

**Инструкция по развертыванию ПО
Централизованная система управления и
мониторинга межсетевыми экранами
«Аргос FW»**

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ	3
1. Вводная часть	3
2. Общие положения.....	3
3. Требования к платформе и операционной системе	3
4. Доступ к установленному экземпляру ПО в сети ООО «ТехАргос»	4
5. Установка ПО	4
6. Контакты техподдержки	16

ТЕРМИНЫ И СОКРАЩЕНИЯ

ООО	– Общество с ограниченной ответственностью
ОС	– Операционная система «Astra Linux Special Edition» версии 1.8 с системой контейнерной изоляции приложений Docker
ПО	– Программное обеспечение

1. Вводная часть

Настоящий документ содержит описание процесса установки программного обеспечения Централизованная система управления и мониторинга межсетевыми экранами «Аргос FW» (ЦСУМ МЭ «Аргос FW») (далее – ЦСУМ МЭ «Аргос FW»).

ЦСУМ МЭ «Аргос FW» предназначен для поддержки и автоматизации регулярных операций управления парком межсетевых экранов «Аргос FW» администраторами информационной безопасности, информационных систем и сетевых администраторов.

2. Общие положения

Настоящий документ относится к ПО, разрабатываемому ООО «ТехАргос». Технические средства разработки, сборки и хранения ПО развернуты на серверах ООО «ТехАргос» и расположены по адресу: г. Москва, ул. Новодмитровская, 2Б.

ЦСУМ МЭ «Аргос FW» функционирует в среде, которая сконфигурирована и контролируется администратором в соответствии с эксплуатационной документацией. В зависимости от условий договора, Заказчик может предоставить доступ операторам техподдержки ООО «ТехАргос» по протоколам SSH и HTTP/HTTPS к узлам в сети Заказчика на которых необходимо установить ПО ЦСУМ МЭ «Аргос FW». При обращении к серверам трансграничная передача данных не осуществляется.

3. Требования к платформе и операционной системе

ЦСУМ МЭ «Аргос FW» устанавливается на физических серверах или виртуальных машинах с архитектурой x86/64 под управлением сертифицированной ОС «Astra Linux Special Edition» версии 1.8 с системой контейнерной изоляции приложений Docker.

Аппаратные требования к техническим средствам, на которых должны быть размещены программные компоненты ЦСУМ МЭ «Аргос FW», представлены в Таблице 1.

Таблица 1 – Аппаратные требования к техническим средствам

Характеристика	Значение
Процессор	Intel x86-64, не менее 8-ми ядер
Объем оперативной памяти	Не менее 16 Гбайт
Объем постоянной памяти (HDD/SSD)	Не менее 256 Гбайт
Интерфейсы	Не менее одного с пропускной способностью не менее 1 Гбит/с. Для целей резервирования сетевых подключений рекомендуется использование двух интерфейсов.

4. Доступ к установленному экземпляру ПО в сети ООО «ТехАргос»

В сети ООО «ТехАргос» развернут экземпляр ЦСУМ МЭ «Аргос FW», функционирующий под управлением тестового приложения, реализующего в полном объеме функции API и имитирующего пользовательское приложение Заказчика.

Доступ в сеть «ТехАргос» осуществляется по протоколу OpenVPN с использованием конфигурационных файлов, предоставленных в архиве [Минцифры VPN ЦСУМ АргосFW.zip](#) (загружен в «Иные документы» к заявке, могут быть повторно предоставлены по запросу). Параметры подключения к сети по OpenVPN:

– логин: *****

– пароль: *****

Инструкции по подключению OpenVPN представлены отдельными документами для Windows и Linux/Ubuntu (загружены в «Иные документы» к заявке, могут быть повторно предоставлены по запросу):

– «Подключение к сети ТехАргос по VPN Ubuntu»;

– «Подключение к сети ТехАргос по VPN Windows».

Примечание: одновременное подключение двух пользователей под этими параметрами не предусмотрено. При попытке второго подключения текущая сессия будет прервана.

После подключения к сети возможен доступ к виртуальной машине с развернутым экземпляром ЦСУМ МЭ «Аргос FW». Доступ осуществляется через интерфейс командной строки (CLI) по протоколу SSH (с использованием SSH-клиента, например, Putty). Параметры подключения к виртуальной машине по SSH:

– IP-адрес: 172.17.100.2 (порт 22)

– логин: *****

– пароль: *****

Примечание: процесс подключения к сети по протоколу SSH описан в документе: Инструкция по доступу к технологическому стеку предоставленного экземпляра ПО ЦСУМ МЭ «Аргос FW».

Для доступа в WEB-интерфейс ЦСУМ МЭ «Аргос FW» по протоколу HTTP следует использовать:

– IP-адрес: 172.17.100.2 (порт 22)

– логин: *****

– пароль: *****

Примечание: логины и пароли указаны в загруженной инструкции по развертыванию к заявлению о включении сведений о программном обеспечении в реестр российского программного обеспечения либо предоставляются по обращению в службу техподдержки ООО «ТехАргос» по контактам, указанным в разделе 6 данной инструкции.

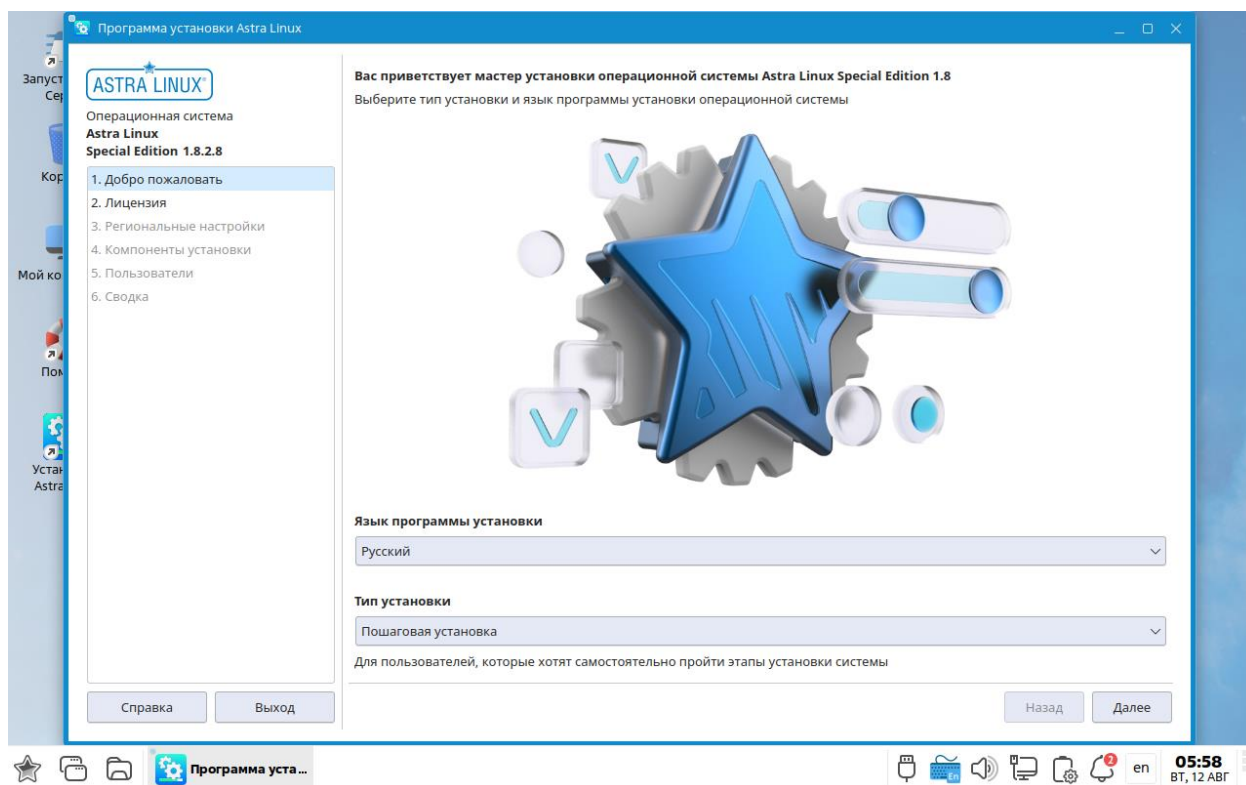
5. Установка ПО

Подготовка операционной системы:

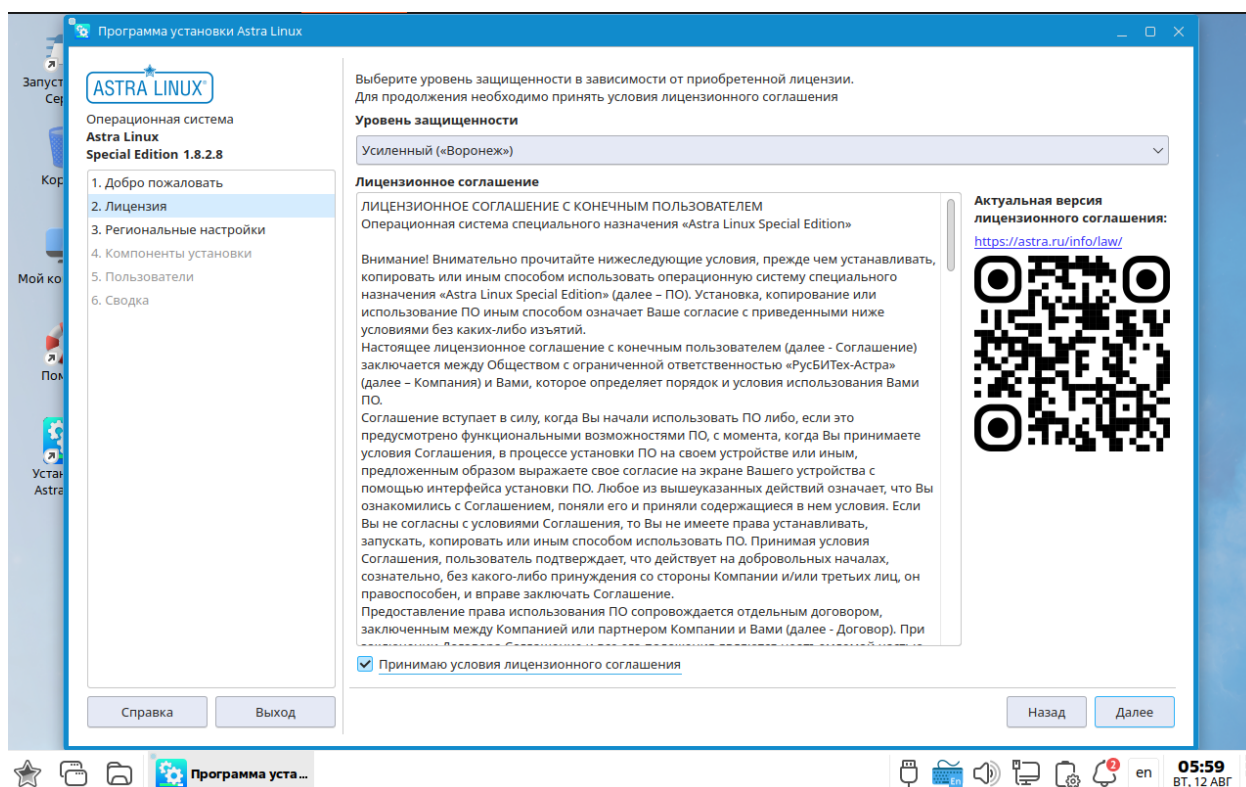
Использовать образ astra-1.8.2.8-06.05.25_11.44.iso ОС «Astra Linux Special Edition».

Установка и настройка системы:

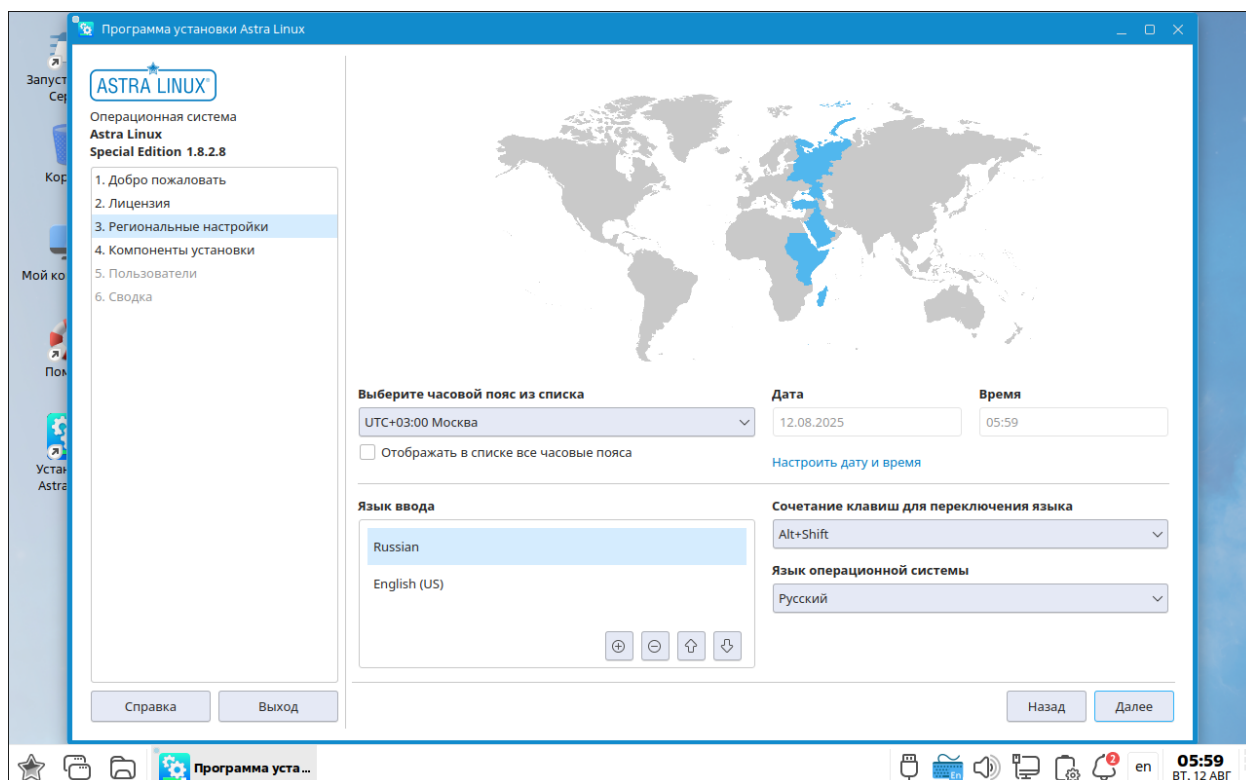
1. Пользователю отображается приветственное окно с выбором языка и типа установки. Необходимо нажать кнопку «Далее».



2. В выпадающем списке выбора уровня защищенности выбрать «Усиленный («Воронеж»)» и принять условия лицензионного соглашения.

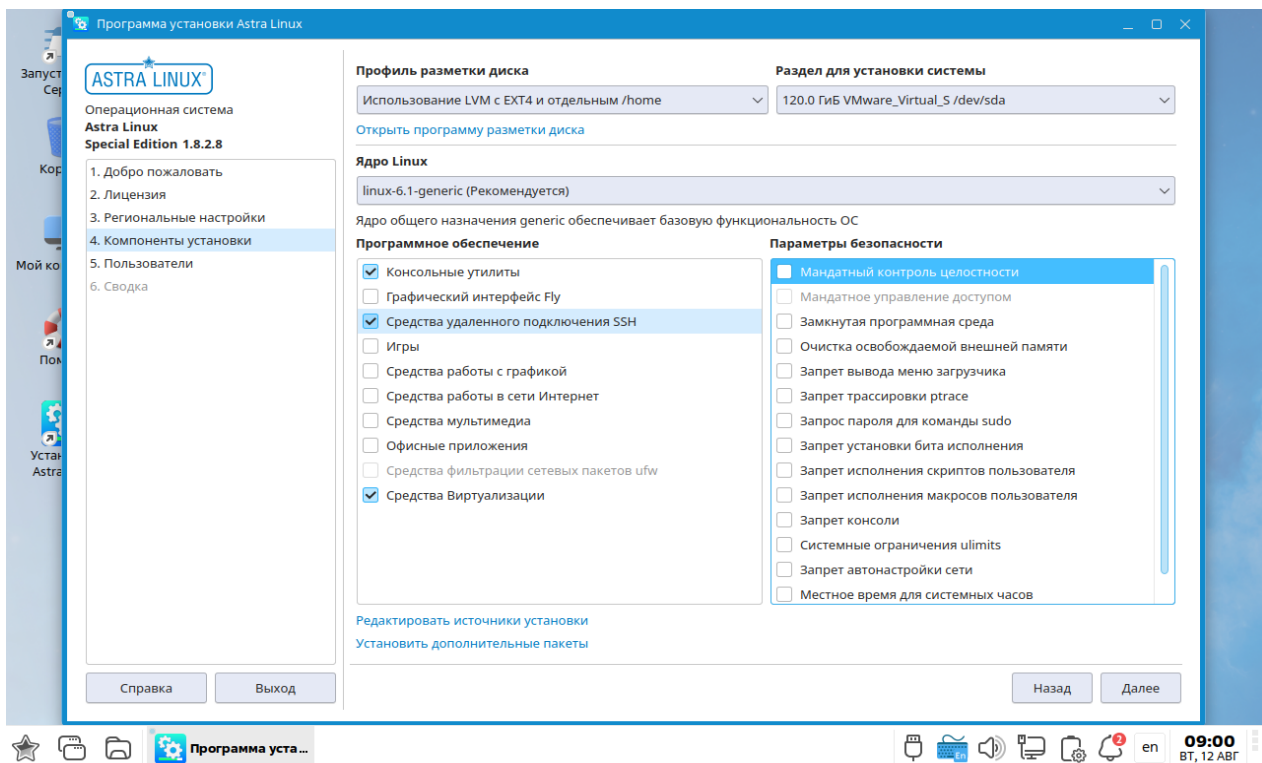


3. В окне «Региональных настроек» нажать «Далее».

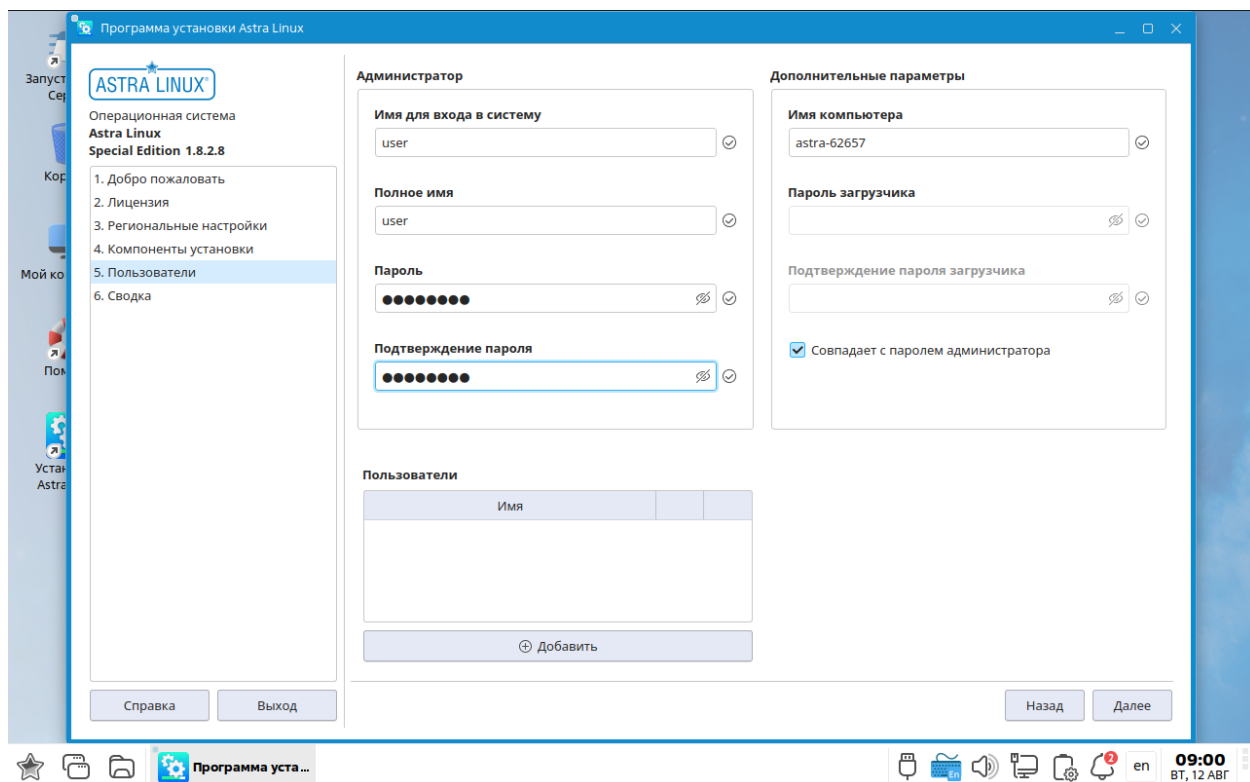


4. В окне «Компоненты установки» предлагается выбрать параметры безопасности и программное обеспечение, которые необходимо установить. Требуется убрать все галочки с компонентов и поставить:

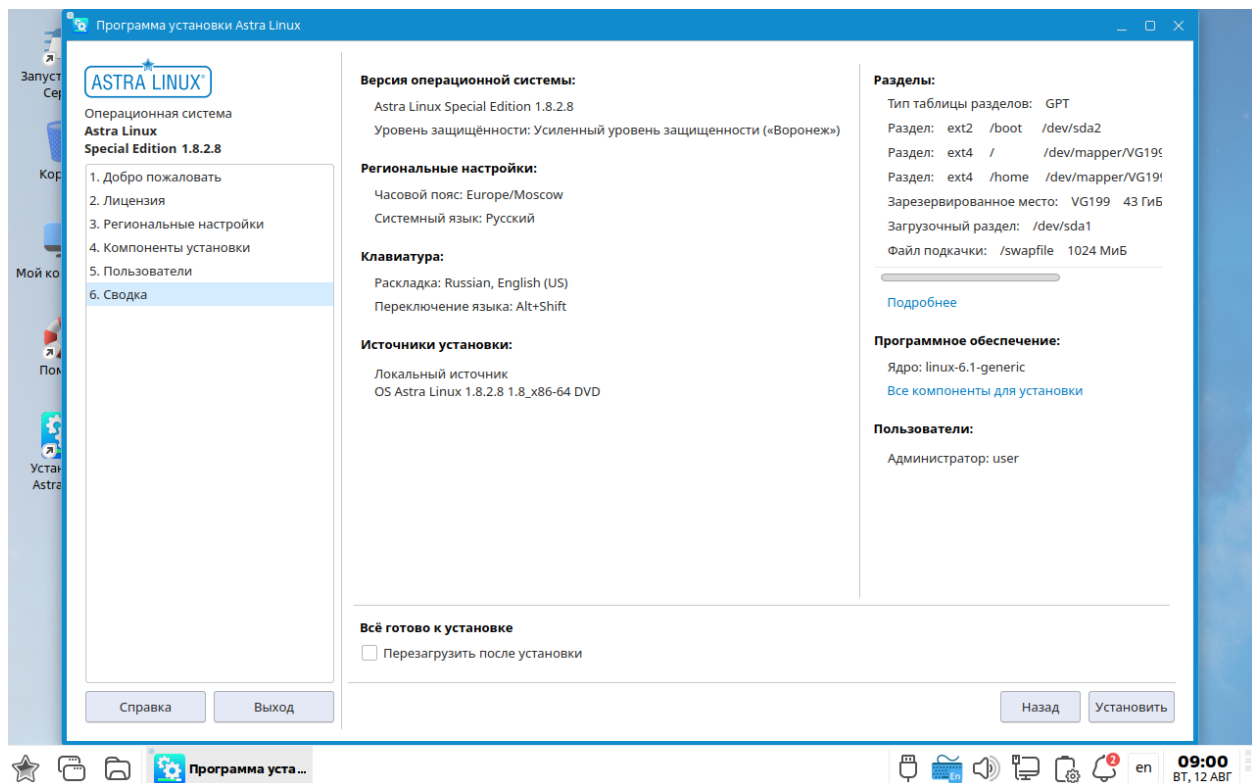
- Программное обеспечение:
 - Консольные утилиты;
 - Средства удаленного подключения SSH;
 - Средства виртуализации.
- Параметры безопасности
 - Запрет автонастройки сети (не требуется для развертывания в среде виртуализации).



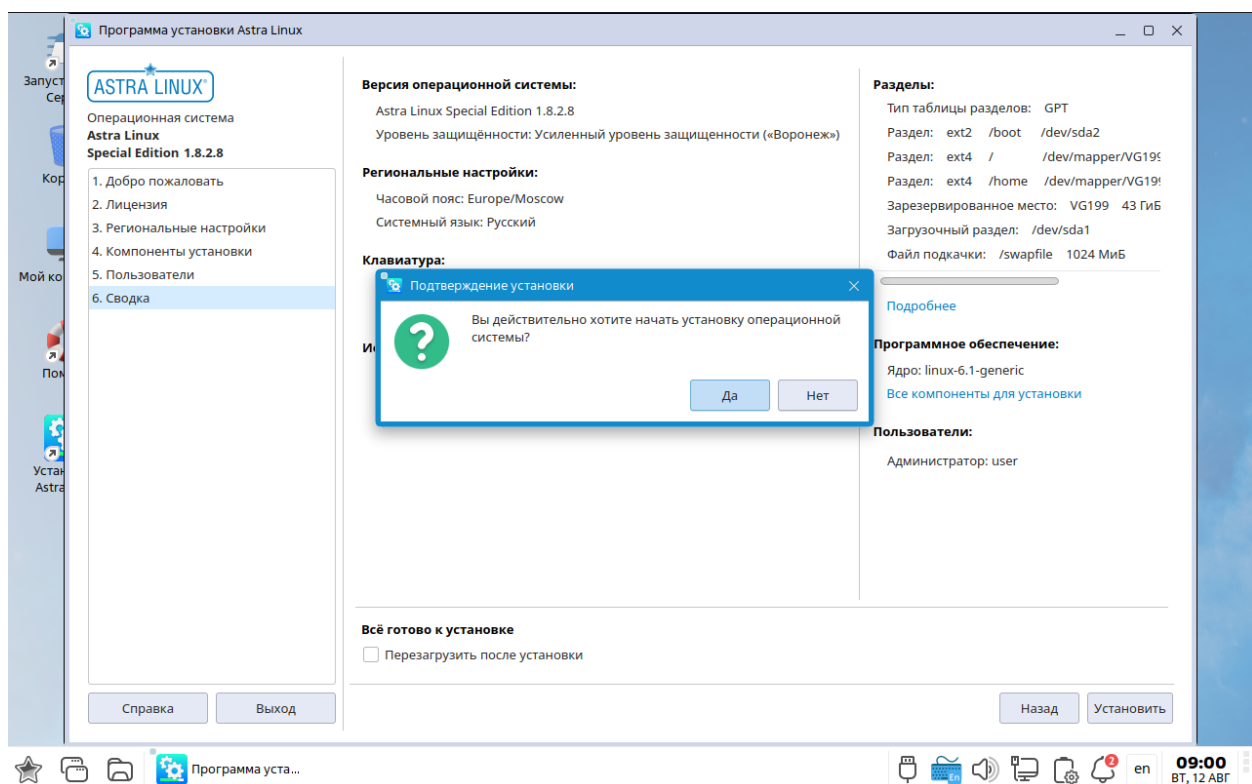
5. В окне «Пользователи» указать имя для входа и пароль администратора.



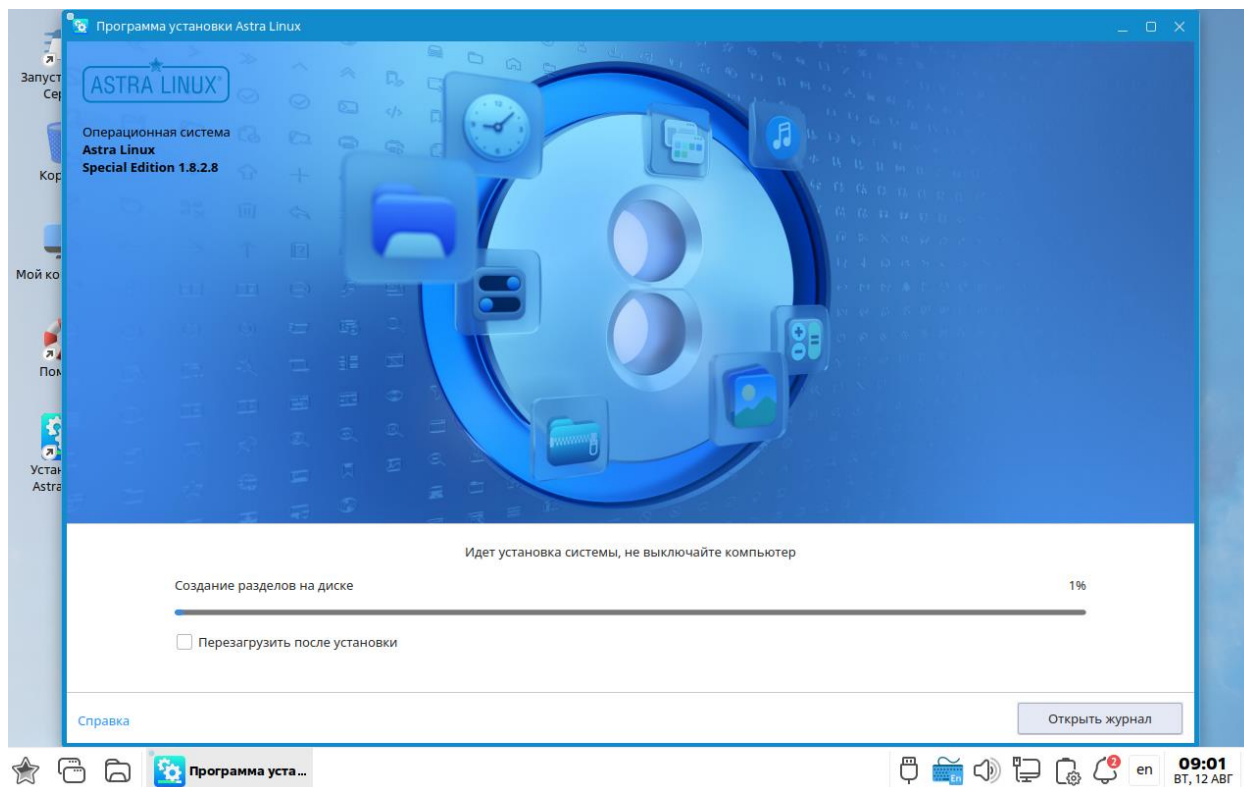
6. В окне «Сводки» нажать «Установить».



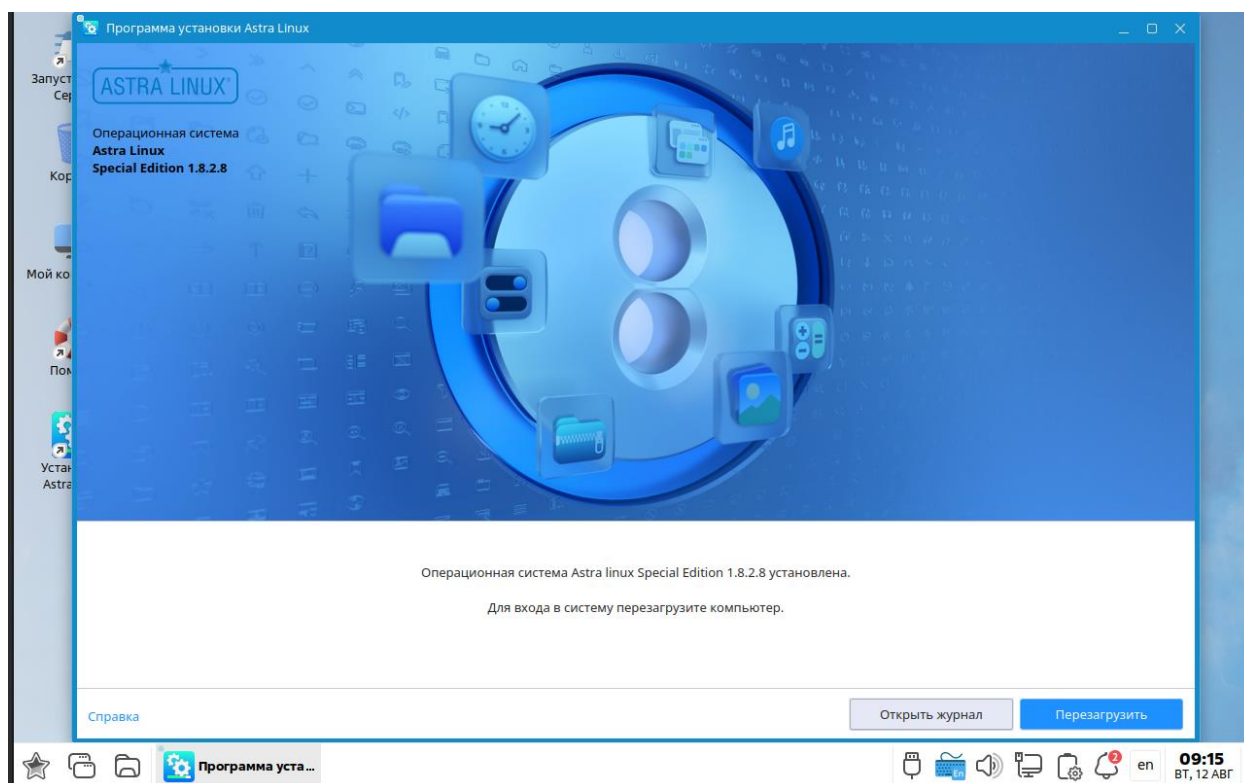
7. Согласится с установкой системы.



8. Дождаться окончания процесса установки.



9. По завершению установки необходимо нажать «Перезагрузить».



10. После перезагрузки откроется рабочее пространство.

```
Astra Linux 1.8.2 astra-62657 tty1
astra-62657 login:
```

Предустановочные действия

Проверка репозитория

Рекомендуется проверить правильность указанных репозитория в `/etc/apt/sources.list`. Если машина имеет доступ в интернет и локальные репозитории отсутствуют, используйте репозитории, указанные ниже:

```
/etc/apt/sources.list
```

```
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-extended/ 1.8_x86-64 main contrib
non-free non-free-firmware
```

```
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main/ 1.8_x86-64 main contrib non-
free non-free-firmware
```

Обновить базу данных доступных пакетов через команду:

```
sudo apt update
```

Установка пакетов

Перед развертыванием дистрибутива необходимо установить следующие пакеты:

```
sudo apt install docker.io docker-compose-v2 git make
```

```
sudo usermod -aG docker $USER
```

```
newgrp docker
```

Редактирование политик безопасности

Начиная с «Astra Linux Special Edition» 1.74 Update 4 (№ 2023-0426SE17), в состав ОС добавлен сканер уязвимостей Openscap, который проверяет наличие уязвимостей по базе oval-db. Сканирование уязвимостей выполняется с использованием файла БД уязвимостей, рекомендуемого ФСТЭК России и содержащего сведения об уязвимостях банка данных угроз безопасности информации ФСТЭК России. При обнаружении уязвимостей дальнейшее использование образа контейнера запрещено. Чтобы

исполнение контейнера не прерывалось инструментом сканирования Openscap необходимо создать файл `/etc/docker/daemon.json`.`

```
mkdir /etc/docker/
```

```
sudo nano /etc/docker/daemon.json
```

Добавить в него строку.

```
{ "astra-sec-level" : 6 }
```

И перезагрузить службу docker:

```
sudo systemctl restart docker
```

Развертывание дистрибутива

Архив для развертывания

Структура архива

Структура архива

argos-control-system.tar.gz

```
|
| └─ Makefile                # команды для управления ЦСУМ (up, down, restart, stop, status)
| └─ README.md              # документация и руководство по развертыванию
|
| └─ deploy/                # env-файлы и docker-compose конфигурации
|   └─ .env                 # основные переменные окружения
|   └─ .build.env           # переменные для сборки
|   └─ .local.env           # локальное окружение
|   └─ docker-compose.yml   # базовый compose-файл
|   └─ docker-compose.prod.yml # compose-файл для запуска из готовых образов
|     └─ README.md          # описание compose-файлов
|
| └─ scripts/               # скрипты для управления ЦСУМ (вызываются через Makefile)
|   └─ ...                  # копируем файлы из репозитория argos-control-system/deploy
|
| └─ volumes/               # конфиги и данные, монтируемые внутрь контейнеров
|   └─ ...                  # копируем файлы из репозитория argos-control-system/deploy
|
| └─ images/                # собранные образы (docker save/load)
|   └─ api-gw.tar
```

```
├─ 📦 nginx.tar
├─ 📦 ctxcontrol.tar
├─ 📦 vector.tar
├─ 📦 usercontrol.tar
├─ 📦 lokicontrol.tar
├─ 📦 router.tar
├─ 📦 keycloak.tar
├─ 📦 grafana.tar
├─ 📦 blog.tar
├─ 📦 vectorcontrol.tar
├─ 📦 controller.tar
├─ 📦 postgres.tar
├─ 📦 frontend.tar
├─ 📦 influxdb.tar
├─ 📦 node_exporter.tar
├─ 📦 prometheus.tar
├─ 📦 gateway.tar
├─ 📦 loki.tar
└─ 📦 clixon-adapter.tar
```

Содержание архива

1. /images - собранные docker образы, которые должны формироваться автоматически в результате CI и храниться в Nexus.
2. /volumes - папка, которая хранит разделы для контейнеров. Часть разделов создастся при развертывании, часть разделов уже созданы.
3. /scripts - содержит скрипты развертывания.
4. /deploy - содержит env-файлы и docker-compose конфигурации

Установка ЦСУМ МЭ «Аргос FW»

Рекомендуется выставить переменные окружения (/deploy/.env)

```
# =====
# COMMON SETTINGS
# =====

HOST_IP=172.17.100.2

HOST_DOMAIN=t-argos.ru
```

```
DOMAIN_HOST_DOMAIN=cmms.t-argos.ru
BACKEND_SYSTEM_ADMIN=sysadmin
BACKEND_SYSTEM_ADMIN_PASS=adminpassword
CMMS_ADMIN=admin
CMMS_ADMIN_PASS=admin
```

```
# Network settings
```

```
NETWORK_SUBNET=172.20.0.0/16
```

```
# =====
```

```
# POSTGRESQL
```

```
# =====
```

```
POSTGRES_PORT=5432
```

```
POSTGRES_ADMIN_USER=${BACKEND_SYSTEM_ADMIN}
```

```
POSTGRES_ADMIN_PASSWORD=${BACKEND_SYSTEM_ADMIN_PASS}
```

```
# Service credentials
```

```
POSTGRES_KEYCLOAK_USER=keycloak
```

```
POSTGRES_KEYCLOAK_PASSWORD=keycloakpassword
```

```
POSTGRES_KEYCLOAK_DATABASE=keycloak
```

```
POSTGRES_GRAFANA_USER=grafana
```

```
POSTGRES_GRAFANA_PASSWORD=grafanapassword
```

```
POSTGRES_GRAFANA_DATABASE=grafana
```

```
POSTGRES_CONTEXT_USER=context
```

```
POSTGRES_CONTEXT_PASSWORD=contextpassword
```

```
POSTGRES_CONTEXT_DATABASE=context
```

```
POSTGRES_VECTOR_USER=vectoragent
```

```
POSTGRES_VECTOR_PASSWORD=vectorpassword
```

```
POSTGRES_VECTOR_DATABASE=vectoragent
```

```
POSTGRES_BLOG_USER=blog
```

POSTGRES_BLOG_PASSWORD=blogpassword

POSTGRES_BLOG_DATABASE=blog

POSTGRES_LOKI_CTRL_USER=loki

POSTGRES_LOKI_CTRL_PASSWORD=lokipassword

POSTGRES_LOKI_CTRL_DATABASE=loki

POSTGRES_CLIXON_ADAPTER_USER=clixonadapter

POSTGRES_CLIXON_ADAPTER_PASS=clixonadapter

POSTGRES_CLIXON_ADAPTER_DBNAME=clixonadapter

=====

INFLUXDB

=====

INFLUXDB_PORT=8086

INFLUXDB_ADMIN_TOKEN=eyJ8xVX4h5PwK_I0USMN6Yp6GZ-

6AJn3OGFnKOQpm0jj1sEh_M2XB1UxzsQHb3CPyCFpsAF8OJ5ipAd4wZDB9kw==

INFLUXDB_LOG_LEVEL=info

=====

LOKI

=====

LOKI_PORT=3100

LOKI_TENANT_ID=__all_services__

=====

GRAFANA

=====

GRAFANA_PORT=3000

GRAFANA_ADMIN_PASSWORD=\${BACKEND_SYSTEM_ADMIN_PASS}

GRAFANA_LOG_LEVEL=error

KEYCLOAK_GRAFANA_CLIENT_UUID=b1918cad-e6a8-40b0-9c2a-5ab016d79c39

=====

KEYCLOAK

=====

KEYCLOAK_PORT=8443

KEYCLOAK_PAM_ID=pam-sso

KEYCLOAK_PAM_SECRET=PJmMVgsgoA4g2BF2SHtjmKnkUQwpO4Ls

KEYCLOAK_PAM_PROTOCOL=openid-connect

SYSTEM_KEYCLOAK_REALM=cmms

SYSTEM_KEYCLOAK_ENDPOINT=https://\${HOST_IP}:\${KEYCLOAK_PORT}

SYSTEM_KEYCLOAK_CLIENTID=pam-sso

SYSTEM_KEYCLOAK_SECRET=PJmMVgsgoA4g2BF2SHtjmKnkUQwpO4Ls

```
SYSTEM_KEYCLOAK_CLIENTSCOPE=pam-sso-dedicated
DOMAIN_SYSTEM_KEYCLOAK_ENDPOINT=https://keycloak.cmms.t-argos.ru
KEYCLOAK_GRAFANA_ID=cmms-sso
KEYCLOAK_GRAFANA_SECRET=uAgEvDTaFYvzqr287p2qZFli7habElf8
KEYCLOAK_GRAFANA_REDIRECT_ONE=https://${HOST_IP}:${GRAFANA_PORT}/login/generic_oauth
KEYCLOAK_GRAFANA_REDIRECT_TWO=https://localhost:${GRAFANA_PORT}/login/generic_oauth
KEYCLOAK_GRAFANA_REDIRECT_THREE=https://grafana:${GRAFANA_PORT}/login/generic_oauth
KEYCLOAK_GRAFANA_PROTOCOL=openid-connect
KEYCLOAK_PAM_REDIRECT_ONE=urn:ietf:wg:oauth:2.0:oob
```

```
# =====
```

```
# VECTOR
```

```
# =====
```

```
VECTOR_PORT=6001
```

```
VECTOR_VOLUME_PORT=6001
```

```
VECTOR_PORT_BEGIN=9002
```

```
VECTOR_PORT_END=9080
```

```
VECTORCONTROL_PORT=5007
```

```
VECTORCONTROL_TEMPLATE_PATH=src/template/vector.tmpl
```

```
SYSTEM_TENANT=__system__
```

```
VECTOR_TENANT_SYSTEM_TRANSPORT=udp
```

```
# =====
```

```
# CLIXON
```

```
# =====
```

```
CLIXON_REST_PORT=8080
```

```
CLIXON_NET_PORT=2222
```

```
CLIXON_DBG_LEVEL="event -D msg -D detail -D nacm -D backend -D parse"
```

```
CLIXON_BACKEND_SSH_PASSWORD=backend
```

```
# =====
```

```
# SERVICES PORTS
```

```
# =====
```

```
LOKI_CTRL_HTTP_PORT=7000
```

```
BLOG_HTTP_PORT=8004
```

```
ROUTER_GRPC_PORT=6000
```

```
ROUTER_HTTP_PORT=5999
```

```
USER_CTRL_HTTP_PORT=8002
```

```
CTX_CTRL_HTTP_PORT=8003
```

```
API_GW_HTTP_PORT=8001
```

```
CLIXON_ADAPTER_HTTP_PORT=8005
```

```
APP_PORT=3001
```

```
# =====
```

```
# LOGGING AND RUNTIME MODES
```

```
# =====
LOKI_CTRL_LOG_LEVEL=debug
BLOG_LOG_LEVEL=debug
ROUTER_LOG_LEVEL=debug
USER_CTRL_LOG_LEVEL=debug
CTX_CTRL_LOG_LEVEL=debug
CLIXON_ADAPTER_LOG_LEVEL=debug
API_GW_LOG_LEVEL=debug
API_GW_GIN_MODE=release
FRONTEND_NODE_ENV=production

# =====
# MONITORING
# =====
NODE_PORT=9100
PROMETHEUS_PORT=9090
PROMETHEUS_PROMETHEUS_TARGETS=prometheus:9090
PROMETHEUS_NODEEXPORTER_TARGETS=node_exporter:9100

# =====
# FRONTEND
# =====
NUXT_PUBLIC_VERSION=2.2.3
NUXT_PUBLIC_GRAFANA_HOST=https://${HOST_IP}
NUXT_PUBLIC_API_GATEWAY_HOST=https://${HOST_IP}
NUXT_PUBLIC_NODE_ENV=production
NUXT_PUBLIC_CONFIG_FILE_MAX_SIZE_BYTES=10485760
NUXT_PUBLIC_CONFIG_FILE_ALLOWED_EXTENSIONS=.xml
# NUXT_PUBLIC_ORIGIN=https://172.17.100.2
DOMAIN_NUXT_PUBLIC_GRAFANA_HOST=https://grafana.cmms.t-argos.ru
DOMAIN_NUXT_PUBLIC_API_GATEWAY_HOST=https://cmms.t-argos.ru
DOMAIN_NUXT_PUBLIC_CMMS_DOMAIN=cmms.t-argos.ru
DOMAIN_NUXT_SSH_HOST=cmms.t-argos.ru
DOMAIN_NUXT_PUBLIC_ORIGIN=https://cmms.t-argos.ru
После этого выполнить команду
make prod
```

6. Контакты техподдержки

По вопросам процесса развертывания ПО ЦСУМ МЭ «Аргос FW», настройки и функционирования обращаться в службу техподдержки ООО «ТехАргос», любым из перечисленных способов:

- Телефон: +7(495)411-90-37;
- E-mail техподдержки: argos-fw@t-argos.ru.

ООО «ТехАргос»

127015, г. Москва, ул. Новодмитровская, 2Б, ДЦ «Дмитровский»

Телефон: +7(495) 411-90-37

Web: <https://t-argos.ru/>

E-mail: mail@t-argos.ru