

Программный комплекс по защите
системно-технической инфраструктуры
«Efros Defence Operations»
Руководство администратора

Аннотация

Данный документ представляет собой руководство администратора для работы с программным комплексом по защите системно-технической инфраструктуры «Efros Defence Operations» (ПК «Efros DO» или комплекс). Руководство содержит сведения, необходимые пользователям для установки и настройки работы комплекса.

Администратор должен знать стандартные программные средства (операционные системы, утилиты, офисные пакеты, антивирусные пакеты), а также обладать общими знаниями по администрированию сетевых устройств.

Содержание

1 Сведения о технических и программных средствах, обеспечивающих выполнение функций программы.....	4
2 Подготовка к установке программы.....	7
3 Установка, настройка и удаление программы.....	8
3.1 Состав и содержание дистрибутива.....	8
3.2 Порядок установки.....	9
3.3 Перенастройка сети.....	20
3.4 Лицензирование.....	20
3.4.1 Online активация комплекса.....	22
3.4.2 Offline активация комплекса.....	24
3.4.3 Реактивация лицензии комплекса.....	28
3.5 Удаление изделия.....	30
3.6 Windows-агент ПК «Efros DO».....	32
3.6.1 Установка Windows-агента.....	32
3.6.2 Настройка параметров службы windows-агента.....	34
3.7 Суппликант ПК «Efros DO».....	38
3.7.1 Установка суппликанта ПК «Efros DO».....	38
3.7.2 Настройка параметров суппликанта.....	38
4 Обновление программного комплекса.....	42
5 Сообщения администратору.....	43
Перечень сокращений.....	44

1 Сведения о технических и программных средствах, обеспечивающих выполнение функций программы

ПК «Efros DO» является высокопроизводительным комплексом по защите системно-технической инфраструктуры. Архитектура комплекса построена на основе микросервисов и модулей:

- платформа интеграции – единый интерактивный интерфейс, представляющий полный контроль над автоматизацией процессов информационной безопасности (далее – ИБ);
- функциональные модули – «Efros Network Assurance» («Efros NA»), «Efros Firewall Assurance» («Efros FA»), «Efros Network Access Control» («Efros NAC»), «Efros Integrity Check Compliance» («Efros ICC»), «Efros Vulnerability Control» («Efros VC»), «Efros Network Flow Analysis» («Efros «NFA»), «Efros Change Manage» («Efros CM»);
- микросервис аутентификации и авторизации пользователей ПК «Efros DO»;
- микросервис лицензирования;
- микросервис объектов защиты;
- микросервис сбора метрик ИБ;
- микросервис расписаний;
- микросервис событий и уведомлений;
- микросервис маршрутизации запросов;
- модуль обмена данными Apache Kafka;
- модуль хранения данных Opensearch;
- подсистема хранения данных: система управления базами данных (далее – СУБД).



Конфигурация ПК «Efros DO» зависит от наличия лицензий на функциональные модули «Efros NA», «Efros FA», «Efros NAC», «Efros ICC», «Efros VC», «Efros «NFA», «Efros CM»).

Минимальный состав технических средств электронно-вычислительной машины (ЭВМ)¹ для установки серверной части и внешних модулей ПК «Efros DO» рассчитывается на основе данных, приведенных в таблице 1.

¹ Под ЭВМ понимается электронно-вычислительная машина, совместимая с архитектурой Intel x86 (x86_64).

Таблица 1 – Технические требования к среде функционирования ПК «Efros DO» и прикладному ПО

Поле	Параметры		
Количество объектов защиты (ОЗ)	До 500	До 1000	До 2000*
Требования к программному обеспечению			
ОС	Astra Linux Special Edition (v. 1.6, v.1.7), сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.) ² ; Astra Linux Common Edition (v.2.12); Альт 10 Server; РЕД ОС 7.3 Муром, сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.)		
Поддерживаемые системы управления базами данных (СУБД)	СУБД PostgreSQL 13; СУБД «Jatoba»		
Прикладное ПО	Docker 18.03.0 и выше; Docker-compose v2.9.0; Confluent Kafka 5.5.0		
Требования к аппаратному обеспечению			
Процессор	12 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)
Оперативная память, не менее Гб	от 16 Гб	от 32 Гб	от 64 Гб
Жесткий диск, Гб (ПК + СУБД)	от 600 Гб	от 1200 Гб	от 2400 Гб
Сервер ПК, Гб	от 200 Гб	от 200 Гб	от 200 Гб
Сервер СУБД, Гб	от 400 Гб	от 1000 Гб	от 2200 Гб
Сетевая карта	1 Гбит/с	1 Гбит/с	1 Гбит/с
Требования для функционирования модуля «Efros NAC»			
TACACS+	порт 49		
RADIUS	порты 1812, 1813		
Требования для функционирования модуля «Efros NFA»			
Netflow v9+, IPFIX	порт 2056		
sFlow	порт 6343		
Netflow v5	порт 2055		
Требования для функционирования модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros CM»			
Для подключения Windows-агента	порт 20002		
syslog	порт 514		
SNMP Trap / Inform	порт 162		
Windows-агент			
ОС	Windows**		
Процессор	1,6 ГГц		


² Рекомендуется использовать ОС с ядром 5.15-Generic

Поле	Параметры
Оперативная память	1 Гб
Жесткий диск	100 Мб
Единый интерактивный веб-интерфейс – обеспечивает доступ пользователей к функциональности ПК «Efros DO» с использованием браузера, который работает на основе проекта с открытым кодом Chromium	
*От 2000 ОЗ – параметры рассчитываются индивидуально. Необходимо обращение в техподдержку;	
**ОС серии Windows:	
Windows Server 2008R2 Foundation Edition SP1 (64-разрядная);	
Windows Server 2008R2 Standard Edition SP1 (64-разрядная);	
Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная);	
Windows Server 2008R2 Datacenter Edition SP1 (64-разрядная);	
Windows Server 2012/2012R2 Foundation (64-разрядная);	
Windows Server 2012/2012R2 Essentials (64-разрядная);	
Windows Server 2012/2012R2 Standard (64-разрядная);	
Windows Server 2012/2012R2 Datacenter (64-разрядная);	
Windows Server 2016 Standard (64-разрядная);	
Windows Server 2016 Datacenter (64-разрядная);	
Windows Server 2016 Essentials (64-разрядная);	
Windows Server 2019 Standard (64-разрядная);	
Windows Server 2019 Datacenter (64-разрядная);	
Windows Server 2019 Essentials (64-разрядная);	
Windows 7 Professional SP1 (32-разрядная/64-разрядная);	
Windows 7 Enterprise SP1 (32-разрядная/64-разрядная);	
Windows 7 Ultimate SP1 (32-разрядная/64-разрядная);	
Windows 8.1 Core (32-разрядная/64-разрядная);	
Windows 8.1 Professional (32-разрядная/64-разрядная);	
Windows 8.1 Enterprise (32-разрядная/64-разрядная);	
Windows 10 Home (32-разрядная/64-разрядная);	
Windows 10 Pro (32-разрядная/64-разрядная);	
Windows 10 Enterprise (32-разрядная/64-разрядная)	

Для корректной работы ПК «Efros DO» необходимо использование только лицензионного программного обеспечения.

2 Подготовка к установке программы

Перед началом эксплуатации ПК «Efros DO» необходимо ознакомиться с сопроводительными документами.

 Установка изделия должна осуществляться под руководством специально подготовленного персонала.

При установке изделия на ЭВМ рекомендуется консультироваться с технической поддержкой ООО «Газинформсервис».

Телефон технической поддержки: 8 (800) 700-09-87

Факс: +7 (812) 677-20-51

Официальный сайт: <https://www.gaz-is.ru/>

E-mail: support@gaz-is.ru

Электронный адрес для обращения в техническую поддержку:

<https://www.gaz-is.ru/poddergka/zajavka.html>

Пользователи изделия могут обратиться в техническую поддержку по указанному телефону в рабочие дни с 09:00 до 18:00 (в пятницу до 17:00), круглосуточно на сайте разработчика или по адресу электронной почты разработчика (производителя).

3 Установка, настройка и удаление программы

3.1 Состав и содержание дистрибутива

Комплект установочных файлов предоставляется производителем в виде ссылки для скачивания. Также комплект может быть поставлен заказчику на установочном компакт-диске.

На дистрибутивном носителе данных (установочный компакт-диск) записан комплект компонентов ПК «Efros DO». Состав дистрибутива указан в таблице 2.

Таблица 2 – Состав дистрибутива ПК «Efros DO» для установки на ОС Astra Linux Special Edition (v. 1.6, v.1.7), Astra Linux Common Edition (v.2.12), Альт 10 Server и РЕД ОС 7.3 Муром

Файл	Назначение
Архив изделия	
efros-do_<название ОС>.tar.gz	дистрибутив, содержащий все компоненты программы и зависимости
deploy.sh	скрипт для установки ПК «Efros DO» в систему
EDO-Agent-<название ОС>-suplicant.deb	файл для установки суппликанта ПК «Efros DO» на конечную точку

3.2 Порядок установки

- i** Процесс установки дистрибутива одинаков для различных поддерживаемых операционных систем (Astra Linux Special Edition (v. 1.6, v.1.7), Astra Linux Common Edition (v.2.12), Альт 10 Server и РЕД ОС 7.3 Муром). При установке на целевую ОС необходимо скопировать архив дистрибутива, действия со скриптом аналогичны.
- !** При установке ПК «Efros DO» на ОС Astra Linux обязательно выполнить действия, описанные в п. 3.2.1. Для других видов ОС п. 3.2.1 пропускается.
- !** При установке ПК «Efros DO» на ОС РЕД ОС 7.3 Муром автоматические выключается система SELinux.

Ниже приведен порядок установки ПК «Efros DO». В качестве примера взята ОС Astra Linux Special Edition v.1.7 (далее – ОС Astra Linux SE). Для ПК «Efros DO» на этапе завершения установки ОС Astra Linux SE нет необходимости в добавлении каких-либо наборов программного обеспечения (рис. 1).

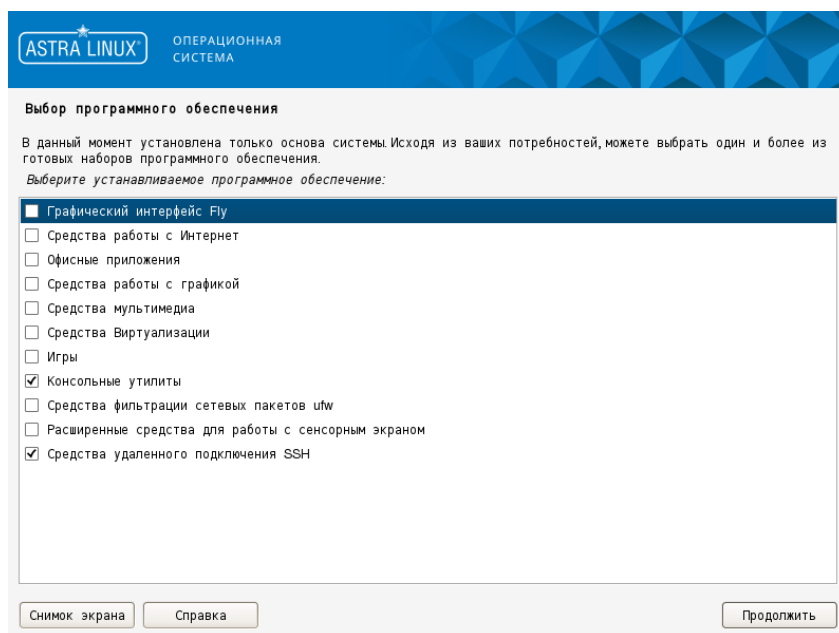


Рисунок 1 – Завершение установки ОС Astra Linux SE

3.2.1 Настройка политик безопасности ОС

Перед установкой ПК «Efros DO» необходимо выполнить следующие настройки ОС Astra Linux SE:

- 1) Перейти в меню «Пуск» → «Системные» → «Политика безопасности» (рис. 2).

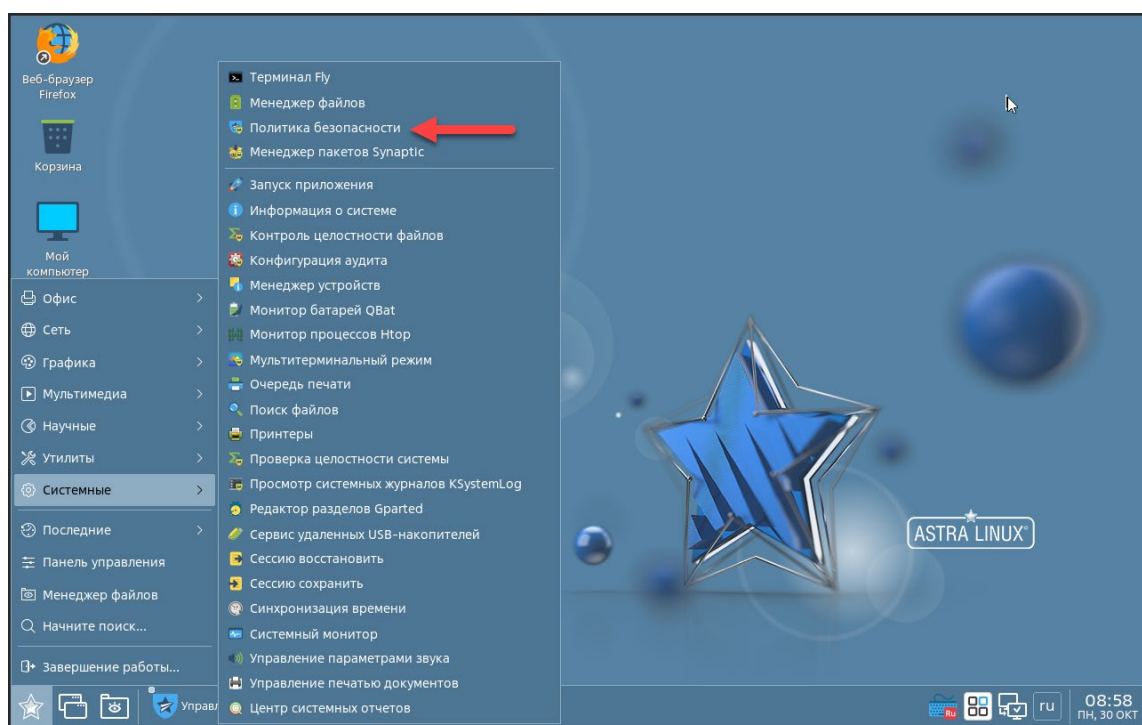


Рисунок 2 – Вкладка «Политики безопасности»

2) Ввести пароль администратора ОС (рис. 3).

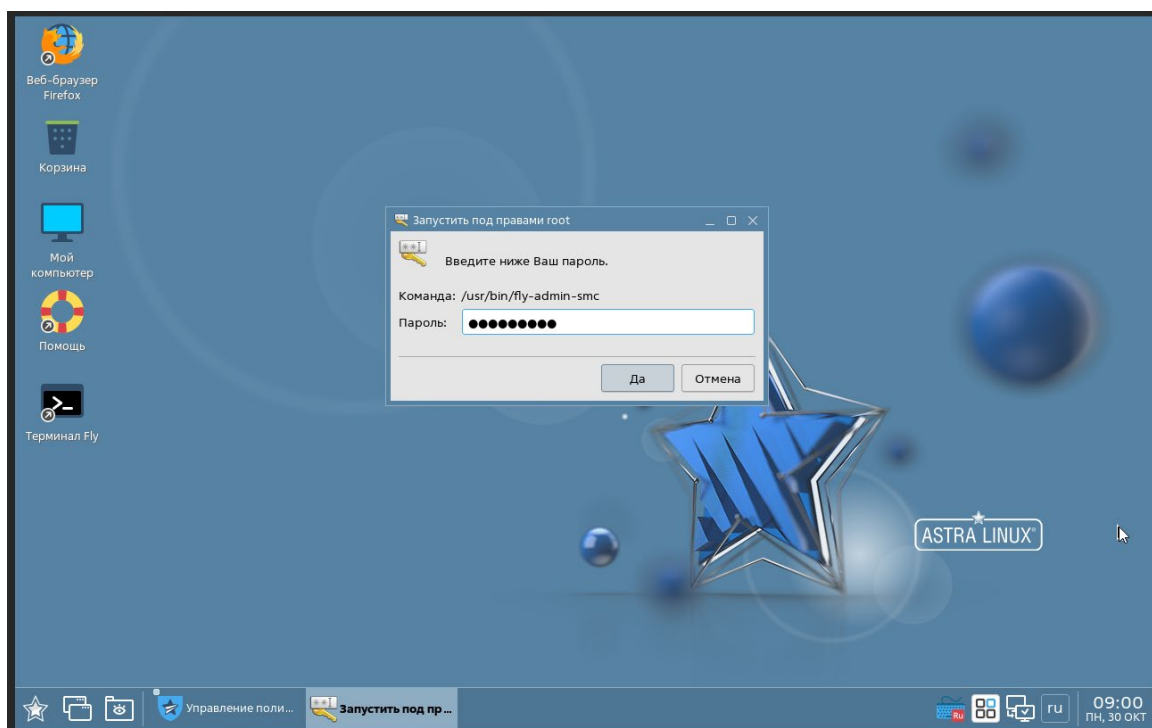


Рисунок 3 – Ввод пароля администратора ОС

3) Откроется окно «Управление политикой безопасности – Локальная политика» (рис. 4).

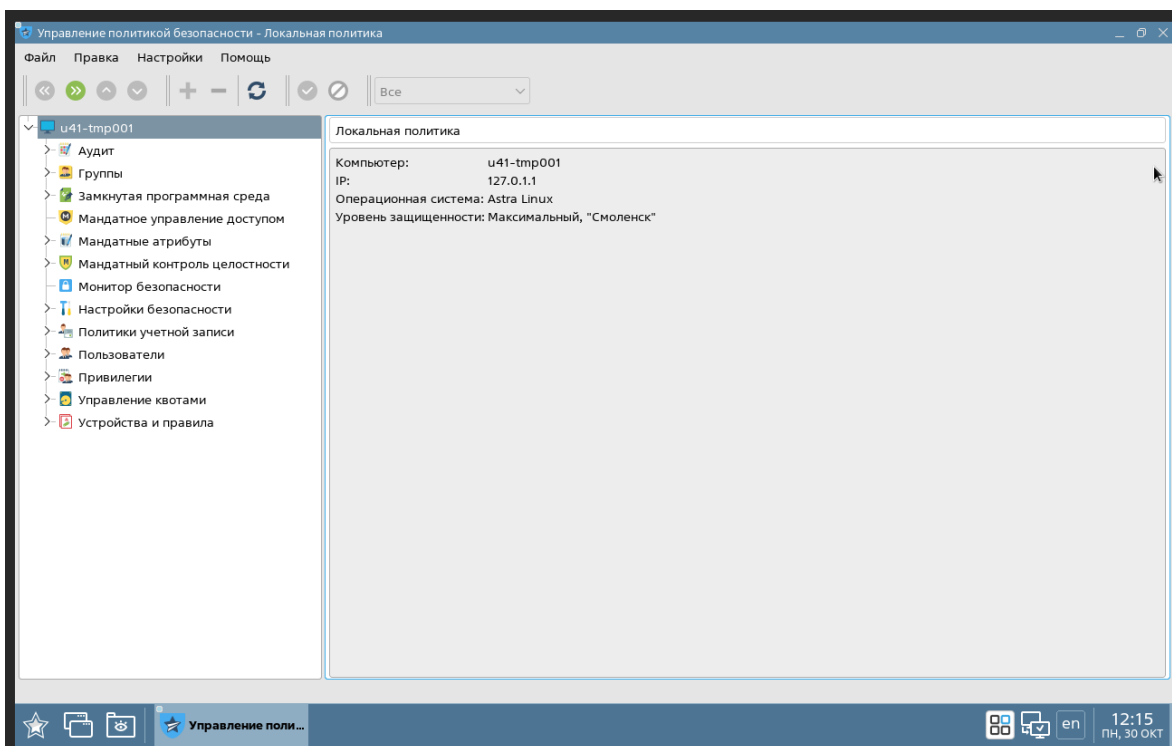


Рисунок 4 – Окно «Управление политикой безопасности – Локальная политика»

4) Перейти в раздел «Замкнутая программная среда» (рис. 5).

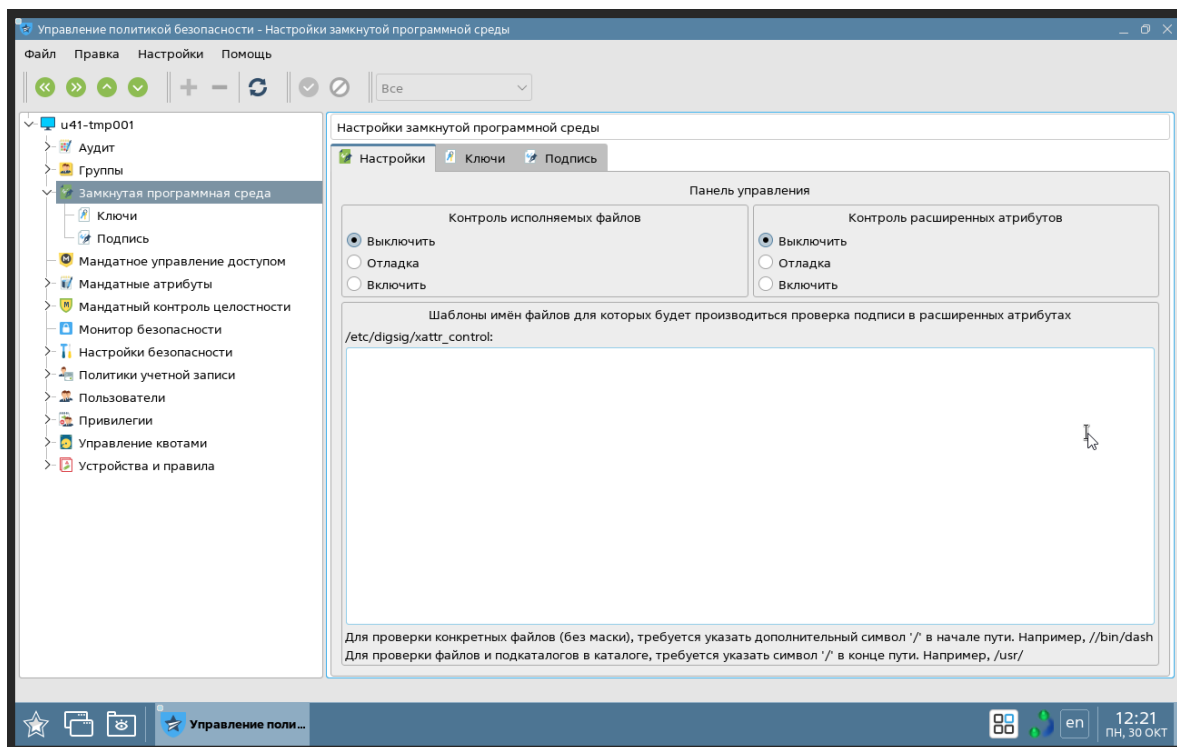


Рисунок 5 – Раздел «Замкнутая программная среда»

По умолчанию функции контроля исполняемых файлов и контроля расширенных атрибутов выключены. Необходимо либо оставить режим «Выключить», либо выбрать режим «Отладка». При использовании режима «Отладка» система будет выводить предупреждения о неподписанных файлах, но запуск их будет разрешен.

Аналогичную настройку можно произвести редактированием конфигурационного файла /etc/digsig/digsig_initramfs.conf:

- для использования отладочного режима для тестирования специального программного обеспечения необходимо установить параметр DIGSIG_ELF_MODE значение 2: DIGSIG_ELF_MODE=2.

5) Перейти в раздел «Мандатное управление доступом» (рис. 6).

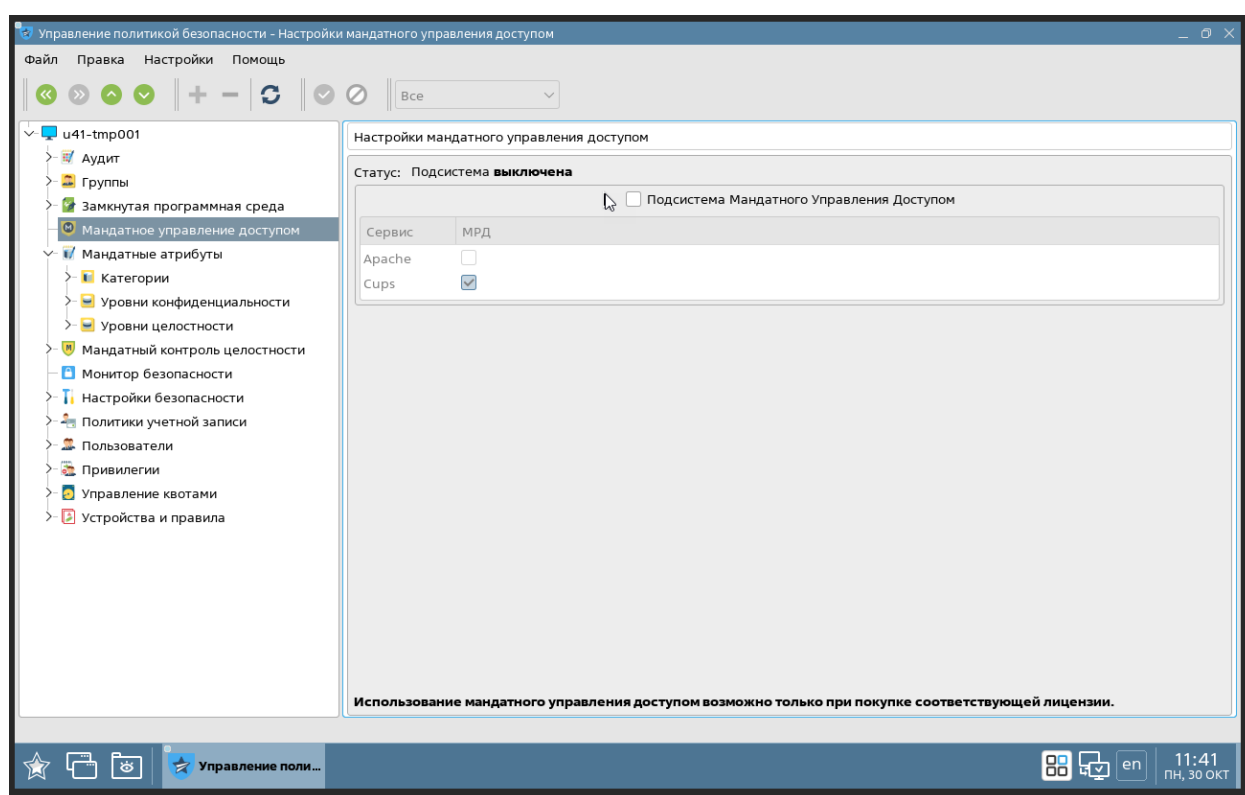


Рисунок 6 – Раздел «Мандатное управление доступом»

Установить флаг напротив поля «Подсистема Мандатного Управления Доступом».

i После активации механизма потребуются перезагрузка системы.

- 6) После активации подсистемы мандатного управления доступом, разблокируется доступ к мандатным атрибутам. В данном разделе изменять настройки не требуется.
- 7) Повторить шаг 1.
- 8) Перейти в раздел «Мандатный контроль целостности» (рис. 7).

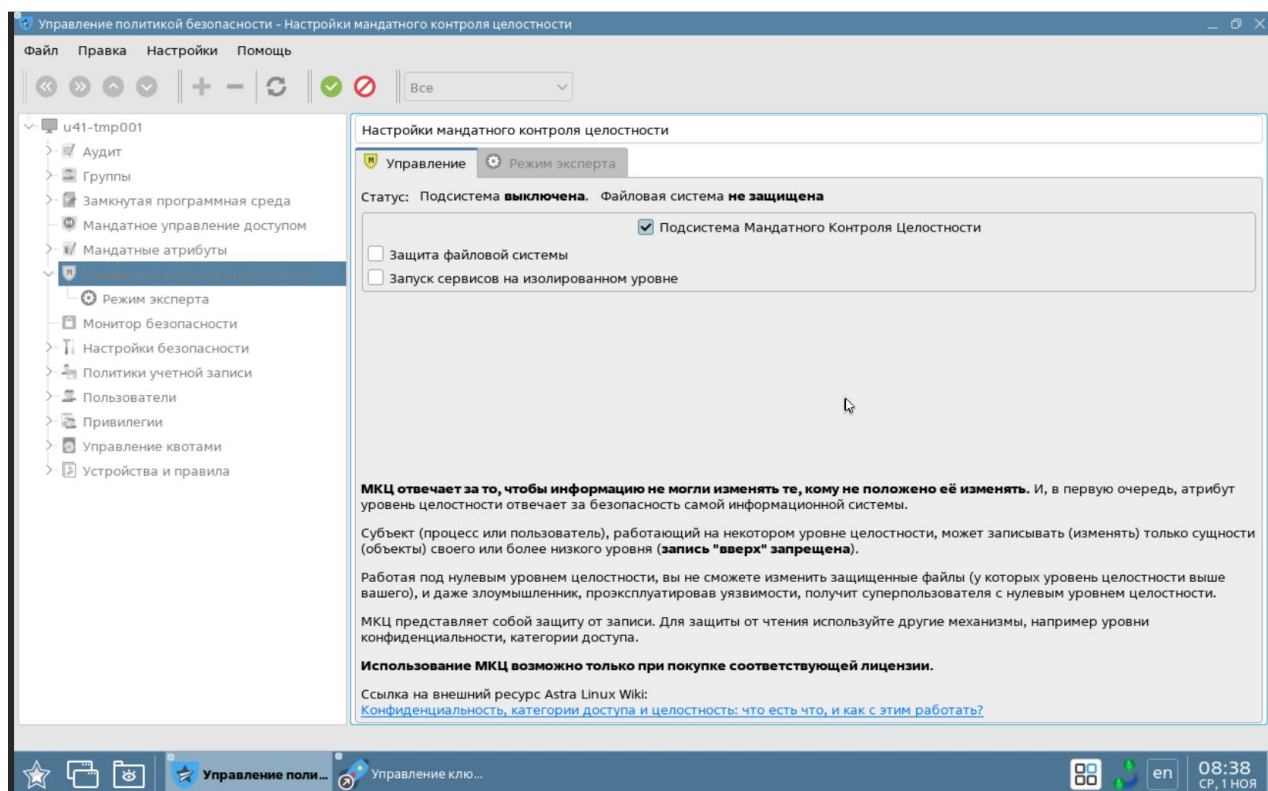


Рисунок 7 – Раздел «Мандатный контроль целостности»

По умолчанию функция «Подсистема Мандатного Контроля Целостности» выключена. Установить флаг в поле «Подсистема Мандатного Контроля Целостности».

- ❗ После активации функции потребуется перезагрузка системы.
- ❗ При повторной авторизации необходимо выбрать в поле «Уровень целостности» значение «Высокий» (рис. 8)

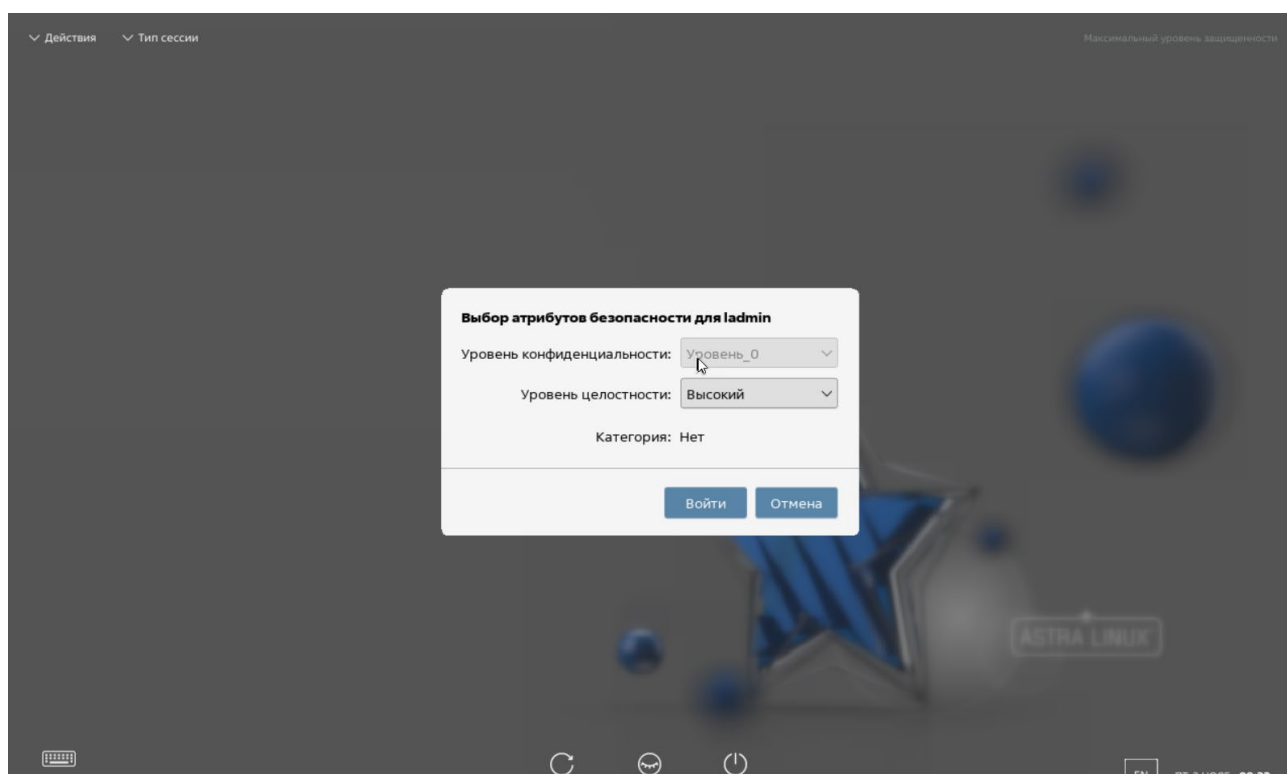


Рисунок 8 – Повторная авторизация

9) Повторить шаг 1.

10) Перейти в подраздел «Политика очистки памяти». Функция «Очистка разделов подкачки» должна быть выключена.

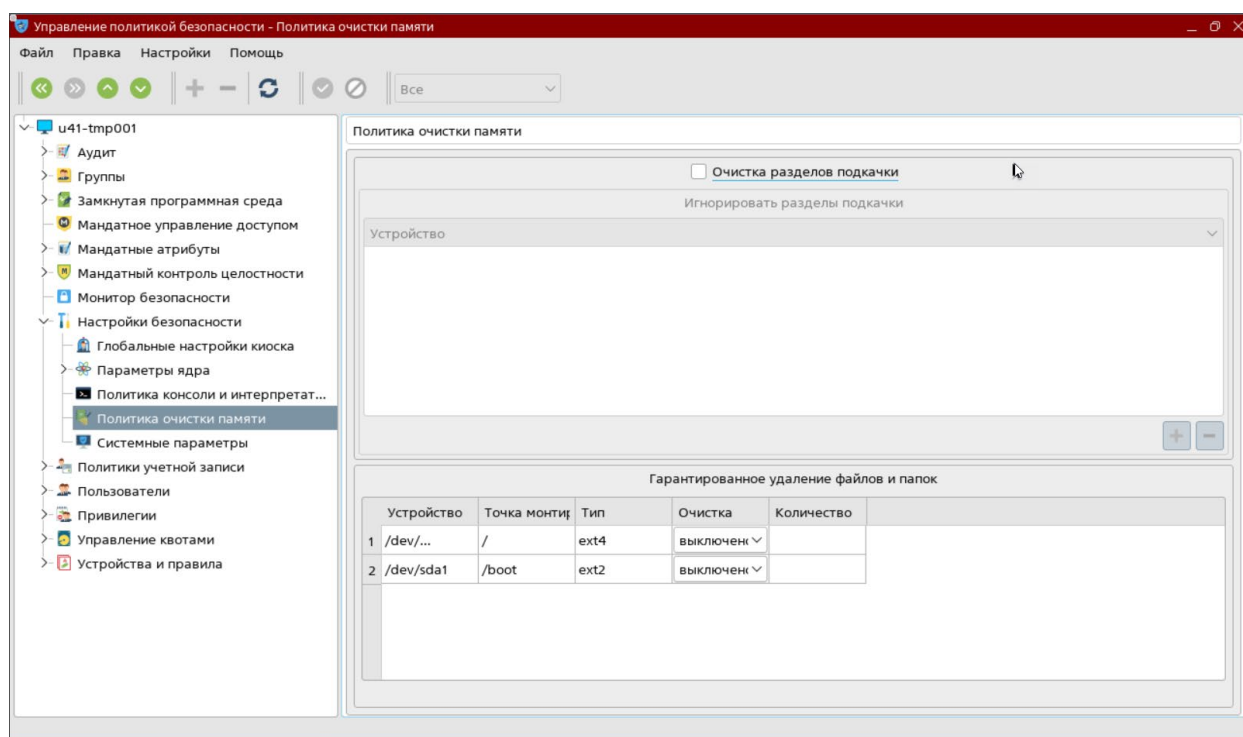


Рисунок 9 – Подраздел «Политика очистки памяти»

11) Перейти в подраздел «Системные параметры» (рис. 10).

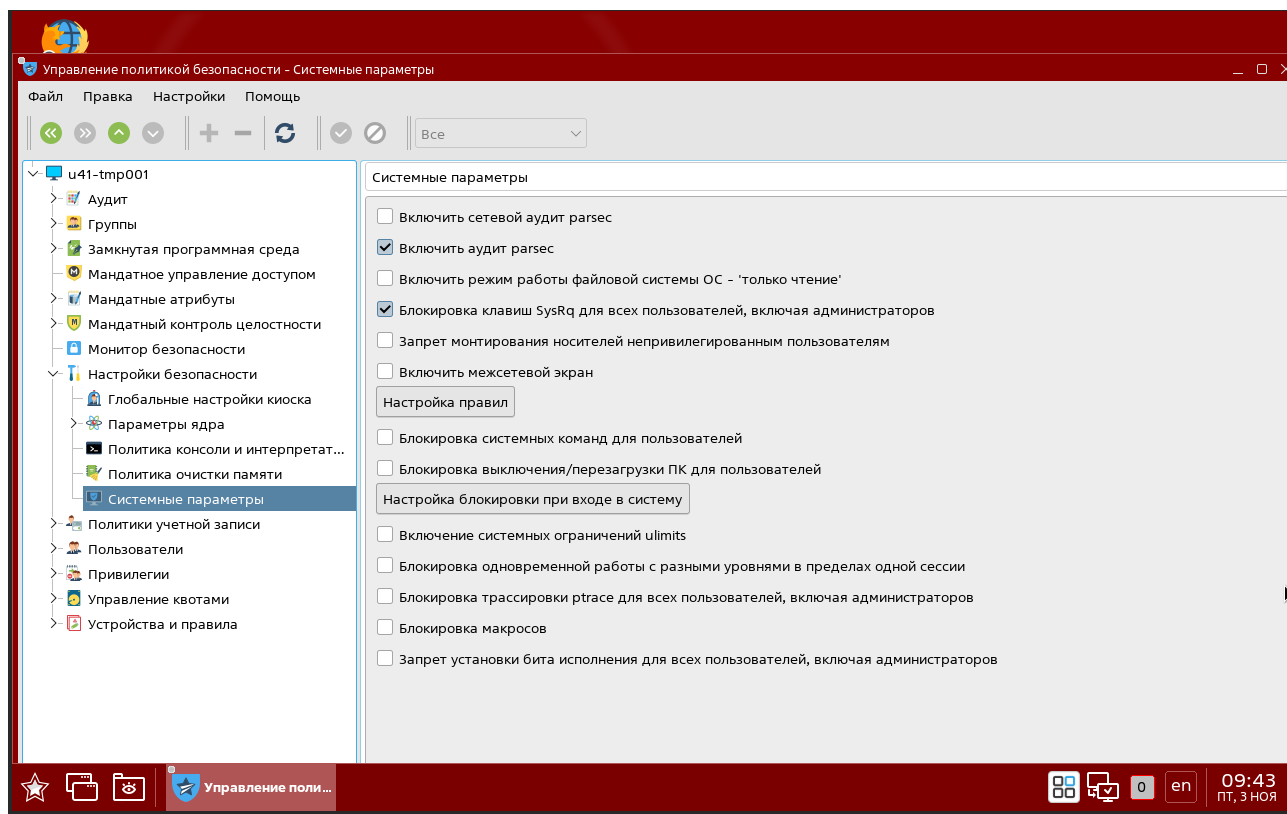


Рисунок 10 – Раздел «Настройки безопасности»

Установить флаги в следующих полях:

- «Включить аудит parsec»;
- «Блокировка клавиш Sysq для всех пользователей, включая администратора».

12) Перейти в подраздел «Политики консоли и интерпретаторов» (рис. 11).

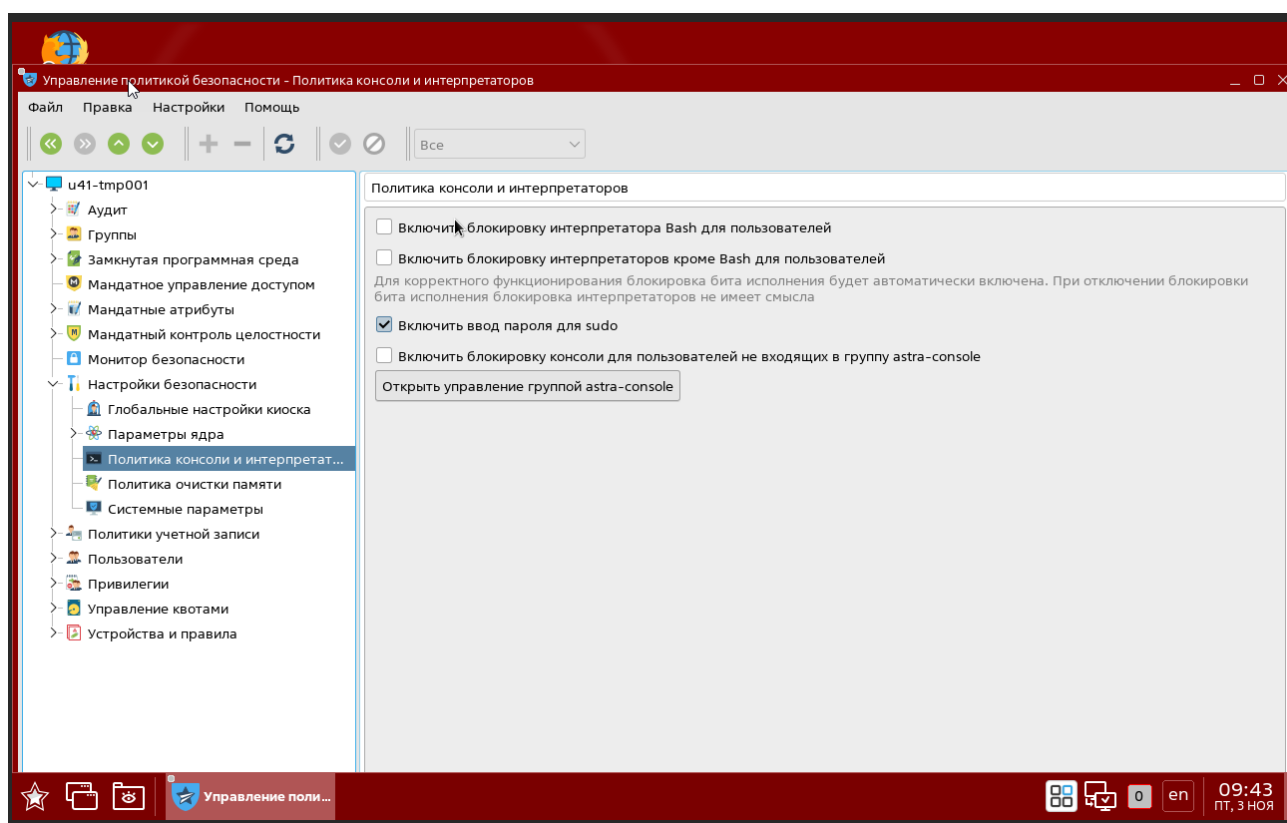


Рисунок 11 – Подраздел «Политики консоли и интерпретаторов»


Необходимо поставить флаг в поле «Включить ввод пароля для sudo».

13) Настройка политик безопасности для ОС Astra Linux SE завершена.

3.2.2 Установка ПК «Efros DO»

Для установки ПК «Efros DO» необходимо скопировать на ЭВМ в домашнюю директорию архив и скрипт, входящие в комплект поставки в соответствии с таблицей 2.

Существует два способа установки комплекса – с использованием встроенной СУБД (по умолчанию), или с подключением к внешней. Для установки комплекса необходимо выполнить следующие действия:

 Команды необходимо вводить от имени суперпользователя **root**, либо используя команду **sudo**.

- 1) Для установки комплекса со встроенной БД (например, СУБД PostgreSQL) – запустить скрипт **deploy.sh** без дополнительных аргументов, с правами администратора (рис. 12).


```
[root@u41ft79 edo-distr]# sudo ./deploy.sh
```

Рисунок 12 – Запуск скрипта

- 2) Для установки с подключением к внешней БД (например, СУБД «Jatoba») необходимо запустить скрипт с аргументом **--dbfree** (рис. 13).

```
[root@u41ft79 edo-distr]# sudo ./deploy.sh --dbfree
```

Рисунок 13 – Запуск скрипта

Запуск скрипта инициирует следующие процессы:

- проверка на наличие старых версий ПК «Efros DO», и, при наличии, удаление;
- распаковка файлов;
- запуск процесса установки и запуска ПК «Efros DO».

- 3) Если выбран вариант установки с подключением к внешней СУБД, то в процессе установки пользователю необходимо указать следующие параметры:

- IP-адрес сервера СУБД (в формате 192.168.1.1);
- порт для подключения к серверу СУБД (в формате 5432);
- учетная запись для подключения к БД;
- пароль для подключения к БД.

```
[INFO] Первый запуск Efros Defence Operations с использованием внешней СУБД
[INFO] Необходимо настроить параметры для подключения к внешней СУБД
Введите IP адрес сервера СУБД: 192.168.1.1
Введите порт: 5432
Введите логин: db_user
Введите пароль: 
```

Рисунок 14 – Процесс установки

- ! В момент установки комплекса, внешний сервер СУБД должен быть уже доступен по указанным параметрам.

- 4) В процессе установки скрипт запросит данные для настройки внутренней сети docker, в формате <адрес>/<маска>. При нажатии на клавишу «Enter» автоматически выбирается следующая сеть: 172.16.0.1/16 (рис. 15). Если данная сеть занята, то необходимо ввести пользовательские параметры сети.

```
[INFO] Первый запуск Efros Defence Operations
Введите сеть для docker, по умолчанию "172.16.0.1/16": 10.20.0.0/16
```

Рисунок 15 – Процесс установки

5) Установка программного комплекса завершена (рис. 16).

```
[+] Running 32/32
# Network edo_default Created
# Volume "edo_data-raddb4" Created
# Volume "edo_data-dict" Created
# Volume "edo_data-raddb" Created
# Volume "edo_data-kafka" Created
# Volume "edo_data-dict4" Created
# Container edo-infr-zookeeper Started
# Container edo-store-opensearch Started
# Container edo-proxy-service Started
# Container edo-ci-service Started
# Container edo-infr-kafka Started
# Container edo-email-sender-service Started
# Container edo-schedule-service Started
# Container edo-flow-collector-dhcp Started
# Container edo-guest-portal-service Started
# Container edo-identity-service Started
# Container edo-vulnerability-collector Started
# Container edo-acis-service Started
# Container edo-flow-collector-sflow Started
# Container edo-report-portal-service Started
# Container edo-knowledge-base-service Started
# Container edo-flow-service Started
# Container edo-task-portal-service Started
# Container edo-metrics-collector Started
# Container edo-flow-collector Started
# Container edo-tacacs Started
# Container edo-radius Started
# Container edo-license-service Started
# Container edo-metrics-service Started
# Container edo-so-service Started
# Container edo-web-service Started
# Container edo-gateway-service Started
[INFO] Инициализация завершена. Docker Даemon настроен. Efros-DO запущен.
[INFO] Первый запуск Efros Defence Operations завершен.
```

Рисунок 16 – Установка завершена

Для различных действий с приложением используется shell-скрипт **/opt/efros-do/edoctl**. Он запускается с аргументами командной строки (если запуск производится не с правами root, то необходима команда sudo):

- **./edoctl --ps** – просмотр запущенных сервисов (рис. 17);
- **./edoctl --stop** – остановка всех сервисов (рис. 18);
- **./edoctl --start** – запуск всех сервисов;
- **./edoctl --restart** – перезапуск сервисов (рис. 19);
- **./edoctl --down** – остановка служб приложения, удаление контейнеров;
- **./efros-do --logs <имя-службы>** – просмотр логов docker одной службы (если задано имя службы) либо всего приложения.

```
root@u41ft63:/opt/efros-do# ./edoctl --ps
```

NAME	COMMAND	SERVICE	STATUS	PORTS
edo-acs-service	"/bin/bash -c 'efros'"	edo-acs-service	running (unhealthy)	5000-5001/tcp
edo-ci-service	"/bin/bash -c 'efros'"	edo-ci-service	running (starting)	0.0.0.0:162→162/udp, 0.0.0.0:514→514/udp, 0.0.0.0:1468→1468/tcp, 0.0.0.0:20002→20002/tcp
edo-email-sender-service	"/usr/bin/EmailSenderSer..."	edo-email-sender-service	running (healthy)	80/tcp
edo-flow-collector	"/usr/bin/flow-collector..."	edo-flow-collector	running	
edo-flow-collector-dhcp	"/usr/bin/flow-collector-dhcp..."	edo-flow-collector-dhcp	running	0.0.0.0:67→67/udp
edo-flow-collector-sflow	"/usr/bin/flow-collector-sflow..."	edo-flow-collector-sflow	running	
edo-flow-service	"/bin/bash -c 'while..."	edo-flow-service	running (unhealthy)	80/tcp
edo-gateway-service	"/usr/bin/VoltronGateway.W..."	edo-gateway-service	running (healthy)	80/tcp
edo-guest-portal-service	"/usr/bin/VoltronGuestPortal..."	edo-guest-portal-service	running	5803/tcp
edo-identity-service	"/usr/bin/Identity.Api"	edo-identity-service	running (healthy)	80/tcp
edo-infr-kafka	"/etc/confluent/docker..."	edo-infr-kafka	running (healthy)	9092/tcp
edo-infr-zookeeper	"/etc/confluent/docker..."	edo-infr-zookeeper	running (healthy)	3888/tcp
edo-knowledge-base-service	"/usr/bin/KnowledgeBaseServ..."	edo-knowledge-base-service	running (healthy)	80/tcp
edo-license-service	"/usr/bin/License.Api"	edo-license-service	running (healthy)	80/tcp
edo-metrics-collector	"/usr/bin/EventsCollector..."	edo-metrics-collector	running	80/tcp
edo-metrics-service	"/usr/bin/AnalyticsMetrics..."	edo-metrics-service	running	80/tcp
edo-proxy-service	"/usr/bin/Proxy.Service"	edo-proxy-service	running (healthy)	0.0.0.0:443→443/tcp, 0.0.0.0:5802→5802/tcp
edo-radius	"/usr/bin/systemd/systemd..."	edo-radius	running (unhealthy)	0.0.0.0:1812-1813→1812-1813/udp
edo-report-portal-service	"/usr/bin/Reporting.WebApi"	edo-report-portal-service	running (healthy)	80/tcp
edo-schedule-service	"/usr/bin/Voltron.Schedule..."	edo-schedule-service	running (healthy)	80/tcp
edo-so-service	"/usr/bin/SecurityObject..."	edo-so-service	running (healthy)	80/tcp
edo-store-opensearch	"/usr/bin/opensearch-docker..."	edo-store-opensearch	running (healthy)	127.0.0.1:5805→9200/tcp
edo-tacacs	"/usr/bin/systemd/systemd..."	edo-tacacs	running	0.0.0.0:49→49/tcp
edo-task-portal-service	"/usr/bin/TaskPortal.WebApi"	edo-task-portal-service	running (unhealthy)	80/tcp
edo-vulnerability-collector	"/usr/bin/VulnerabilityS..."	edo-vulnerability-collector	running (healthy)	80/tcp
edo-web-service	"/usr/bin/Voltron.WebApi"	edo-web-service	running (healthy)	80/tcp

```
root@u41ft63:/opt/efros-do#
```

Рисунок 17 – Просмотр запущенных сервисов

```
root@u41ft63:/opt/efros-do# ./edoctl --stop
```

[+] Running 3/16		
Container edo-tacacs	Stopping	3.2s
Container edo-flow-collector-dhcp	Stopped	2.7s
Container edo-email-sender-service	Stopping	3.2s
Container edo-vulnerability-collector	Stopping	3.2s
Container edo-ci-service	Stopping	3.2s
Container edo-gateway-service	Stopping	3.2s
Container edo-knowledge-base-service	Stopping	3.1s
Container edo-guest-portal-service	Stopping	3.1s
Container edo-report-portal-service	Stopping	3.1s
Container edo-task-portal-service	Stopping	3.1s
Container edo-flow-collector-sflow	Stopped	1.4s
Container edo-metrics-collector	Stopping	3.1s
Container edo-schedule-service	Stopping	3.1s
Container edo-radius	Stopping	3.1s
Container edo-flow-collector	Stopped	1.4s
Container edo-proxy-service	Stopping	3.1s

Рисунок 18 – Остановка всех сервисов

```
root@u41ft63:/opt/efros-do# ./edoctl --restart
```

[+] Running 9/22		
Container edo-proxy-service	Started	0.7s
Container edo-store-opensearch	Started	0.9s
Container edo-infr-zookeeper	Started	1.0s
Container edo-ci-service	Started	0.6s
Container edo-infr-kafka	Started	0.5s
Container edo-flow-collector-dhcp	Started	1.4s
Container edo-task-portal-service	Restarting	2.5s
Container edo-acs-service	Restarting	2.5s
Container edo-identity-service	Started	1.3s
Container edo-report-portal-service	Restarting	2.5s
Container edo-flow-service	Restarting	2.5s
Container edo-metrics-collector	Restarting	2.5s
Container edo-vulnerability-collector	Restarting	2.5s
Container edo-knowledge-base-service	Restarting	2.5s
Container edo-schedule-service	Restarting	2.5s
Container edo-guest-portal-service	Restarting	2.5s
Container edo-flow-collector-sflow	Started	0.4s
Container edo-email-sender-service	Started	2.3s
Container edo-license-service	Restarting	1.3s
Container edo-web-service	Restarting	1.3s
Container edo-so-service	Restarting	1.3s
Container edo-metrics-service	Restarting	1.3s

Рисунок 19 – Перезапуск всех сервисов

- 6) После установки доступен просмотр списка запущенных сервисов и их параметров.
- 7) Для настройки комплекса необходимо открыть браузер и ввести IP-адрес сервера, на котором производилась установка. При возникновении предупреждения о ненадежности сертификата безопасности необходимо продолжить открытие веб-сайта, после чего отобразится интерфейс комплекса. Пользователю необходимо выполнить ряд действий:
 - активировать комплекс в соответствии с п. 3.3 руководства;
 - настроить ПК «Efros DO» в соответствии с руководством пользователя.

3.3 Перенастройка сети

Настройка сетевого интерфейса `docker0` и подсети, в которой работают контейнеры комплекса, осуществляется следующим образом:

- 1) Перейти **`cd/opt/efros-do`**.
- 2) Выполнить остановку контейнеров **`./edoctl -down`**.
- 3) Удалить неиспользуемые сети **`docker network prune -f`**.
- 4) Изменить сеть в конфигурации **`./edoctl -init`**.
- 5) Ввести пользовательские параметры сети в формате «10.0.0.0/16» или оставить по умолчанию.

3.4 Лицензирование

После установки и настройки ПК «Efros DO» в БД комплекса автоматически создается учетная запись пользователя с ролью «GlobalAdministrator»: с логином «SuperAdmin» и паролем «\$Qwerty123456». При первом запуске ПК «Efros DO» для такого пользователя открывается окно смены пароля (рис. 20), в котором необходимо указать в качестве старого пароля значение «\$Qwerty123456», дважды указать новый пароль и нажать кнопку «Сменить пароль».

**Смена текущего пароля**

Для входа в систему необходимо задать новый пароль

Новый пароль

 Пароль

Подтверждение пароля

 Пароль

Сменить пароль

Отменить

Русский
Версия 2.5.67.0.20230525.2.dev



Рисунок 20 – Окно смены пароля

Будет выполнена автоматическая проверка соответствия пароля заданной в комплексе сложности. По умолчанию пароль должен:

- быть не менее 8 символов;
- содержать хотя бы одну цифру;
- содержать хотя бы одну латинскую букву верхнего регистра;
- содержать хотя бы одну латинскую букву нижнего регистра;
- содержать хотя бы один специальный символ;
- отличаться от предыдущего пароля хотя бы на 3 символа;
- не совпадать с предыдущими тремя паролями пользователя.

При возникновении ошибки в ходе смены пароля в верхней части страницы авторизации отобразится соответствующее сообщение об ошибке.

После успешной смены пароля вновь откроется страница авторизации. Для доступа к веб-приложению ПК «Efros DO» администратору необходимо выполнить повторную авторизацию в комплексе с новым паролем. Для проведения активации комплекса необходимо перейти в раздел «Администрирование», подраздел «Лицензия» (рис. 21).

Возможны два варианта проведения активации комплекса:

- online активация – при наличии подключения к серверу лицензирования;
- offline активация – при отсутствии подключения к серверу лицензирования.

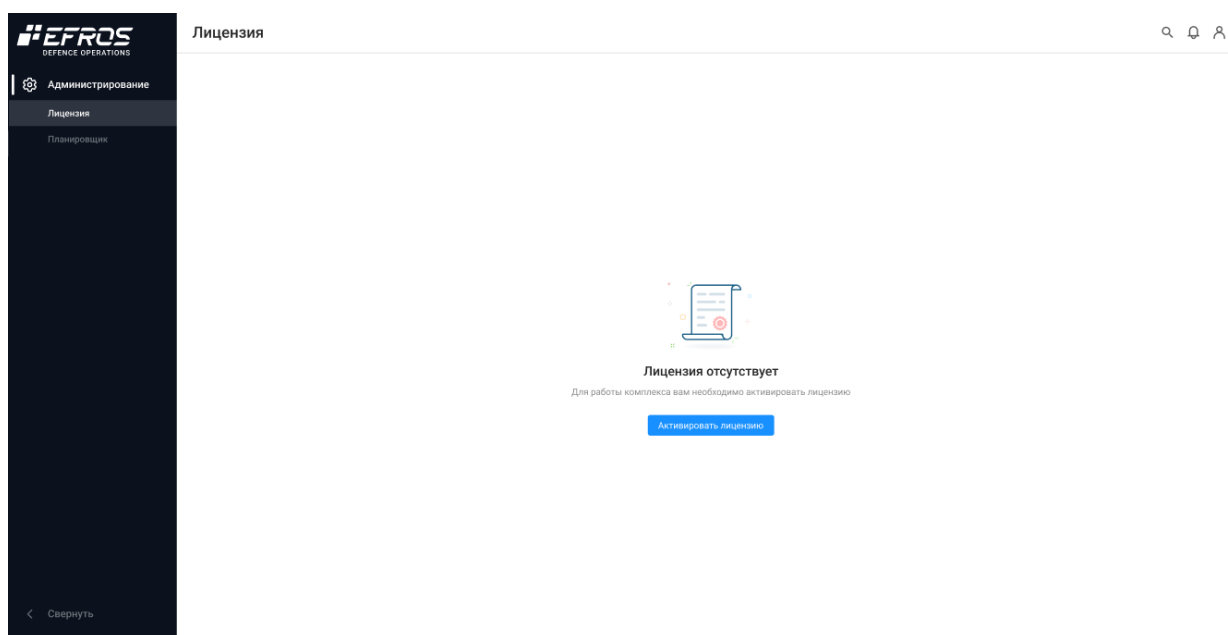


Рисунок 21 – Подраздел «Лицензия»

3.4.1 Online активация комплекса

Online активация комплекса осуществляется при наличии подключения к сети Internet и возможности подключения к серверу лицензирования ООО «Газинформсервис».

Для активации ПК «Efros DO» необходимо нажать на кнопку «Активировать лицензию» (рис. 21). При подключении к сети Internet и к серверу лицензирования ООО «Газинформсервис» появится диалоговое окно (рис. 22):

- 1) В диалоговом окне (рис. 22) необходимо указать ключ лицензии, полученный при покупке комплекса.

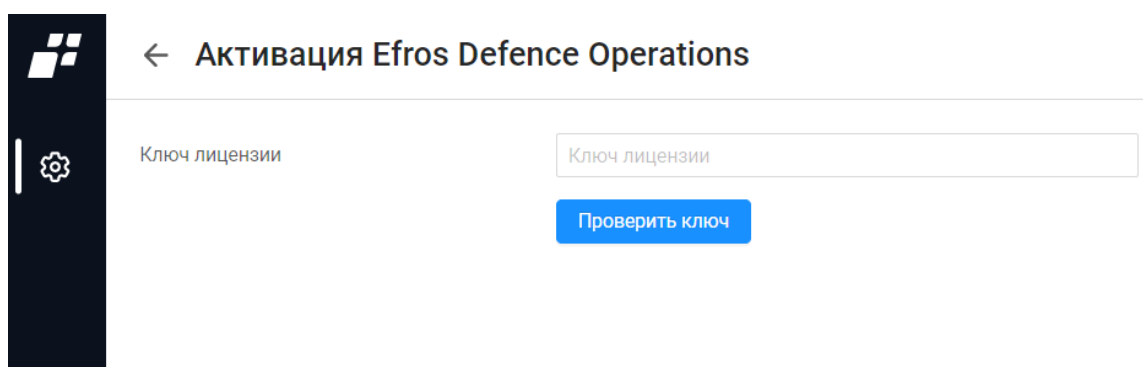
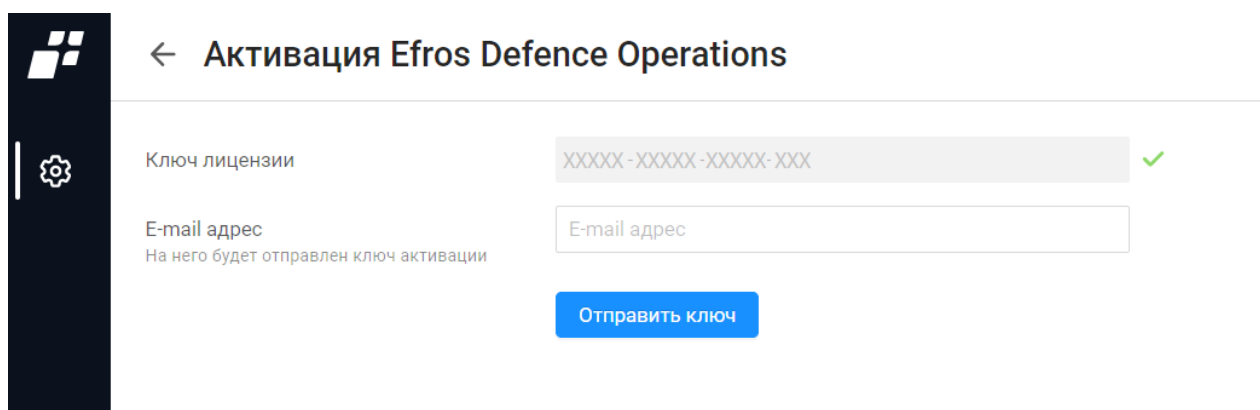


Рисунок 22 – Окно online активации комплекса. Проверка ключа

- 2) Нажать кнопку «Проверить ключ». При успешной проверке напротив ключа лицензии появится галочка « ✓ ».
- 3) Далее указать данные (электронную почту) для получения ключа активации лицензии (рис. 23).



← Активация Efros Defence Operations

Ключ лицензии XXXXX-XXXXX-XXXXX-XXX ✓

E-mail адрес
На него будет отправлен ключ активации

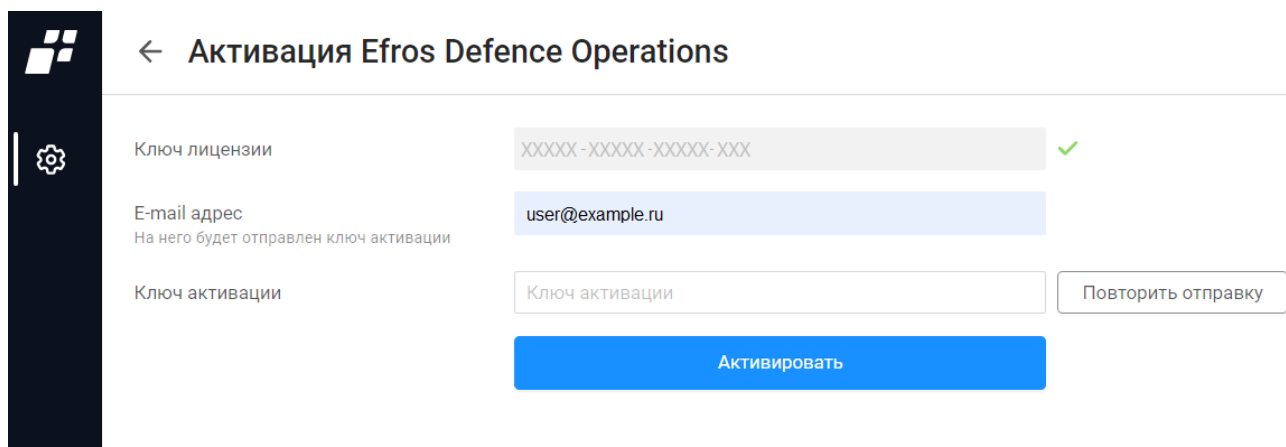
Отправить ключ

Рисунок 23 – Окно online активации комплекса. Отправка ключа

- 4) Затем нажать кнопку «Отправить ключ». На указанный адрес электронной почты придет письмо с ключом для активации продукта.

! Активацию комплекса необходимо провести в течение 20 минут после формирования запроса на активацию.

- 5) Ввести ключ активации в соответствующее поле (рис. 24) и нажать кнопку «Активировать». Если ключ не был использован спустя 20 минут, необходимо нажать кнопку «Повторить отправку». На указанную почту придет новое письмо с новым ключом активации лицензии.



← Активация Efros Defence Operations

Ключ лицензии XXXXX-XXXXX-XXXXX-XXX ✓

E-mail адрес
На него будет отправлен ключ активации user@example.ru

Ключ активации Ключ активации

Активировать Повторить отправку

Рисунок 24 – Указание необходимых данных для активации

Активация комплекса завершена (рис. 25), на электронный адрес будет отправлен архив **license.zip** с файлом лицензии **license.bin**. Данный файл в дальнейшем можно использовать для переноса лицензии.

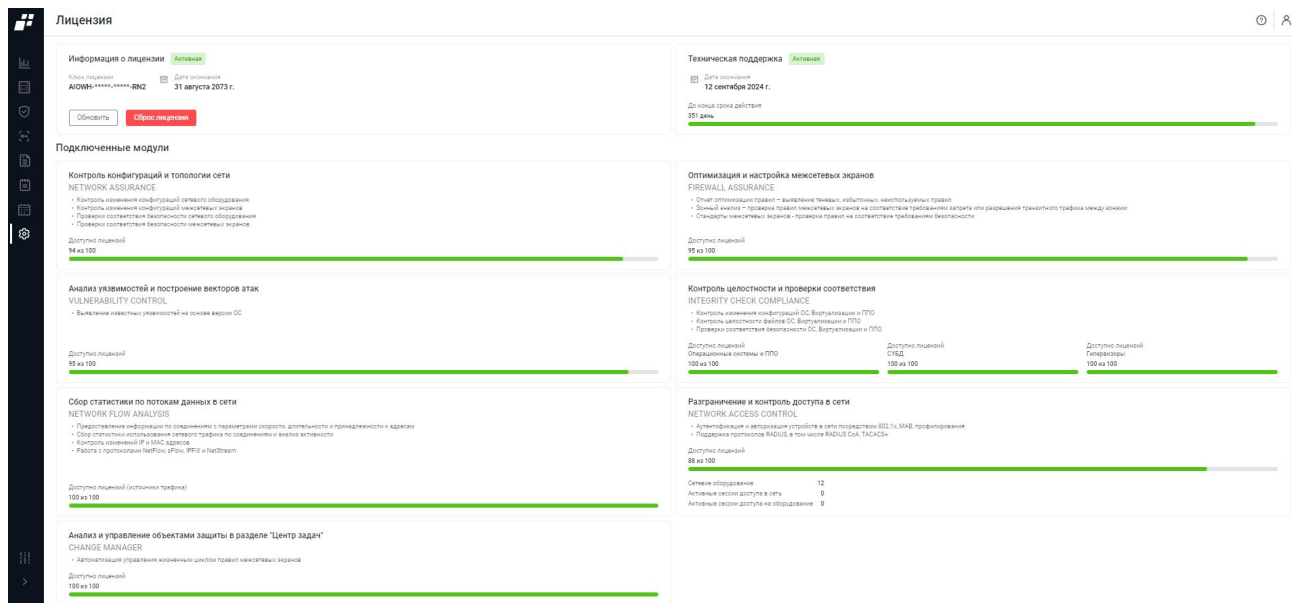


Рисунок 25 – Активация комплекса завершена

3.4.2 Offline активация комплекса

Проведение offline активации осуществляется при отсутствии подключения к сети Internet либо если связь с сервером лицензирования ООО «Газинформсервис» не установлена. В таком случае, при нажатии кнопки «Активировать лицензию», появится соответствующее окно (рис. 26).

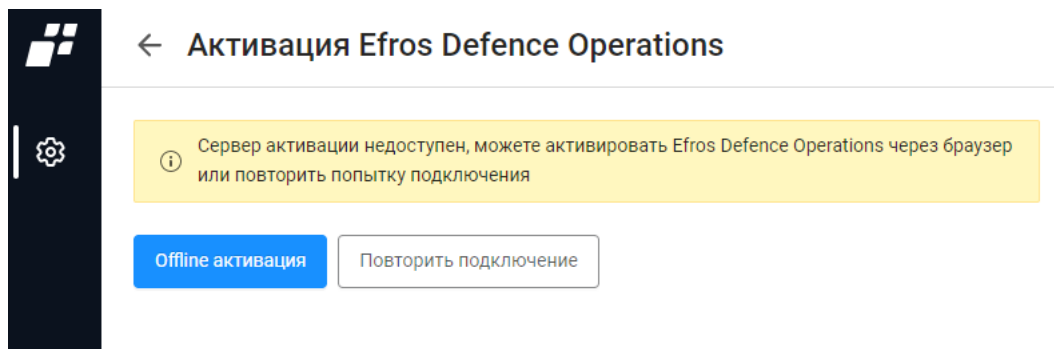
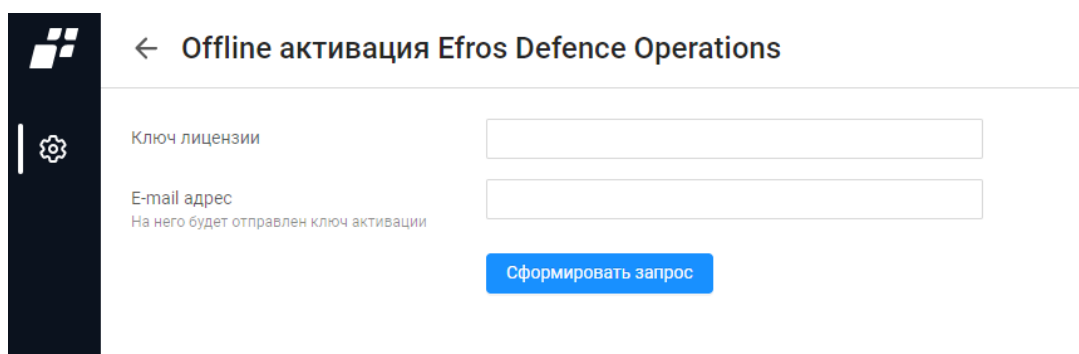


Рисунок 26 – Окно активации

При нажатии кнопки «Offline активация», откроется окно для проведения offline активации программного комплекса (рис. 27).



← Offline активация Efros Defence Operations

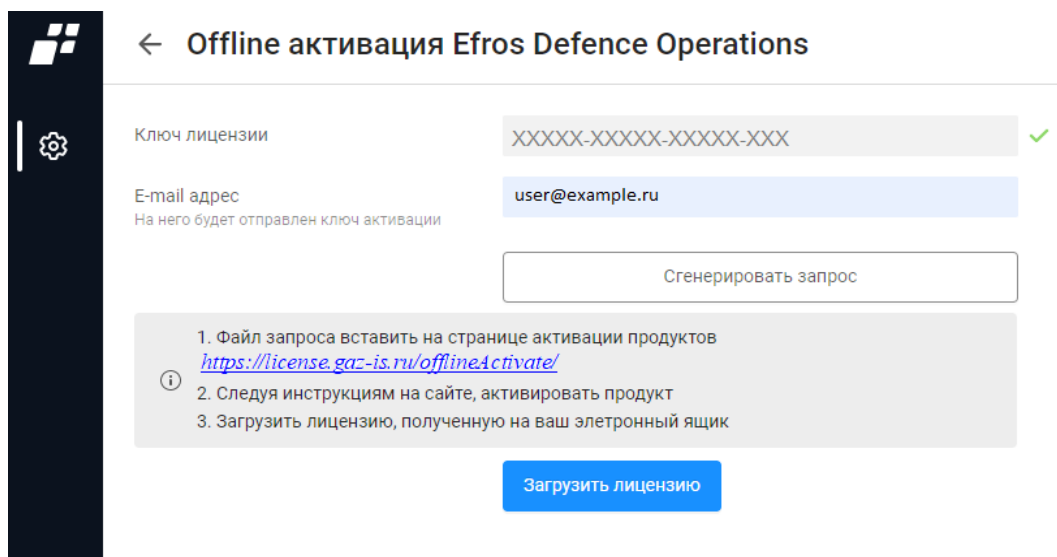
Ключ лицензии

E-mail адрес
На него будет отправлен ключ активации

Сформировать запрос

Рисунок 27 – Проведение offline активации

В данном диалоговом окне необходимо указать ключ активации, адрес электронной почты и нажать кнопку «Сформировать запрос». В результате будет сформирован файл с запросом на лицензию формата .json – **request.json** (рис. 28).



← Offline активация Efros Defence Operations

Ключ лицензии XXXXXX-XXXXXX-XXXXXX-XXXX ✓

E-mail адрес
На него будет отправлен ключ активации user@example.ru

Сгенерировать запрос

1. Файл запроса вставить на странице активации продуктов
<https://license.gaz-is.ru/offlineActivate/>
2. Следуя инструкциям на сайте, активировать продукт
3. Загрузить лицензию, полученную на ваш элктронный ящик

Загрузить лицензию

Рисунок 28 – Проведение offline активации

Необходимо перейти на другую ЭВМ с устойчивым подключением к сети Internet, открыть браузер и указать адрес для проведения offline активации продукта: <https://license.gaz-is.ru/offlineActivate/> (рис. 29).

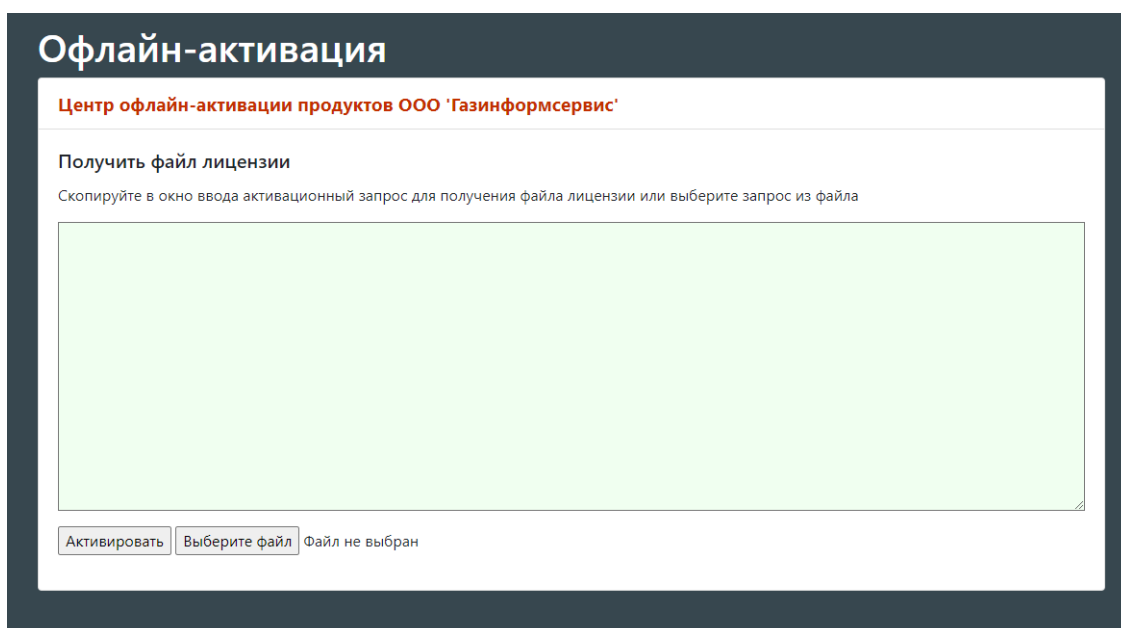


Рисунок 29 – Центр активации продуктов

Открыть ранее сгенерированный файл **request.json** и скопировать содержимое файла в соответствующее окно (рис. 29) либо воспользоваться кнопкой «Выберите файл», затем нажать кнопку «Активировать». Будет отправлено письмо на электронную почту, указанную для запроса, с ключом активации (рис. 30).

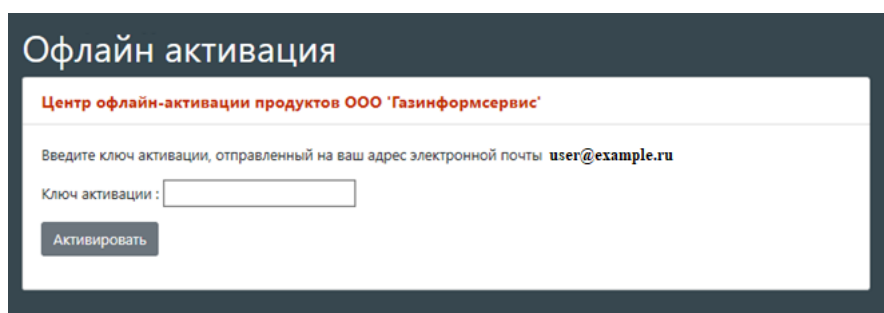


Рисунок 30 – Окно для ввода ключа активации

Указать полученный ключ активации и нажать кнопку «Активировать». В случае успешного прохождения активации на электронный адрес будет отправлено письмо с архивом **license.zip**, в котором содержится файл **license.bin** и появится соответствующее информационное сообщение в веб-браузере (рис. 31).

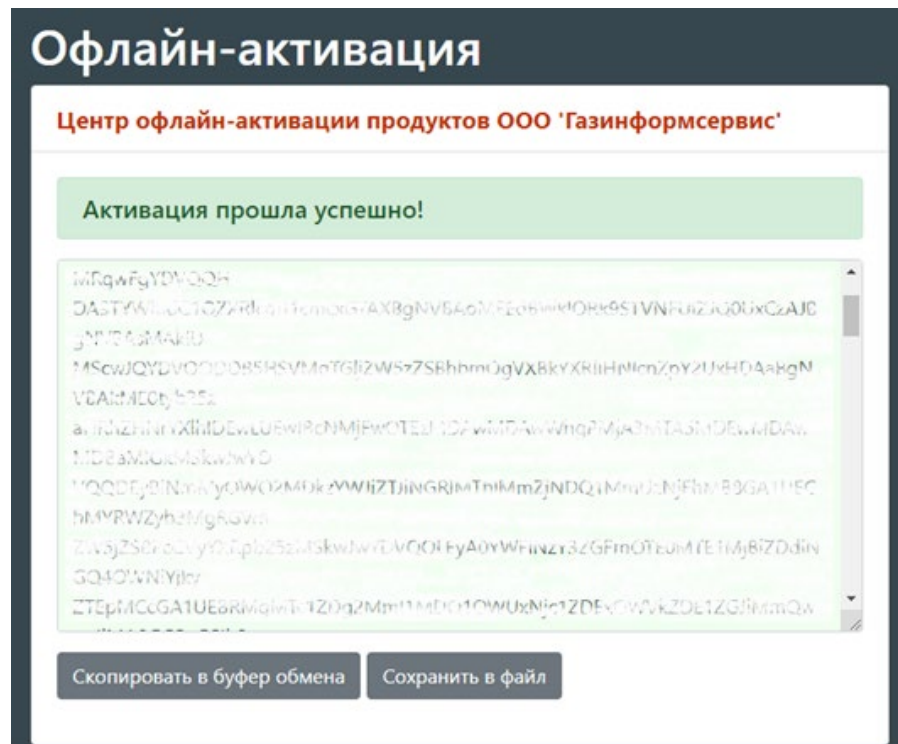


Рисунок 31 – Успешное прохождение активации

Перейти на ЭВМ, на которой необходимо активировать комплекс, и в окне offline активации (рис. 28) с помощью кнопки «Загрузить лицензию», загрузить полученный файл лицензии license.bin. Автоматически откроется вкладка с активированной лицензией. Offline активация комплекса завершена (рис. 32).

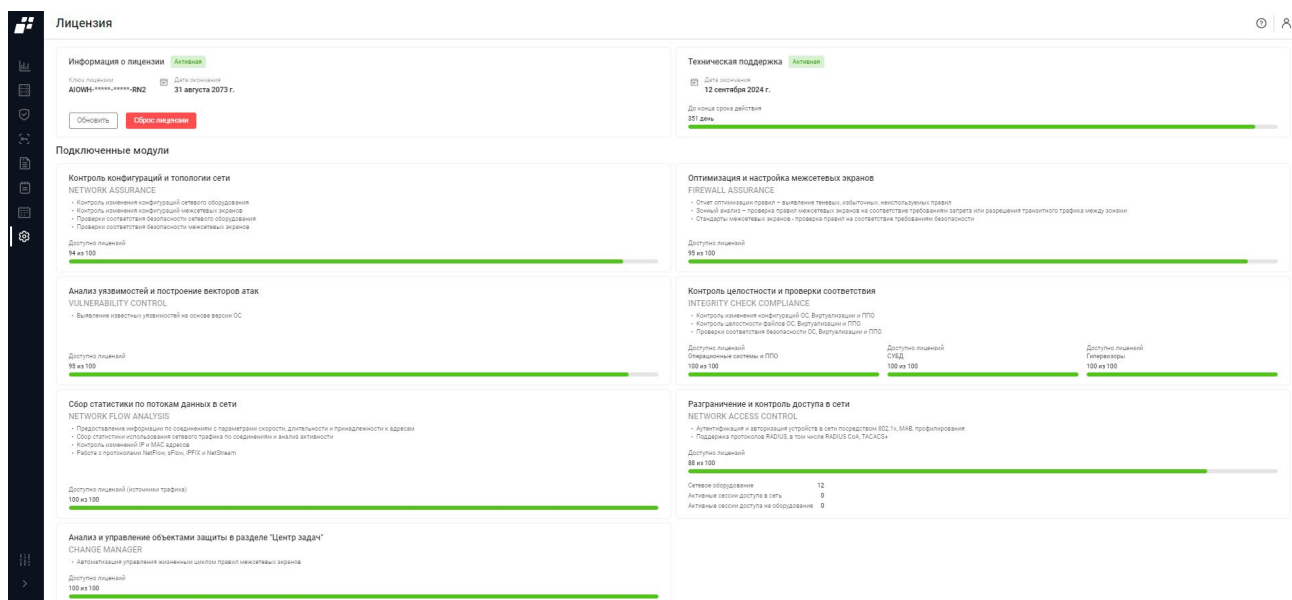



Рисунок 32 – Завершение прохождения активации

3.4.3 Реактивация лицензии комплекса

Для осуществления переноса лицензии необходимо после установки ПК на другой ЭВМ, перейти в диалоговое окно активации комплекса (Администрирование/Лицензия) и указать ключ лицензии, полученный при покупке комплекса. В таком случае, при нажатии кнопки «Активировать лицензию», появится соответствующее сообщение (рис. 33).

Активация Efros Defence Operations

 Данная лицензия была активирована ранее, вы можете ее реактивировать или ввести другой ключ. При реактивации лицензии, активированная ранее лицензия будет деактивирована.

Ключ лицензии

XXXXX - XXXXX - XXXXX - XXX

Реактивировать

Проверить снова

Рисунок 33 – Повторная активация лицензии

Для реактивации лицензии необходимо нажать кнопку «Реактивировать».


При наличии устойчивого подключения к сети Internet, дальнейшая активация комплекса осуществится online.

← Активация Efros Defence Operations

Ключ лицензии

XXXXX - XXXXX - XXXXX - XXX

✓

 Для реактивации необходимо приложить файл ранее активированной лицензии

Файл лицензии

license.bin

🔗

E-mail адрес

user@example.ru


На него будет отправлен ключ активации

Отправить ключ

Рисунок 34 – Ввод данных

При успешной проверке введенного ключа активации напротив поля появится галочка « ✓ ». Затем необходимо приложить файл **license.bin**, который был получен ранее при активации комплекса на другой ЭВМ.

Далее указать электронную почту и нажать «Отправить ключ» (рис. 34).

 Необходимо указать адрес электронной почты, который использовался при

прошлой активации комплекса. В случае, если адреса электронной почты не будут совпадать, появится сообщение «Для данного ключа уже задан e-mail. Для изменения свяжитесь с технической поддержкой».

На указанный адрес электронной почты будет отправлен ключ активации продукта. Активацию комплекса необходимо провести в течение 20 минут после формирования запроса на активацию (рис. 35).

← Активация Efros Defence Operations

Ключ лицензии XXXXX - XXXXX - XXXXX - XXX ✓

ⓘ Для реактивации необходимо приложить файл ранее активированной лицензии

Файл лицензии license.bin ↗

Е-mail адрес user@example.ru
На него будет отправлен ключ активации

Ключ активации XXX - XXX - XXX - XXX Повторить отправку

Ключ отправлен. Время действия ключа 19:55

Активировать

Рисунок 35 – Ввод ключа активации

Ввести ключ активации, полученный по электронной почте, в соответствующее поле (см. рис. 35) и нажать кнопку «Активировать». Перенос ключа активации лицензии завершен. Реактивация лицензии возможна также в offline режиме. Алгоритм действий аналогичен проведению offline активации комплекса (см. п.3.4.2).

3.5 Удаление изделия

Для удаления приложения необходимо выполнить команду ***apt-get remove efros-do*** (рис. 36).

```
administrator@efros-do:~$ sudo apt-get remove efros-do_
```

Рисунок 36 – Запуск команды для последующего удаления

```
Хотите продолжить? [Д/Н]
(Чтение баз данных ... На данный момент установлено 49290 файлов и каталогов.)
Удаляется efros-do (1.4.2) ...
Stopping edo-gateway-service ... done
Stopping edo-license-service ... done
Stopping edo-so-service ... done
Stopping edo-metrics-service ... done
Stopping edo-web-service ... done
Stopping edo-tacacs ... done
Stopping edo-radius ... done
Stopping edo-accs-service ... done
Stopping edo-identity-service ... done
Stopping edo-ci-service ... done
Stopping edo-flow-service ... done
Stopping edo-flow-collector-sflow ... done
Stopping edo-flow-collector ... done
Stopping edo-schedule-service ... done
Stopping edo-metrics-collector ... done
Stopping edo-store-postgres ... done
Stopping edo-infr-kafka ... done
Stopping edo-store-elasticsearch ... done
Stopping edo-infr-zookeeper ... done
Stopping edo-proxy-service ... done
Going to remove edo-gateway-service, edo-license-service, edo-so-service, edo-metrics-service, edo-web-service, edo-tacacs, edo-radius, edo-accs-service, edo-identity-service, edo-ci-service, edo-flow-service, edo-flow-collector-sflow, edo-flow-collector, edo-schedule-service, edo-metrics-collector, edo-store-postgres, edo-infr-kafka, edo-store-elasticsearch, edo-infr-zookeeper, edo-proxy-service
Removing edo-gateway-service ... done
Removing edo-license-service ... done
Removing edo-so-service ... done
Removing edo-metrics-service ... done
Removing edo-web-service ... done
Removing edo-tacacs ... done
Removing edo-radius ... done
Removing edo-accs-service ... done
Removing edo-identity-service ... done
Removing edo-ci-service ... done
Removing edo-flow-service ... done
Removing edo-flow-collector-sflow ... done
Removing edo-flow-collector ... done
Removing edo-schedule-service ... done
Removing edo-metrics-collector ... done
Removing edo-store-postgres ... done
Removing edo-infr-kafka ... done
Removing edo-store-elasticsearch ... done
Removing edo-infr-zookeeper ... done
Removing edo-proxy-service ... done
-
```

Рисунок 37 – Процесс удаления файлов и каталогов

```
Deleted: sha256:688f65ce3a33d5aae47eb089c6f608c4026364ddaba08f87f9f94b4c22b995dc
Deleted: sha256:291f6e4771a7b4399b0c6fb40ab4fe0331ddf76eda11080f052b003d96c7726
Untagged: edo-infr-kafka:5.5.0
Untagged: localhost:80/edo-infr-kafka:5.5.0
Untagged: localhost:80/edo-infr-kafka@sha256:ad865d13e75acc38a252a6641213d5b1f86cd1ce74a96c5a18ef64853f7fee2b
Deleted: sha256:7d3fff76bebeec000934e06652b732d8affe94a6770e7f603dc538da3e139472
Deleted: sha256:f642031e18cfbb570bff4d1a12665f8cea1e7601de8bf2f8335ce49bba2b5222
Deleted: sha256:91475761aec75919d22452098f684a34ee5c0244549bd85d7f343ad56833911c
Deleted: sha256:283dd1b3aa373ca8db49275d08c794ad8593809aaab4c1995df52e8bd6d1f4db
Deleted: sha256:2bf35c488a79e4d5fc62cf3b2241b7a7be7b2359aa6fb034333d1c8c1d144ed2
Untagged: edo-infr-zookeeper:5.5.0
Untagged: localhost:80/edo-infr-zookeeper:5.5.0
Untagged: localhost:80/edo-infr-zookeeper@sha256:6e33666a21ed552cf4a6b9096a2fa94c954a60c17ec470a20f0422b9cbaa6a26
Deleted: sha256:124ff6469e3d01eb72c58afa0668a5a19f7bf031835e98847a4b4e28fcddbea
Deleted: sha256:7c1b2a63d63d4e8a4bc26812347923d30df54e09fd069ba09633cdc590e6fd37
Deleted: sha256:cf7c6836cab0ee5a22bf97d37d3cc5ba22658f8248de66dbe9e045bbb3ed4fcb
Deleted: sha256:5ae1074330ca9e55e23f527aa4323f440379637b6ee79c815354a09609b4e2be
Deleted: sha256:d9ad8c636ab061323a045478cbb0b0aab95ed152d6b42e4d7696f658bf1a9b1d
Deleted: sha256:6966a3782a9b048a87507999bca0503e5971f5c83164ce8ce775dfefcc7f3d29
Deleted: sha256:a8ff4211732a595e112b39fd1c98459406ef1a3ae94b743df60d1996ca19bc75
Deleted Volumes:
edo_data-logs-secondary
edo_data-pg
edo_data-raddb-ssl
edo_data-zookeeper
edo_data-ci-modules
edo_data-dict
edo_data-docker-ssl
edo_data-kafka-secrets
edo_data-db-backup
edo_data-logs
edo_data-raddb
edo_data-www-ssl
edo_data-raddb-secondary
edo_data-zookeeper-log
edo_data-db-acs
edo_data-dict-secondary
edo_data-kafka
edo_data-license
edo_data-tac-plus-secondary
edo_data-zookeeper-secrets
edo_data-ci-configurations
edo_data-raddb-ssl-secondary
edo_data-samba
edo_data-tac-plus
Total reclaimed space: 1.305GB
administrator@efros-do:~$ _
```

Рисунок 38 – Процесс удаления файлов и каталогов

3.6 Windows-агент ПК «Efros DO»

3.6.1 Установка Windows-агента

Windows-агент устанавливается на контролируемые сервера под управлением ОС MS Windows, и предназначен для обеспечения операций контроля целостности файловых объектов. Для установки windows-агента необходимо войти на контролируемый сервер от имени учетной записи с правами администратора этого сервера, скопировать на контролируемый сервер файл **EfrosCI.agent.msi** и запустить его на исполнение. Файл расположен внутри архива **efros-do_<название ОС>.tar.gz** и становится доступен после распаковки архива (путь **/opt/efros-do/EfrosCI.agent.msi**).

Откроется окно мастера установки windows-агента, в котором следует выбрать папку для установки агента или оставить заданную по умолчанию (**C:\Program Files (x86)\EFROS Config Inspector 4**) и нажать кнопку «Далее» (рис. 39).

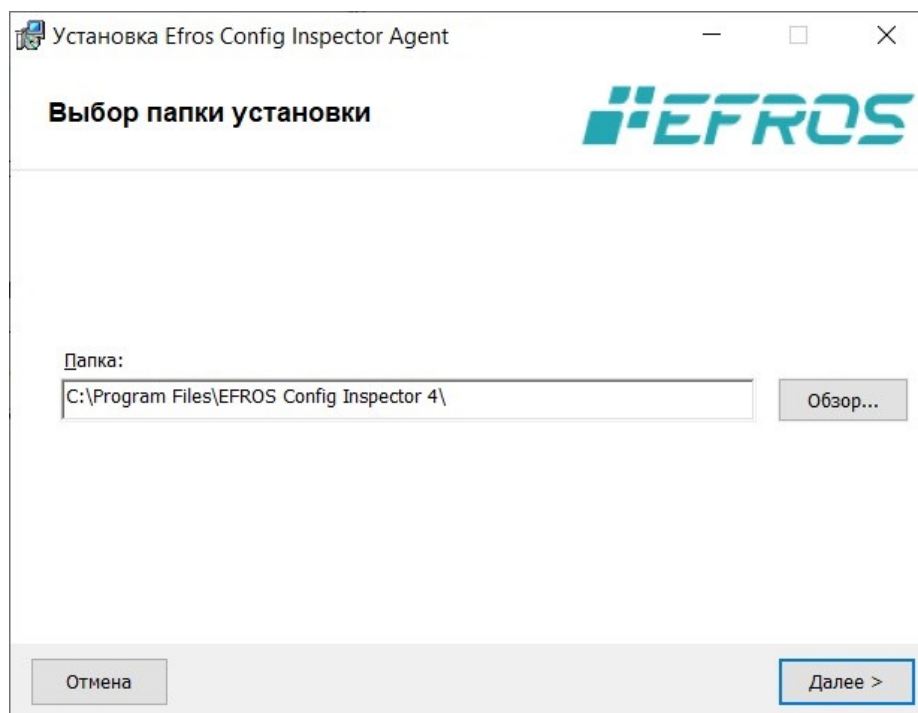


Рисунок 39 – Диалоговое окно выбора установки windows-агента

В диалоговом окне готовности мастера к установке (рис. 40) для запуска процесса инсталляции с заданными ранее параметрами следует нажать кнопку «Установить».

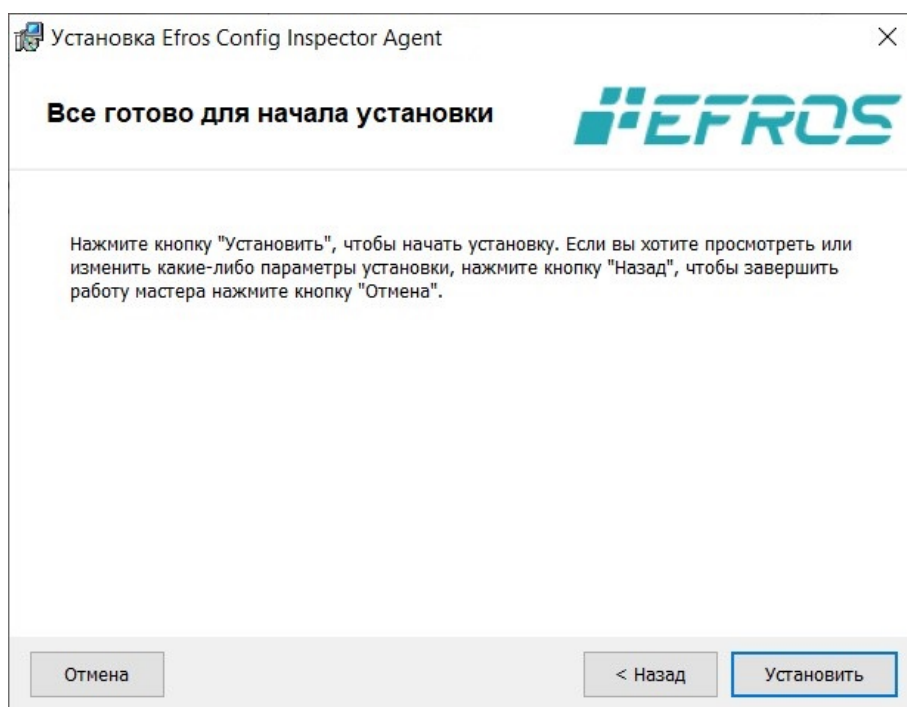


Рисунок 40 – Диалоговое окно готовности к установке

Ход установки windows-агента программного комплекса будет отображаться в окне мастера установки (рис. 41).

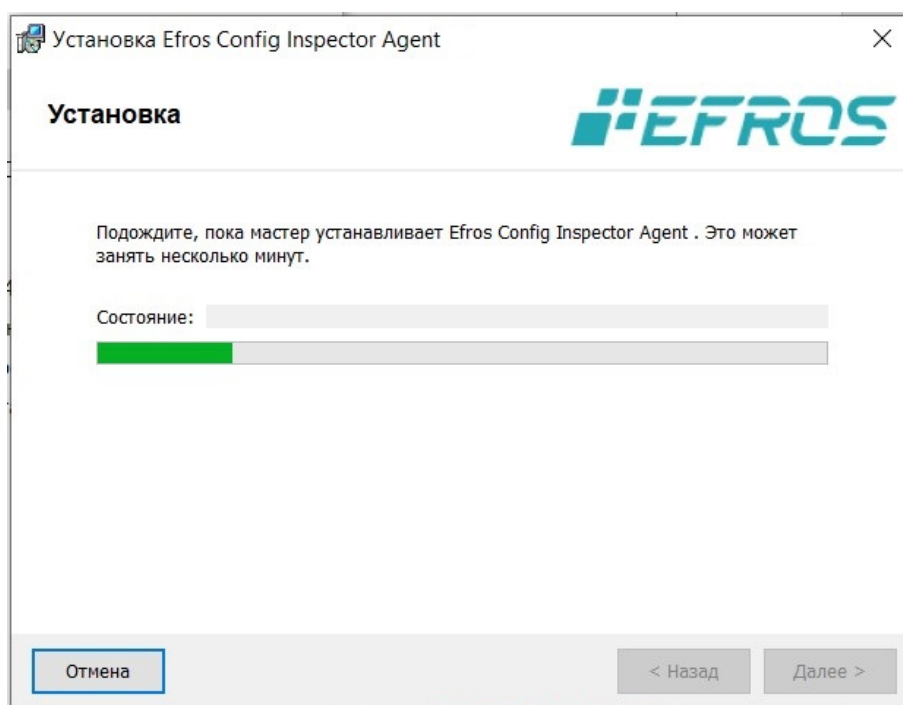


Рисунок 41 – Диалоговое окно процесса установки

После окончания установки windows-агента откроется диалоговое окно завершения работы мастера установки (рис. 42), в котором следует нажать кнопку «Готово».

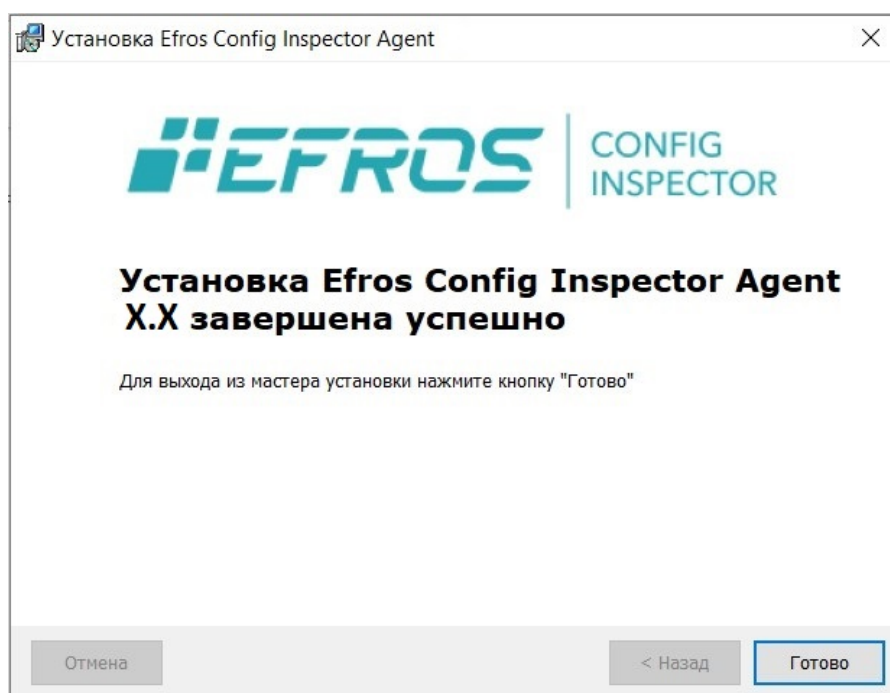


Рисунок 42 – Диалоговое окно завершения работы мастера установки

Windows-агент устанавливается на контролируемый рабочий сервер в качестве службы EFROS CI Agent Service 4, которая запускается в автоматическом режиме при загрузке ОС от имени системной учетной записи (Local System).

Настройка параметров службы Windows-агента выполняется в окне настройки параметров службы «Efros Config Inspector» (**C:\Program Files\EFROS Config Inspector 4\Agent\WASetup.exe**).

3.6.2 Настройка параметров службы windows-агента

Вызов окна настройки параметров службы «Efros Config Agent» осуществляется путем запуска файла **WASetup.exe** из директории **C:\Program Files\EFROS Config Inspector 4\Agent**.

После запуска появится окно с вкладкой «Службы» для настройки параметров службы «Efros Config Agent» (рис. 43).

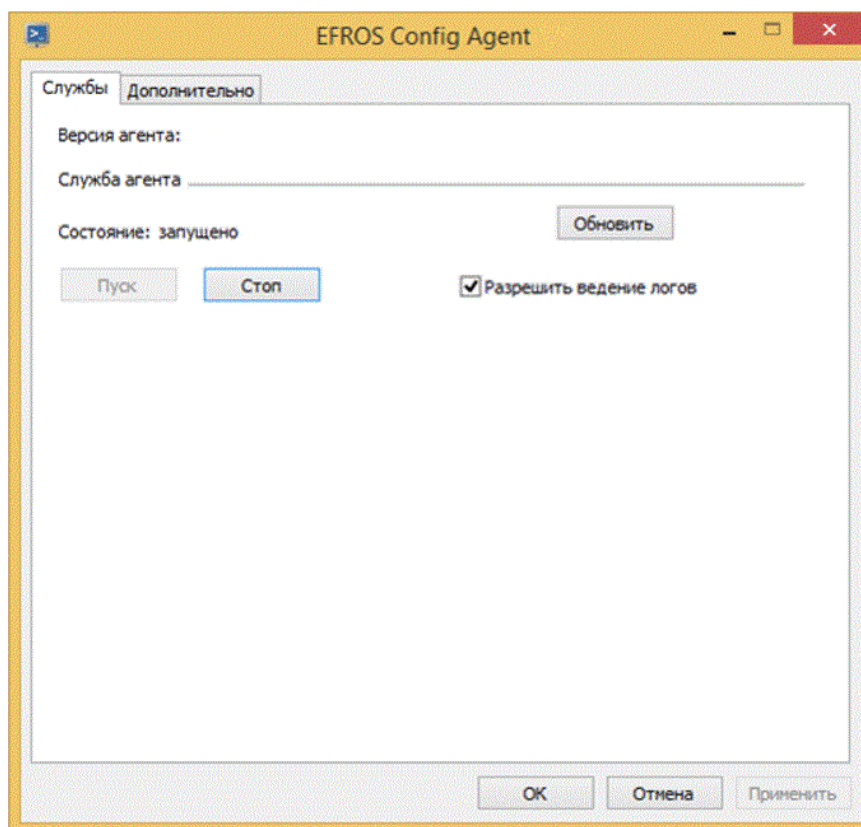


Рисунок 43 – Вкладка «Службы» окна настройки параметров службы «Efros Config Agent»

Состав и описание полей вкладок страницы приведены в таблице 3.

Таблица 3 – Состав и описание полей вкладки «Службы» окна настройки параметров службы «Efros Config Agent»

Поле	Описание
Поле «Версия агента»	Отображает последнюю версию установленного агента
Раздел «Служба агента»	
Поле «Состояние»	Отображает статус агента: — запущено; — установлено
Поле «Разрешить ведение логов»	Включает/отключает ведение логов программы настройки windows-агента WASetup
Кнопки управления	
Пуск	Запуск службы windows-агента
Стоп	Остановка службы windows-агента
Обновить	Для обновления статуса службы windows-агента

После завершения настройки службы windows-агента, необходимо нажать кнопку «Применить» и кнопку «ОК» для закрытия окна. После этого, настроенные параметры будут приняты и вступят в силу при следующем запуске службы windows-агента. В случае, если агент запущен, будет предложен перезапуск.

При переходе на вкладку «Дополнительно» отображаются дополнительные настройки службы, рис. 44.

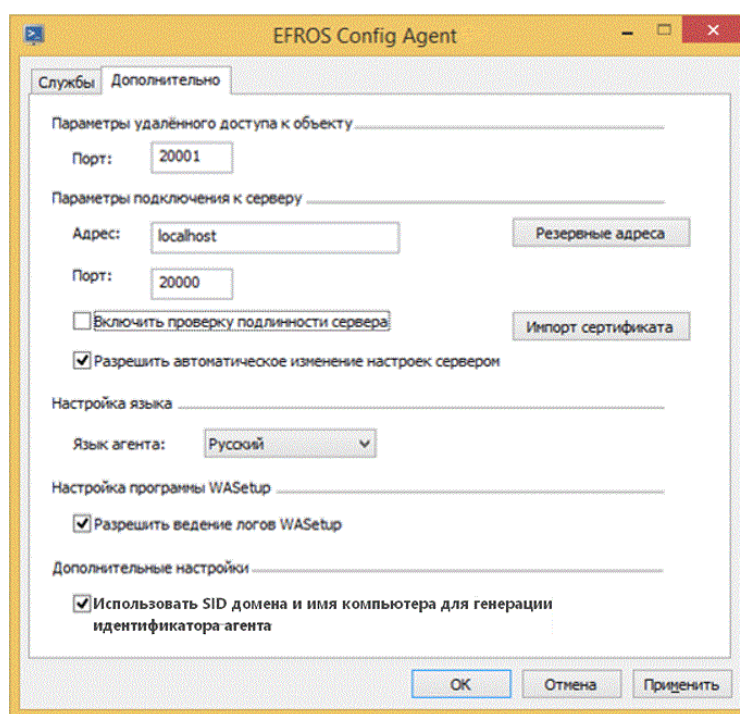


Рисунок 44 – Вкладка «Дополнительно» окна настройки параметров службы «Efros Config Agent»

Состав и описание полей вкладки приведены в таблице 4.

Таблица 4 – Состав и описание полей вкладки «Дополнительно» окна настройки параметров службы «Efros Config Agent»

Поле	Описание
Параметры удаленного доступа к объекту	
Поле «Порт»	Номер порта, используемого для установки связи между сервером ПК «Efros DO» и windows-агентом (для оповещения о включении windows-агента)
Параметры подключения к серверу	
Поле «Адрес»	IP-адрес сервера ПК «Efros DO» или его DNS-имя
Поле «Порт»	Номер порта, используемого для подключения сервера ПК к

Поле	Описание
	windows-агенту
Кнопка «Резервные адреса»	Позволяет задавать резервные адреса для установки связи с резервными серверами комплекса. В случае работы комплекса в режиме отказоустойчивости, windows-агент получает информацию о резервных серверах, с которыми он может работать в случае отказа основного сервера ПК «Efros DO»
Поле «Включить проверку подлинности сервера»	При включенном параметре (флаг в поле установлен) происходит проверка серверной части и windows-агента с помощью сертификата
Кнопка «Импорт сертификата»	Позволяет устанавливать сертификат взаимодействия с серверной частью вручную
Поле «Разрешить автоматическое изменение настроек сервером»	При включенном параметре (флаг в поле установлен) настройки windows-агента (адрес сервера, проверка подлинности сертификатом) могут быть автоматически изменены сервером ПК «Efros DO»
Поле «Язык агента»	Позволяет выбрать язык windows-агента (русский, английский)
Поле «Разрешить ведение логов WSetup»	Включает/отключает ведение логов программы настройки windows-агента WSetup
Поле «Использовать SID домена и имя компьютера для генерации идентификатора агента»	Позволяет автоматически генерировать uuid windows-агента на основе SID домена при подключении ОС в домен. Используется для обеспечения уникальности uuid windows-агента в случае клонирования виртуальных машин с предустановленным windows-агентом

3.7 Суппликант ПК «Efros DO»

3.7.1 Установка суппликанта ПК «Efros DO»

Суппликант ПК «Efros DO» (далее – суппликант) устанавливается на контролируемые конечные точки. Суппликант предназначен для проверки конечных точек на соответствие политикам безопасности и передачи результатов на сервер ПК «Efros DO». Если проверки не пройдены, суппликант мгновенно реагирует согласно заданным в комплексе политикам безопасности.

Для установки суппликанта необходимо выполнить следующие действия:

1) Скопировать на контролируруемую конечную точку файл **EDO-Agent-<название ОС>-suplicant.deb**.

2) В интерфейсе командной строки ввести следующие команды:

```
sudo dpkg -i EDO-Agent-0.1.0-Linux-suplicant.deb  
systemctl enable edo-suplicant-wired@eth1.service  
systemctl start edo-suplicant-wired@eth1.service
```

 Команды необходимо вводить от имени суперпользователя **root**.

 Параметр «eth1» является уникальным именем сетевого интерфейса.

3) Установка суппликанта завершена.

3.7.2 Настройка параметров суппликанта

Для настройки суппликанта необходимо выполнить следующее:

1) Запустить суппликант. Появится стартовое окно (рис. 45).

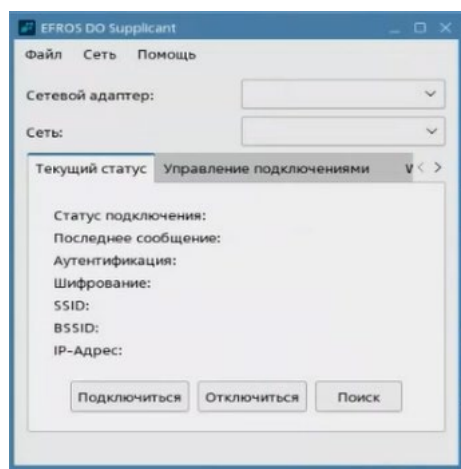


Рисунок 45 – Стартовое окно

2) Перейти на вкладку «Управление подключениями» (рис. 46). Для добавления нового подключения необходимо нажать на кнопку «Добавить». Для

корректировки существующего подключения необходимо из раскрывающихся списков «Сетевой адаптер» и «Сеть» выбрать требуемые параметры и нажать кнопку «Изменить».

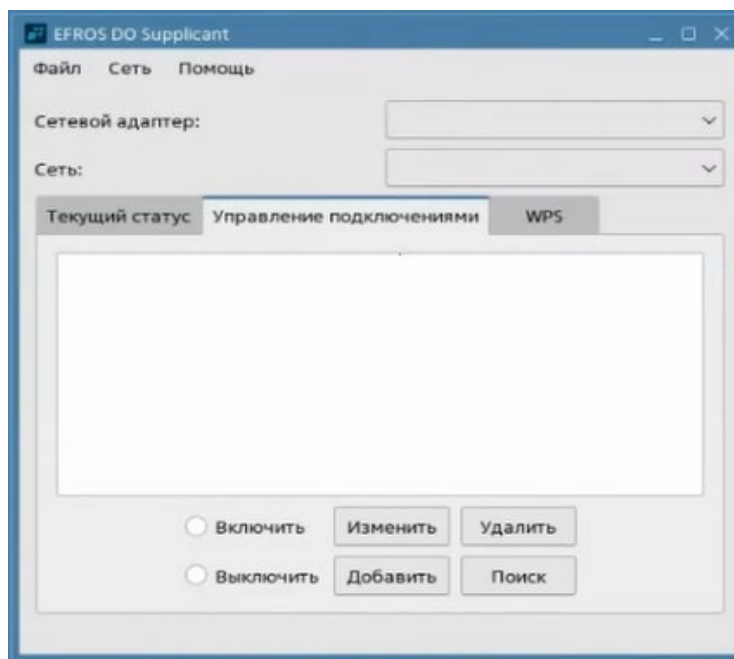


Рисунок 46 – Вкладка «Управление подключениями»

- 3) Откроется окно «Настройка подключения» (рис. 47). Состав и описание полей окна приведены в таблице 5.

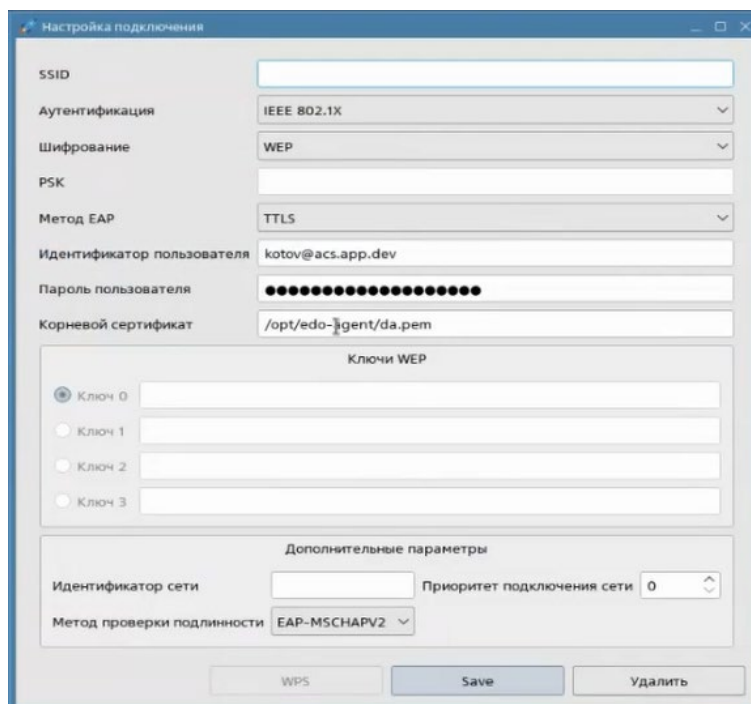


Рисунок 47 – Окно «Настройка подключения»

Таблица 5 – Состав и описание полей окна «Настройка подключения»

Поле	Описание
Поле «SSID»	Текстовое поле для ввода имени беспроводной сети. Для проводной сети поле не заполняется
Поле «Аутентификация»	Раскрывающийся список видов аутентификации: <ul style="list-style-type: none"> — «Открытая (без аутентификации)»; — «Статический WEP (без аутентификации)»; — «Статический WEP (Аутентификация с общим ключом)»; — «IEEE 802.1X»; — «WPA-Personal (PSK)»; — «WPA-Enterprise (EAP)»; — «WPA2-Personal (PSK)»; — «WPA2- Enterprise (EAP)»
Поле «Шифрование»	Раскрывающийся список типов шифрования подключения
Поле «PSK»	Пароль для подключения к беспроводной сети. Поле заполняется, если в поле «Аутентификация» выбран вид аутентификации по беспроводной сети
Поле «Метод EAP»	Раскрывающийся список EAP-протоколов
Поле «Идентификатор пользователя»	Логин пользователя, у которого есть доступ в сеть
Поле «Пароль пользователя»	Пароль пользователя, у которого есть доступ в сеть
Поле «Корневой сертификат»	Сертификат организации, в которой расположена конечная точка с установленным суппликантом
Группа полей «Ключи WEP»	Ключи для метода аутентификации WEP. Поле доступно для заполнения, если в поле «Аутентификация» выбран вид аутентификации WEP
Группа полей «Дополнительные параметры»	
Поле «Идентификатор сети»	Параметр для идентификации сетей
Поле «Приоритет подключения сети»	Уровень приоритета для подключения сети, если добавлено несколько подключений
Поле «Метод	Раскрывающийся список дополнительных методов

Поле	Описание
проверки подлинности»	проверки подлинности
Элементы управления	
WPS	Недоступна для выполнения действий
Save	При нажатии на кнопку введенные данные сохраняются
Удалить	При нажатии на кнопку введенные данные удаляются

- 4) Нажать кнопку «Save».
- 5) Закрывать окно «Настройка подключения». На вкладке «Управление подключениями» появится добавленное подключение.
- 6) Перейти на вкладку «Текущий статус» (рис. 48). Выбрать добавленное подключение и нажать кнопку «Подключиться».
- 7) На вкладке «Текущий статус» отобразятся данные по подключению.

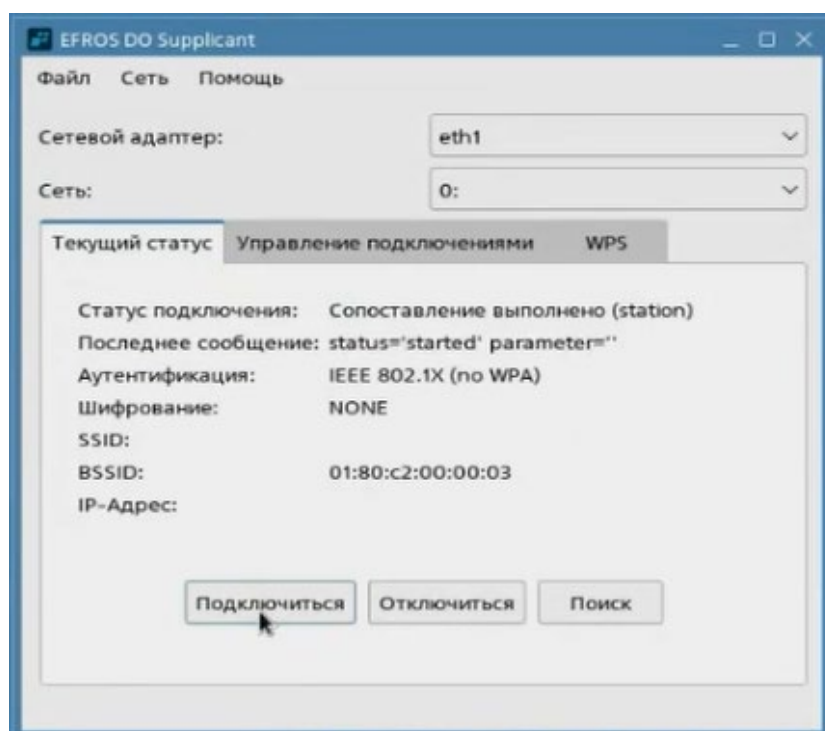


Рисунок 48 – Вкладка «Текущий статус»

4 Обновление программного комплекса

Обновление ПК «Efros DO» осуществляется после предоставления нового дистрибутива разработчиком. Процесс обновления аналогичен процессу установки программного комплекса:

- 1) Скопировать файлы ***efros-do_<название ОС>.tar.gz*** и ***deploy.sh*** в одну директорию.
- 2) Для обновления комплекса со встроенной БД – запустить скрипт ***deploy.sh*** без дополнительных аргументов, с правами администратора.
- 3) Для обновления комплекса с подключенной внешней БД необходимо запустить скрипт с аргументом ***--dbfree***. В процессе обновления пользователю необходимо будет повторно указать следующие параметры:
 - IP адрес сервера СУБД (в формате 192.168.1.1);
 - порт для подключения к серверу СУБД (в формате 5432);
 - учетную запись для подключения к БД;
 - пароль для подключения к БД.

Подробнее процесс установки рассмотрен в разделе 3 документа.

5 Сообщения администратору

ПК «Efros DO» не предусматривает каких-либо диагностических сообщений. Сообщения об ошибках в настройке ПК «Efros DO» либо об ошибках комплекса выводятся в виде стандартных диалоговых окон с соответствующими пояснениями.

Перечень сокращений

CM	–	Change Manager
DNS	–	Domain Name System
FA	–	Firewall Assurance
HTTP	–	HyperText Transfer Protocol
HTTPs	–	HyperText Transfer Protocol Secure
ICC	–	Integrity Check Compliance
IP	–	Internet Protocol
IPFIX	–	Internet Protocol Flow Information Export
NA	–	Network Assurance
NAC	–	Network Access Control
NFA	–	Network Flow Analysis
RADIUS	–	Remote Authentication in Dial-In User Service
SE	–	Special Edition
SID	–	Security Identifier
SNMP	–	Simple Network Management Protocol
SP	–	Service Pack
TACACS+	–	Terminal Access Controller Access Control System plus
VC	–	Vulnerability Control
БД	–	База данных
ИБ	–	Информационная безопасность
ОЗ	–	Объект защиты
ООО	–	Общество с ограниченной ответственностью
ОС	–	Операционная система
ПК	–	Программный комплекс
СУБД	–	Система управления базами данных
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭВМ	–	Электронно-вычислительная машина