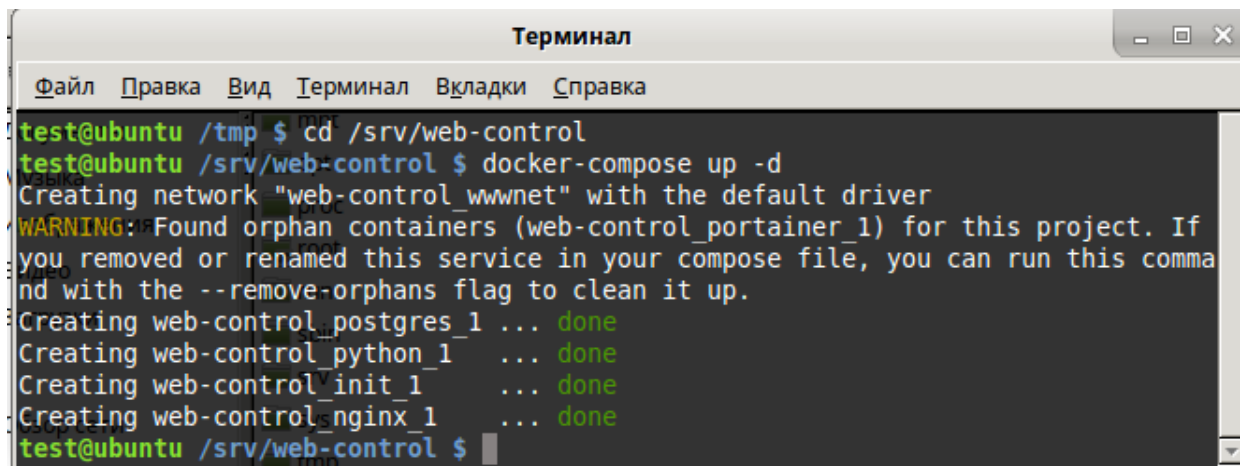
Рисунок 3.4 – Загрузка нового образа

6. Перейти обратно в папку с установленным WK (папка /srv/web-control)

cd /srv/web-control

и запустить сервер WK командой

docker-compose up -d



```
Терминал
Файл  Правка  Вид  Терминал  Вкладки  Справка
test@ubuntu /tmp $ cd /srv/web-control
test@ubuntu /srv/web-control $ docker-compose up -d
Creating network "web-control_wwwnet" with the default driver
WARNING: Found orphan containers (web-control_portainer_1) for this project. If
you removed or renamed this service in your compose file, you can run this comma
nd with the --remove-orphans flag to clean it up.
Creating web-control_postgres_1 ... done
Creating web-control_python_1 ... done
Creating web-control_init_1 ... done
Creating web-control_nginx_1 ... done
test@ubuntu /srv/web-control $
```

Рисунок 3.5 – Запуск сервера Web-контроль

В браузере в Web-Контроль для проверки версии ПО мышкой навести на логотип (рисунок 3.6)

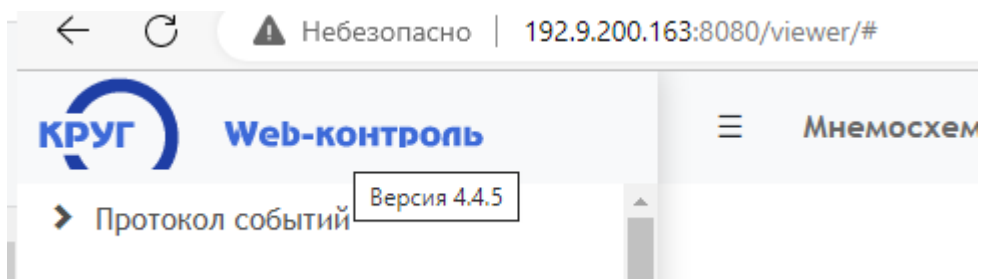


Рисунок 3.6 – Проверка версии Web-контроль

ПРИЛОЖЕНИЕ А. ОГРАНИЧЕНИЯ ПО WEB-КОНТРОЛЬ, СВЯЗАННЫЕ С ЭЛЕКТРОННЫМ КЛЮЧОМ ЗАЩИТЫ

Электронный ключ защиты является средством, подтверждающим санкционированное использование Web-Контроль. Для полноценного функционирования ПО Web-Контроль необходимо обеспечить сетевой доступ сервера WEB-Контроль к ПЭВМ, на которой установлен аппаратный ключ SCADA КРУГ-2000. Адрес этой ПЭВМ (Сервера защиты) необходимо указать в настройках сервера WEB-Контроль в разделе «Настройки приложения» (рисунок А.1):

Администрирование "WEB-контроль" SCADA КРУГ2000

ДОБРО ПОЖАЛОВАТЬ, ADMIN. [ОТКРЫТЬ САЙТ](#) / [ИЗМЕНИТЬ ПАРОЛЬ](#) / [ВЫЙТИ](#)

Домой · Viewer · Настройки приложения · Русский

Изменить Настройки приложения ИСТОРИЯ

Язык приложения: Русский

Адрес сервера защиты: 192.168.10.32

Задержка обновления мнемосхем, мс. 1000

Задержка обновления протокола событий, мс. 1000

Количество отображаемых строк протокола событий: 25

Удалить Сохранить и добавить другой объект Сохранить и продолжить редактирование СОХРАНИТЬ

Рисунок А.1 – Редактирование настроек приложения

После сохранения настроек потребуется перезагрузка сервера WEB-Контроль для корректной работы приложения с ключом защиты.

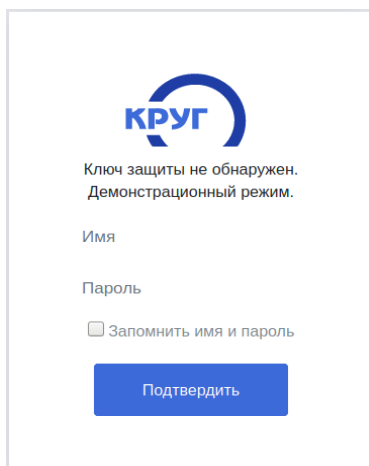


ВНИМАНИЕ!!!

Для успешной работы ПО WEB-Контроль на ПЭВМ с установленным электронным ключом защиты должны быть настроен драйвер USB-устройства ключа и сетевой менеджер лицензий.

При работе приложения с ключом защиты необходимо помнить следующие ограничения:

- В электронном ключе может быть запрещён запуск ПО Web-Контроль. В этом случае, а также в случае отсутствия сетевого доступа сервера Web-Контроль к электронному ключу защиты работа ПО Web-Контроль будет осуществляться в демонстрационном режиме. Сообщение об этом пользователи будут видеть на странице авторизации (рисунок А.2):



В демонстрационном режиме будут действовать ограничения: одновременно с ПО WEB-Контроль сможет работать только один пользователь. Продолжительность сессии пользователя будет не более 5 минут, после чего потребуются повторная авторизация. В демонстрационном режиме возможно добавить и работать только с одним сервером SCADA.

Рисунок А.2 – Страница авторизации в демонстрационном режиме

- В электронном ключе также задаётся ограничение на максимально возможное количество одновременно работающих с ПО Web-Контроль пользователей. Если такое ограничение превышено, авторизация очередного пользователя закончится неудачей с выдачей диагностического сообщения. Также в электронном ключе может быть задано ограничение на количество подключаемых SCADA серверов.

Более подробно электронный ключ защиты описан в документации к SCADA КРУГ-2000.