

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.....	5
2	Подготовка к установке программы.....	13
3	Установка, настройка и удаление программы.....	14
3.1	Состав и содержание дистрибутива.....	14
3.2	Предварительная настройка СУБД.....	15
3.3	Порядок установки.....	16
3.3.1	Настройка политик безопасности ОС для типа защиты «Максимальный» («Смоленск»).....	17
3.3.2	Настройка политик безопасности ОС для типа защиты «Усиленный» («Воронеж»).....	23
3.3.3	Настройка политик безопасности ОС для типа защиты «Базовый» («Орел»).....	29
3.3.4	Установка ПК «Efros DO».....	29
3.4	Перенастройка сети.....	33
3.5	Лицензирование.....	33
3.5.1	Online активация комплекса.....	35
3.5.2	Offline активация комплекса.....	37
3.5.3	Реактивация лицензии комплекса.....	41
3.6	Удаление изделия.....	43
3.7	Кластеризация.....	45
3.7.1	Кластеризация на Astra Linux SE.....	48
3.7.1.1	Предварительные настройки.....	48
3.7.1.2	Установка кластера.....	49
3.7.1.3	Возможные ошибки и способы их устранения.....	53
3.7.1.4	Удаление кластера.....	55
3.7.2	Кластеризация на РЕД ОС.....	55
3.7.2.1	Предварительные настройки.....	55
3.7.2.1.1	Настройка хостов.....	55
3.7.2.1.2	Настройка master-нод.....	56
3.7.2.1.3	Настройка управления кластером.....	68
3.7.2.2	Установка кластера.....	69
3.7.2.3	Удаление кластера.....	73
3.8	Windows-агент ПК «Efros DO».....	75

3.8.1	Установка windows-агента	75
3.8.2	Настройка параметров службы windows-агента.....	77
3.9	Агент ПК «Efros DO».....	80
3.9.1	Установка агента ПК «Efros DO» на Windows.....	80
3.9.2	Удаление агента ПК «Efros DO» на Windows	85
3.9.3	Установка агента ПК «Efros DO» на Linux.....	85
3.9.4	Удаление агента ПК «Efros DO» на Linux	85
3.9.5	Установка агента ПК «Efros DO» на MacOS	86
3.9.6	Удаление агента ПК «Efros DO» на MacOS	86
3.10	Суппликант ПК «Efros DO»	87
3.10.1	Установка суппликанта ПК «Efros DO» на Windows	87
3.10.2	Удаление суппликанта ПК «Efros DO» на Windows.....	90
3.10.3	Установка суппликанта ПК «Efros DO» на Linux.....	90
3.10.4	Настройка параметров суппликанта ПК «Efros DO» на Linux.....	91
3.10.5	Удаление суппликанта ПК «Efros DO» на Linux.....	96
4	Обновление программного комплекса	97
5	Сообщения администратору	98
	Перечень сокращений	99

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

ПК «Efros DO» является высокопроизводительным комплексом по защите системно-технической инфраструктуры. Конфигурация ПК «Efros DO» зависит от наличия лицензий на следующие 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 Manager» («Efros CM»);
- «Efros Secure DNS» («Efros DNS»).

Архитектура комплекса построена на основе микросервисов на базе платформы контейнеризации Docker и модулей платформы «Efros DO»:

- платформа интеграции – единый интерактивный интерфейс, представляющий полный контроль над автоматизацией процессов информационной безопасности (ИБ);
- подсистема хранения данных;
- модуль обмена данными Apache Kafka;
- модуль хранения данных OpenSearch;
- модуль распределенного хранения объектов MinIO;
- функциональные модули – «Efros NA», «Efros FA», «Efros NAC», «Efros ICC», «Efros VC», «Efros «NFA», «Efros CM», «Efros DNS»;
- микросервис лицензирования;
- микросервис аутентификации и авторизации;
- микросервис уведомлений и событий;
- микросервис объектов защиты;
- микросервис сбора метрик ИБ;
- микросервис маршрутизации запросов;
- микросервис генерации отчетов;
- микросервис базы знаний;
- микросервис драйверов сканеров уязвимостей;
- микросервис системы заявок;
- микросервис отправки сообщений;

- микросервис расписаний;
- микросервис гостевых порталов;
- микросервис службы DNS;
- микросервис управления службами DNS;
- микросервис поддержки иерархии;
- микросервис управления агентами ПК «Efros DO»;
- микросервис поиска маршрутов для моделирования трафика на карте сети;
- микросервис управления контейнеризацией и кластеризацией.

Необходимым условием работы комплекса является возможность подключения к системам хранения данных. В работе комплекса используются 2 категории баз данных (БД): SQL и NoSQL. БД SQL применяется для хранения всех данных, используемых и получаемых комплексом. БД NoSQL применяется сервисами аудита для хранения записей аудита, а также хранения данных сетевых потоков, таких как NetFlow.

По умолчанию возможно установить СУБД свободного лицензирования, как PostgreSQL 13 и OpenSearch 1.3.7.

Упрощенная архитектурная схема сервисов и потоков данных представлена на рис. 1.

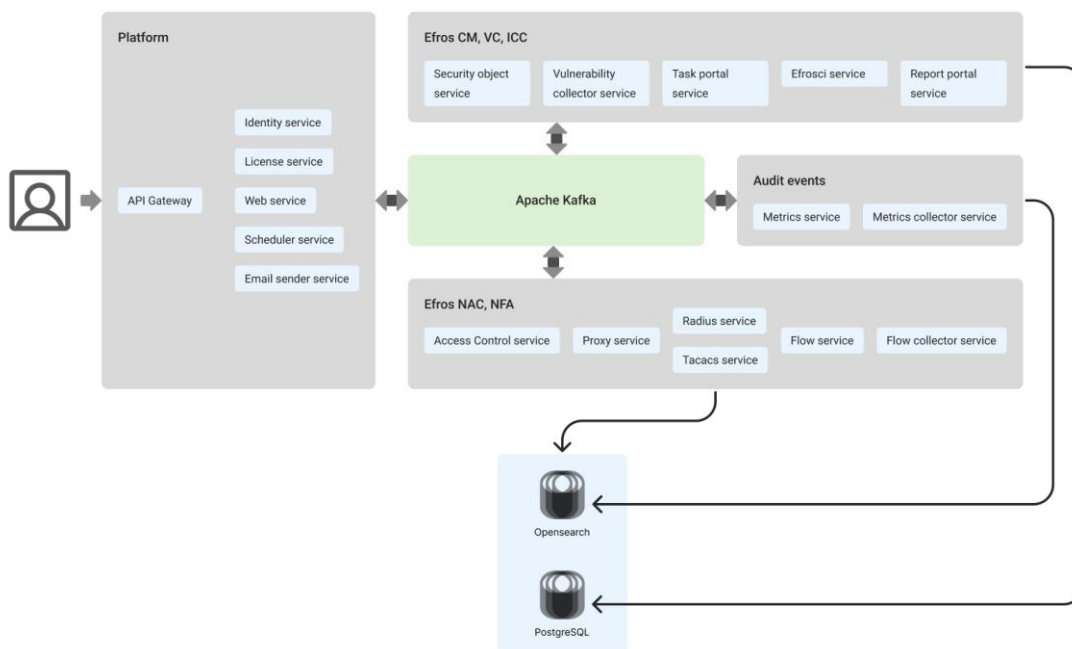


Рисунок 1 – Схема сервисов и потоков данных


Взаимосвязь сервисов в ПК «Efros DO» приведена в таблице 1.

Таблица 1 – Взаимосвязь сервисов в комплексе

Название сервиса	Описание	Связь с другими сервисами
Edo web service	Микросервис, отвечающий за пользовательский веб-интерфейс	— Edo identity service tcp 80/443; — Postgres DB tcp 5432; — Kafka service tcp 9092
Edo proxy service	Сервер Nginx, выполняющий шифрование трафика и обратное проксирование	
Edo gateway service	Микросервис маршрутизации запросов	— Edo license service tcp 80/443; — Edo identity service tcp 80/443; — Edo so service tcp 80/443; — Edo metrics service tcp 80/443; — Edo web service tcp 80/443
Edo identity service	Микросервис аутентификации и авторизации пользователей и служб комплекса, а также парольной политики	— Kafka service tcp 9092; — Opensearch DB tcp 9200/9300
Edo license service	Микросервис, контролирующий работу выданных лицензий. Связывается с сервером лицензирования для активации и обновления лицензионных пакетов	— Edo identity service tcp 80/443; — Postgres DB tcp 5432; — Kafka service tcp 9092
Edo so service	Микросервис по работе с объектами защиты (ОЗ)	— Edo identity service tcp 80/443; — Postgres DB tcp 5432; — Kafka Service tcp 9092
Edo acs service	Микросервис контроля доступа в сеть и к сетевому оборудованию	— Postgres DB tcp 5432; — Kafka service tcp 9092
Edo radius	RADIUS сервер	— Edo acs service tcp 80/443

Название сервиса	Описание	Связь с другими сервисами
Edo tacacs	TACACS+ сервер	— Edo acs service tcp 80/443
Edo samba service	SMB сервер	— Edo acs service tcp 80/443
Edo efroscli service	Микросервис управления и загрузки конфигураций, контроля сетевых устройств и других объектов сетевой инфраструктуры	— Postgres DB tcp 5432; — Opensearch DB tcp 9200/9300
Edo email sender service	Микросервис по отправке почтовых уведомлений	— Kafka service tcp 9092; — Postgres DB tcp 5432
Edo vulnerability collector	Микросервис драйверов сканеров уязвимостей	— Kafka service tcp 9092; — Postgres DB tcp 5432
Edo knowledge base service	Микросервис базы знаний	— Kafka service tcp 9092; — Postgres DB tcp 5432
Edo flow collector	Микросервис сбора данных сетевой активности с сетевых устройств	— Kafka Service tcp 9092; — Edo flow service tcp 80/443; — Opensearch DB tcp 9200/9300
Edo flow service	Микросервис сбора отчетов по сетевой активности	— Kafka service tcp 5803/5804; — Opensearch DB tcp 9200/9300
Edo portal api	Микросервис гостевых порталов для доступа в сеть	— Postgres DB tcp 5432
Edo metrics collector	Микросервис централизованного сбора событий системы	— Kafka Service tcp 9200/9300
Edo metrics service	Микросервис отчетов событий системы	— Edo identity service tcp 80/443; — Opensearch DB tcp 9200/9300; — Postgres DB tcp 5432; — kafka Service tcp 9092

Название сервиса	Описание	Связь с другими сервисами
Edo schedule service	Микросервис расписаний	— Kafka service tcp 9092; — Opensearch DB tcp 9200/9300
Edo report portal service	Микросервис генерации отчетов	— Kafka service tcp 9092; — Postgres DB tcp 5432
Edo task portal service	Микросервис по работе с заявками и управления изменениями	— Kafka service tcp 9092; — Postgres DB tcp 5432
Apache Kafka	Микросервис распределенного обмена сообщениями между серверными приложениями в режиме реального времени Apache Kafka	— Zookeeper tcp 2181
Zookeeper	Централизованный микросервис по хранению информации о конфигурации, а также распределенной синхронизации, необходимый для функционирования сервиса Kafka	

 В случае возникновения каких-либо ошибок с развертыванием сервисов необходимо посмотреть логи сервиса. Для этого нужно выполнить команду:

```
docker logs -t <имя контейнера>
```

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 2.

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

Таблица 2 – Технические требования к среде функционирования ПК «Efros DO» и прикладному программному обеспечению

Поле	Параметр		
	До 500	До 1000	До 2000*
Количество объектов защиты (ОЗ)			
Требования к программному обеспечению			
Операционная система (ОС)	Astra Linux Special Edition (v.1.7), сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.), поддерживается установка на ОС с ядром 5.15-Generic; Альт Server 10; РЕД ОС (v. 7.3), сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.)		
Поддерживаемые системы управления базами данных (СУБД)	СУБД PostgreSQL 13; СУБД «Jatoba» (поддерживается версия «ядра» 4)		
Прикладное программное обеспечение	Docker v. 18.03.0 и выше; Docker-compose v. 2.9.0; Confluent Kafka v. 5.5.0; СУБД OpenSearch v. 1.3.7; СУБД MinIO v. 220218		
Требования к аппаратному обеспечению			
Процессор	16 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)
Оперативная память	от 32 Гб	от 48 Гб	от 64 Гб
Жесткий диск (комплекс + СУБД)	от 600 Гб	от 1200 Гб	от 2400 Гб
Сервер комплекса	от 200 Гб	от 200 Гб	от 200 Гб
Сервер СУБД	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»			
Подключение	Порт	Протокол	Направление
TACACS+	49	tcp	входящий
RADIUS	1812, 1813	udp	входящий
Гостевые порталы	5802	tcp	в обе стороны
Требования для функционирования модуля «Efros NFA»			
Подключение	Порт	Протокол	Направление
Netflow v5	2055	udp	входящий
Netflow v9+, IPFIX	2056	udp	входящий
sFlow	6343	udp	входящий
Требования для функционирования модуля «Efros DNS»			
Подключение	Порт	Протокол	Направление
DNS	53	tcp/udp	в обе стороны
Требования для функционирования модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros CM»			
Подключение	Порт	Протокол	Направление
Для подключения Windows-агента	20002	tcp	входящий


Поле	Параметр		
Syslog	514	udp	входящий
SNMP Trap / Inform	162	udp	входящий
Windows-агент			
ОС	Windows**		
Процессор	1,6 ГГц		
Оперативная память	1 Гб		
Жесткий диск	100 Мб		
Агент ПК «Efros DO»			
ОС	Windows** (поддерживается только 64-разрядная версия ОС); РЕД ОС (рабочая станция, сервер) (7.3 и выше); Astra Linux Special Edition (1.6 и выше); Ubuntu (22.04 и выше); MacOS Monterey (12.6 и выше) x86_64		
Суппликант ПК «Efros DO»			
ОС	Windows** (поддерживается только 64-разрядная версия ОС); РЕД ОС (рабочая станция, сервер) (7.3 и выше); Astra Linux Special Edition (1.6 и выше)		
Минимальные требования к производительности рабочей станции, на которую устанавливается агент ПК «Efros DO» и суппликант ПК «Efros DO», обусловлены требованиями используемой ОС			
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:			
<ul style="list-style-type: none"> — 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); 			

Поле	Параметр
	— 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);
	— Windows 11 Home (64-разрядная);
	— Windows 11 Pro (64-разрядная);
	— Windows 11 Enterprise (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. Состав дистрибутива указан в таблице 3.

Таблица 3 – Состав дистрибутива ПК «Efros DO» для установки

Файл	Назначение
efros-do_<название ОС>.tar.gz	дистрибутив, содержащий все компоненты программы, образы и зависимости
deploy.sh	скрипт для установки ПК «Efros DO» на ОС
edo-agent-<версия>.msi	файл для установки агента ПК «Efros DO» на конечную точку ОС Windows
edo-agent-<версия>.rpm	файл для установки агента ПК «Efros DO» на конечную точку РЕД ОС
edo-agent-<версия>.deb	файл для установки агента ПК «Efros DO» на конечную точку ОС Astra Linux Special Edition или ОС Ubuntu
edo-agent-<версия>.pkg	файл для установки агента ПК «Efros DO» на конечную точку ОС MacOS
edo-suplicant-<версия>.msi	файл для установки суппликанта ПК «Efros DO» на конечную точку ОС Windows
edo-suplicant-<версия>.rpm	файл для установки суппликанта ПК «Efros DO» на конечную точку РЕД ОС
edo-suplicant-<версия>.deb	файл для установки суппликанта ПК «Efros DO» на конечную точку ОС Astra Linux Special Edition
EfrosCl.agent.msi	файл для установки windows-агента на контролируемый сервер

Состав образов функциональных модулей и микросервисов ПК «Efros DO», поставляемых пользователю, приведен в таблице 4.

Таблица 4 – Состав образов ПК «Efros DO»

Файл	Назначение
edo-acsc-service.tar.gz	функциональный модуль централизованного управления контролем доступа к сетевым устройствам
edo-efros-ci.tar.gz	функциональный модуль управления конфигурациями, анализа защищенности, анализа сетевой безопасности и оценки рисков
edo-ci-route-service.tar.gz	микросервис поиска маршрутов для моделирования трафика на карте сети
edo-agent-service.tar.gz	микросервис управления агентами ПК «Efros DO»
edo-hierarchy-service.tar.gz	микросервис поддержки иерархии

Файл	Назначение
edo-dns-manager.tar.gz	микросервис управления службами DNS
edo-dns-service.tar.gz	микросервис службы DNS
edo-email-sender-service.tar.gz	микросервис отправки сообщений
edo-flow-collector.tar.gz	модуль сбора статистики
edo-flow-service.tar.gz	модуль Flow Service
edo-gateway-service.tar.gz	микросервис маршрутизации запросов
edo-identity-service.tar.gz	микросервис аутентификации и авторизации
edo-knowledge-base-service.tar.gz	микросервис базы знаний
edo-license-service.tar.gz	микросервис лицензирования
edo-metrics-collector.tar.gz	микросервис уведомлений и событий
edo-metrics-service.tar.gz	микросервис сбора метрик ИБ
edo-portal-api.tar.gz	микросервис гостевых порталов
edo-proxy-service_1.23.1.tar.gz	микросервис маршрутизации запросов
edo-radius_3.0.21-latest.tar.gz	модуль протокола RADIUS
edo-report-portal-service.tar.gz	микросервис генерации отчетов
edo-samba-service_4.9.5.tar.gz	функциональный модуль централизованного управления контролем доступа к сетевым устройствам
edo-schedule-service.tar.gz	микросервис расписаний
edo-so-service.tar.gz	микросервис объектов защиты
edo-tacacs_4.0.65535-latest.tar.gz	модуль протокола TACACS+
edo-task-portal-service.tar.gz	микросервис системы заявок
edo-vulnerability-collector.tar.gz	микросервис драйверов сканеров уязвимостей
edo-web-service.tar.gz	платформа интеграции
edo-k8s-operator.tar.gz	микросервис управления контейнеризацией и кластеризацией

3.2 Предварительная настройка СУБД

Перед установкой комплекса необходима предварительная настройка СУБД PostgreSQL\СУБД «Jatoba»:

- 1) Создать служебного пользователя для ПК «Efros DO», который будет владельцем БД для программного комплекса.
- 2) Разрешить служебному пользователю подключаться к БД комплекса с IP-адреса сервера, на котором установлен непосредственно комплекс. Для этого необходимо в файле *pg_hba.conf* для *IPv4 local connections* прописать значения, в зависимости от установки СУБД и комплекса.

Если СУБД установлена отдельно от сервера комплекса:

```
host {имя_базы_данных} {имя_служебного_пользователя_edo}
x.x.x.x/32 md5
```

где x.x.x.x – IP-адрес сервера комплекса.

В случае установки СУБД и ПК на один сервер:

```
host {имя_базы_данных} {имя_служебного_пользователя_edo}  
x.x.x.x/32 md5
```

где x.x.x.x – IP-адрес сервера, на который установлен комплекс и СУБД.

```
host {имя_базы_данных} {имя_служебного_пользователя_edo}  
172.16.128.0/17 md5
```

где 172.16.128.0 – IP-адрес сети docker по умолчанию.

- 3) В конфигурационном файле **postgresql.conf** разрешить прослушивать другие адреса. По умолчанию, СУБД прослушивает только **localhost**. Необходимо раскомментировать строку **listen_addresses = 'localhost'** и указать или IP-адрес сервера (рекомендуется), на котором установлен комплекс, или разрешить прослушивание запросов на всех IP-адресах (*):

```
listen_addresses = '*'
```

- ❗ При создании базы данных необходимо, чтобы были указаны следующие параметры:
 - тип кодировки – Encoding UTF8;
 - порядок сортировки строк – LC_COLLATE en-US;
 - классификация символов – LC_CTYPE en-US.

3.3 Порядок установки

- ℹ Процесс установки дистрибутива одинаков для различных поддерживаемых операционных систем: Astra Linux Special Edition (v.1.7) (Astra Linux SE), Альт Server 10, РЕД ОС (v. 7.3). При установке на целевую ОС необходимо скопировать архив дистрибутива, действия со скриптом аналогичны.
- ❗ При установке ПК «Efros DO» на ОС Astra Linux SE обязательно выполнить действия, описанные в пунктах 3.3.1 – 3.3.3. Для других ОС пункты 3.3.1 – 3.3.3 пропускаются.

- ! При установке ПК «Efros DO» на ОС РЕД ОС (v. 7.3) автоматически выключается система контроля доступа Security-Enhanced Linux. Допускается включение функции системы контроля доступа только в режиме "Permissive". В этом случае информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.

Ниже приведен порядок установки ПК «Efros DO». В качестве примера взята ОС Astra Linux SE. Для ПК «Efros DO» на этапе завершения установки ОС Astra Linux SE, необходимо добавить следующие наборы программного обеспечения, приведенные на рис. 2.

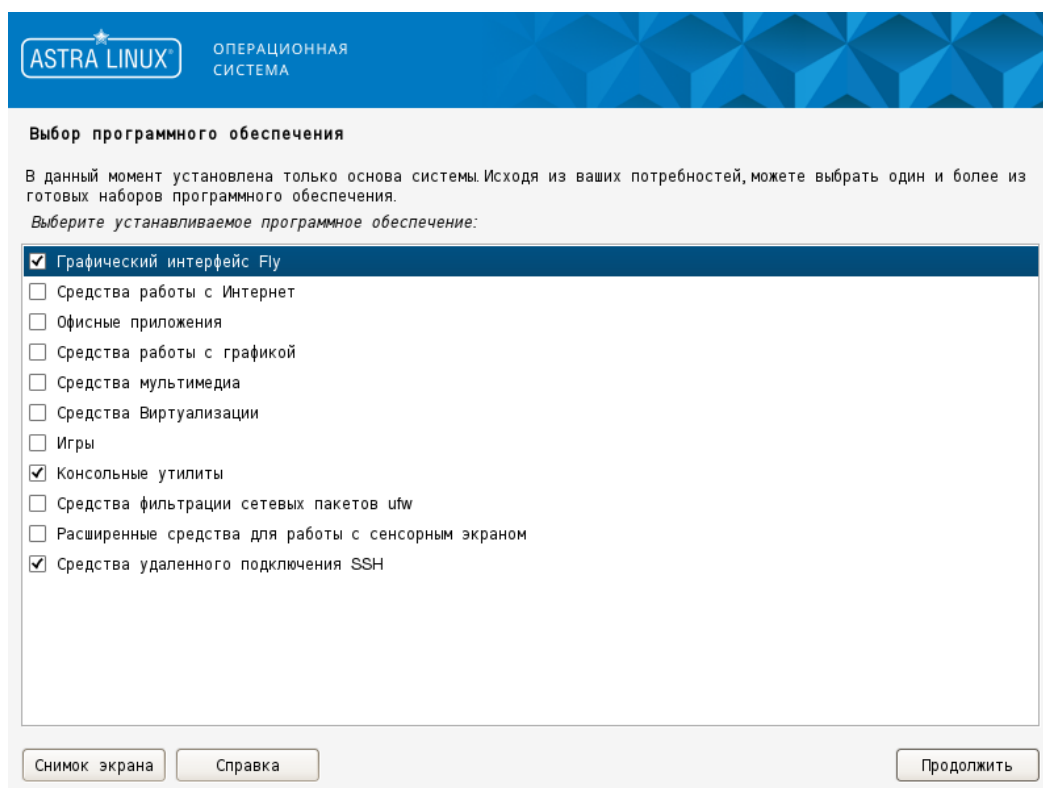


Рисунок 2 – Завершение установки ОС Astra Linux SE

3.3.1 Настройка политик безопасности ОС для типа защиты «Максимальный» («Смоленск»)

Перед установкой ПК «Efros DO» необходимо выполнить следующие настройки ОС Astra Linux SE для типа защиты «Максимальный» («Смоленск»):

- 1) После ввода логина и пароля, при выборе атрибутов безопасности для учетной записи из раскрывающегося списка необходимо выбрать уровень целостности «Высокий» (рис. 3).

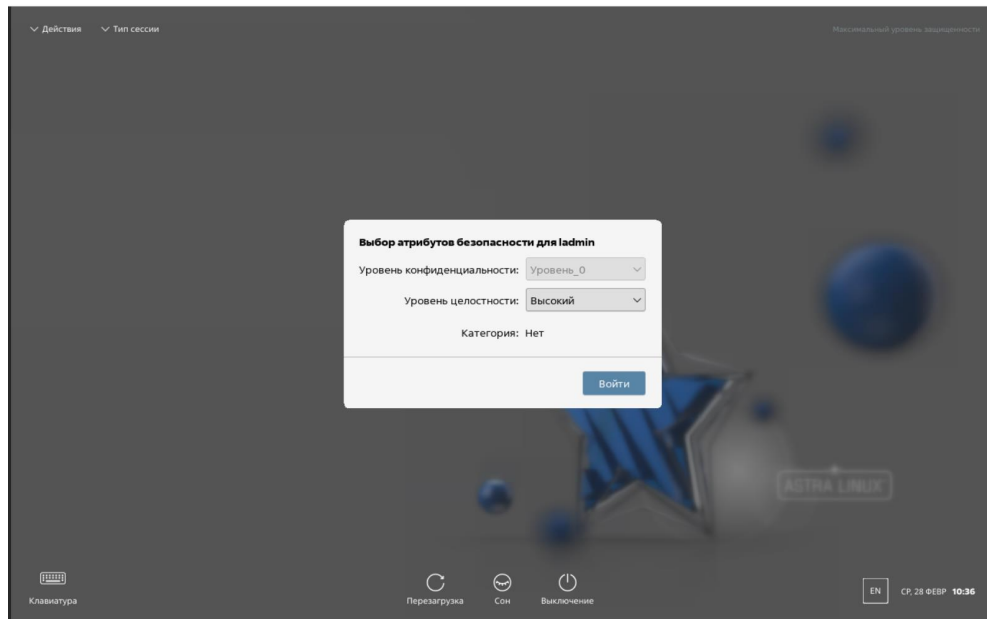


Рисунок 3 – Выбор атрибутов безопасности

2) Перейти в меню «Пуск» → «Системные» → «Политика безопасности» (рис. 4).

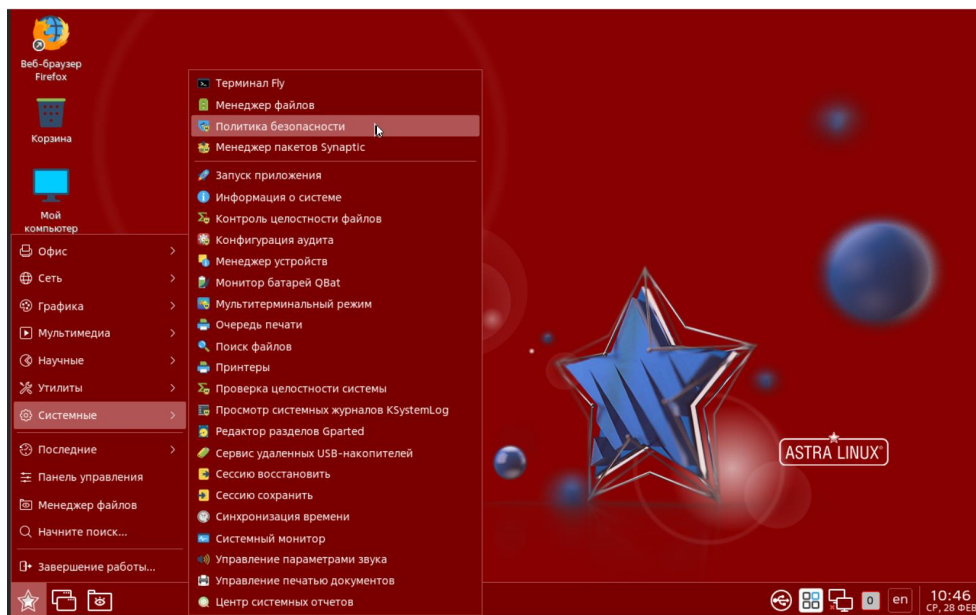


Рисунок 4 – Вкладка «Политики безопасности»

3) Ввести пароль администратора ОС (рис. 5).

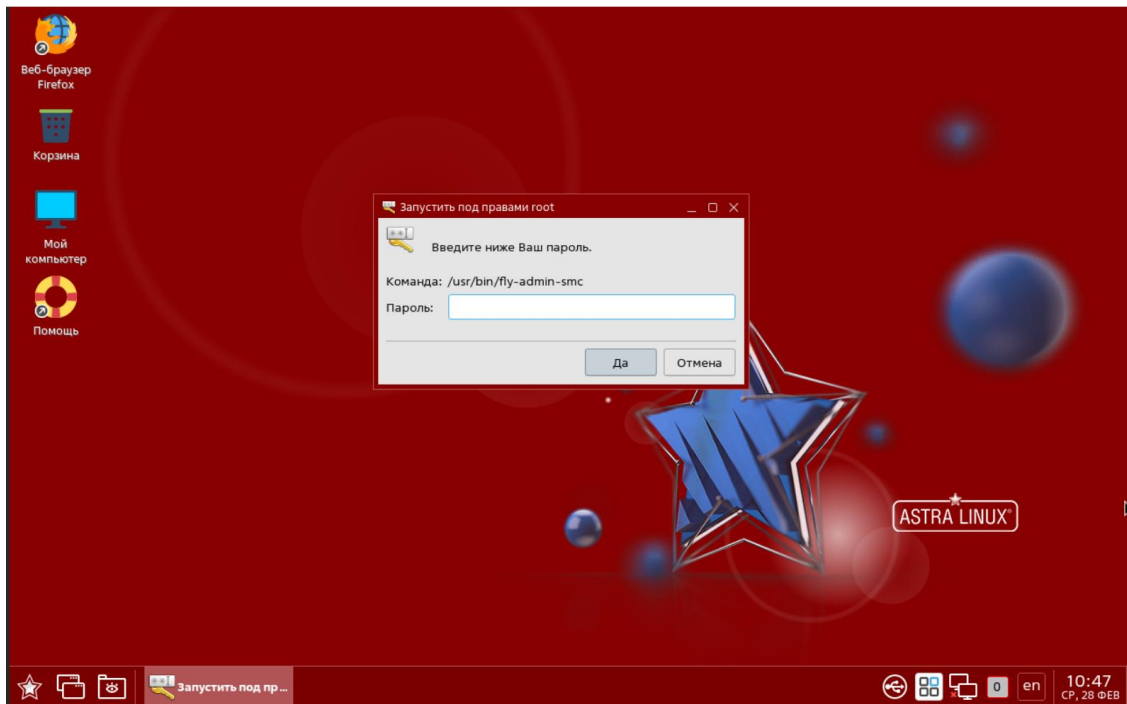


Рисунок 5 – Ввод пароля администратора ОС

- 4) Откроется окно «Управление политикой безопасности – Локальная политика» (рис. 6).

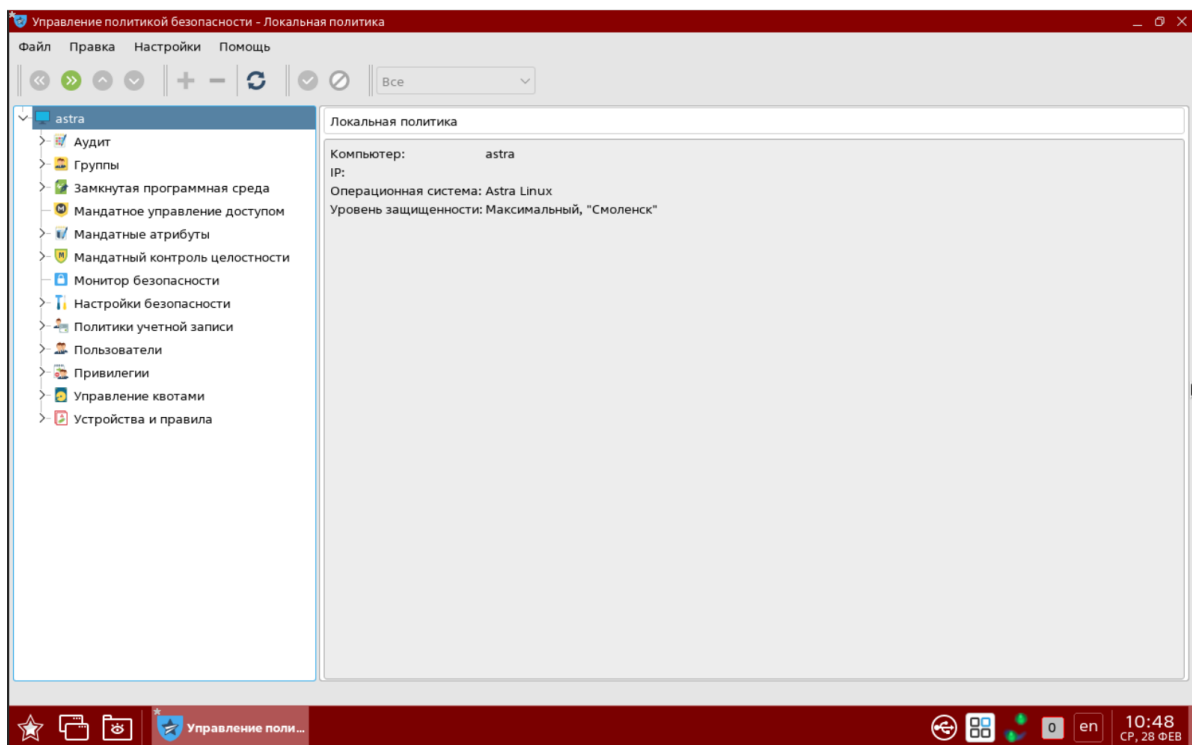


Рисунок 6 – Окно «Управление политикой безопасности – Локальная политика»

- 5) Перейти в раздел «Замкнутая программная среда» (рис. 7).

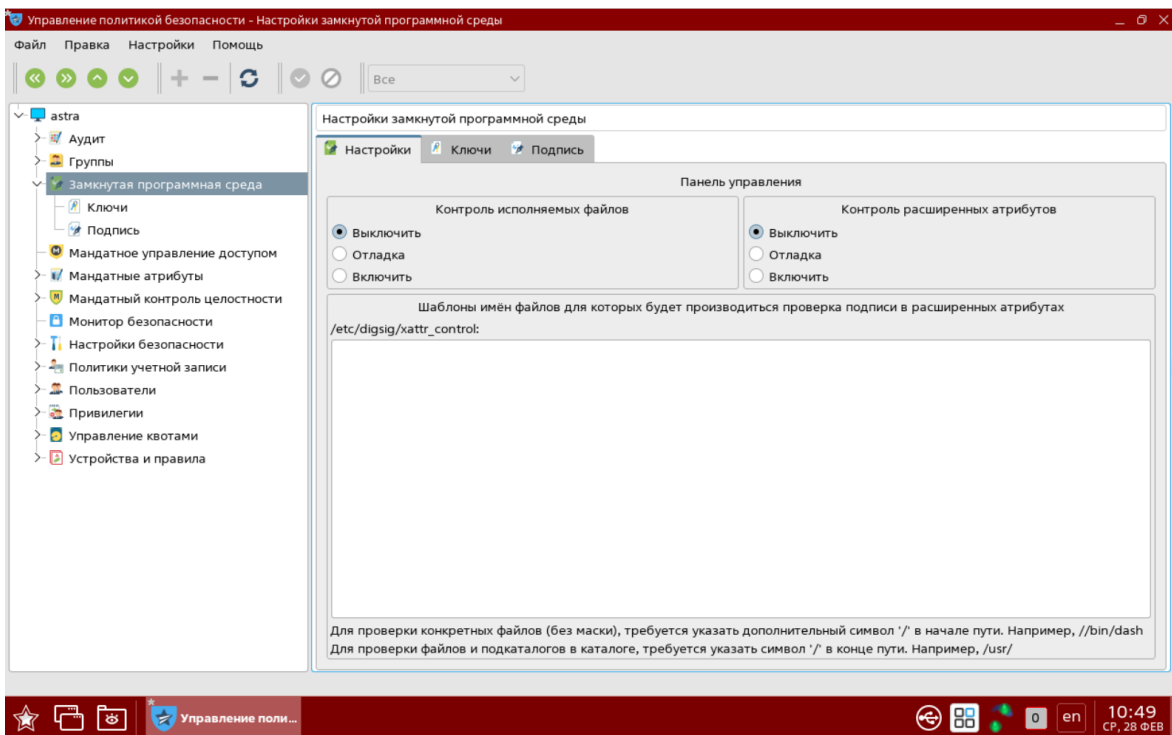


Рисунок 7 – Раздел «Замкнутая программная среда»

По умолчанию функции контроля исполняемых файлов и контроля расширенных атрибутов выключены. Необходимо 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/digisig/digisig_initramfs.conf*** – для использования отладочного режима для тестирования специального ПО параметру DIGSIG_ELF_MODE необходимо установить значение 2: ***DIGSIG_ELF_MODE=2***.

- 6) Перейти в раздел «Мандатное управление доступом» (рис. 8). Убедиться, что в поле «Подсистема Мандатного Управления Доступом» проставлен флаг.

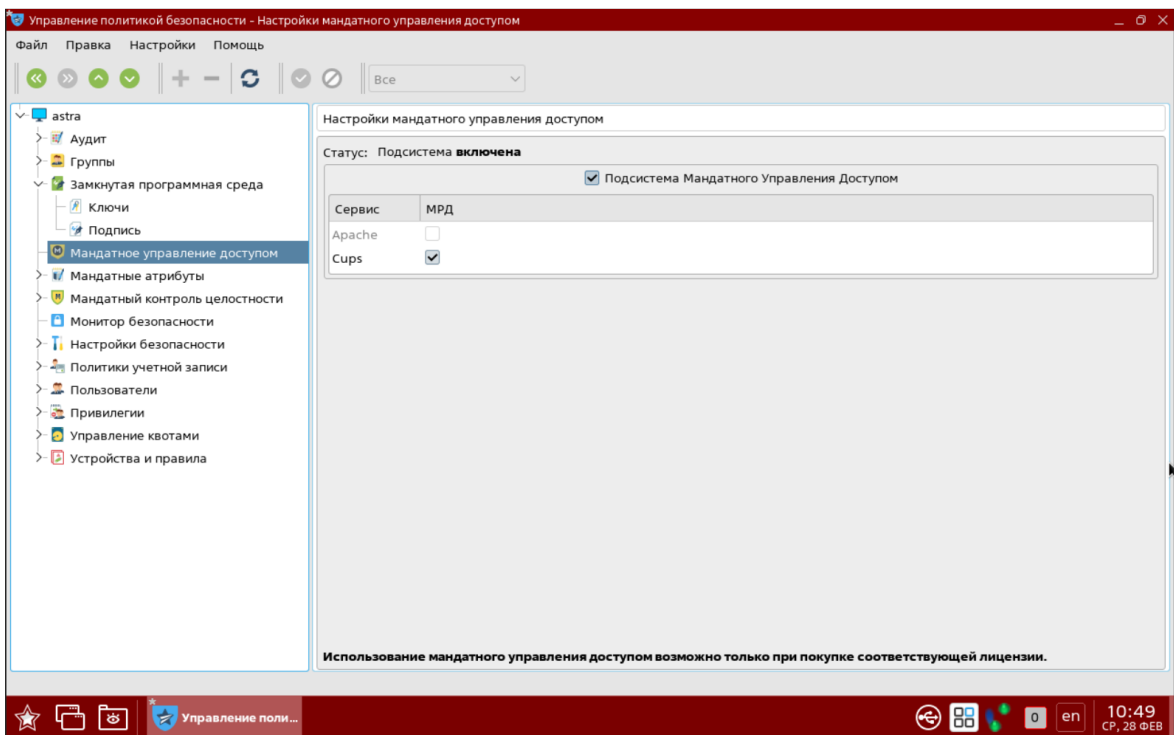


Рисунок 8 – Раздел «Мандатное управление доступом»

- 7) Перейти в раздел «Мандатный контроль целостности» (рис. 9). Убедиться, что в поле «Подсистема Мандатного Контроля Целостности» проставлен флаг.

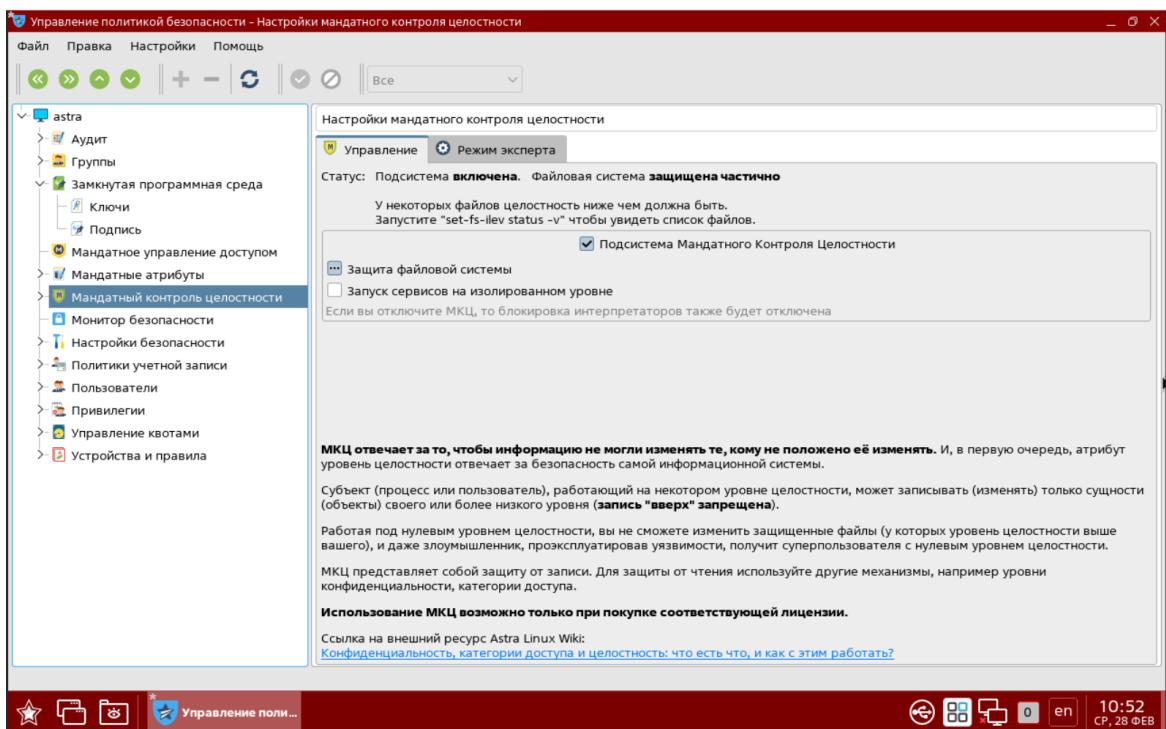


Рисунок 9 – Раздел «Мандатный контроль целостности»

- 8) Перейти в подраздел «Политика очистки памяти». Флаг в поле «Очистка разделов подкачки» должен отсутствовать (рис. 10).

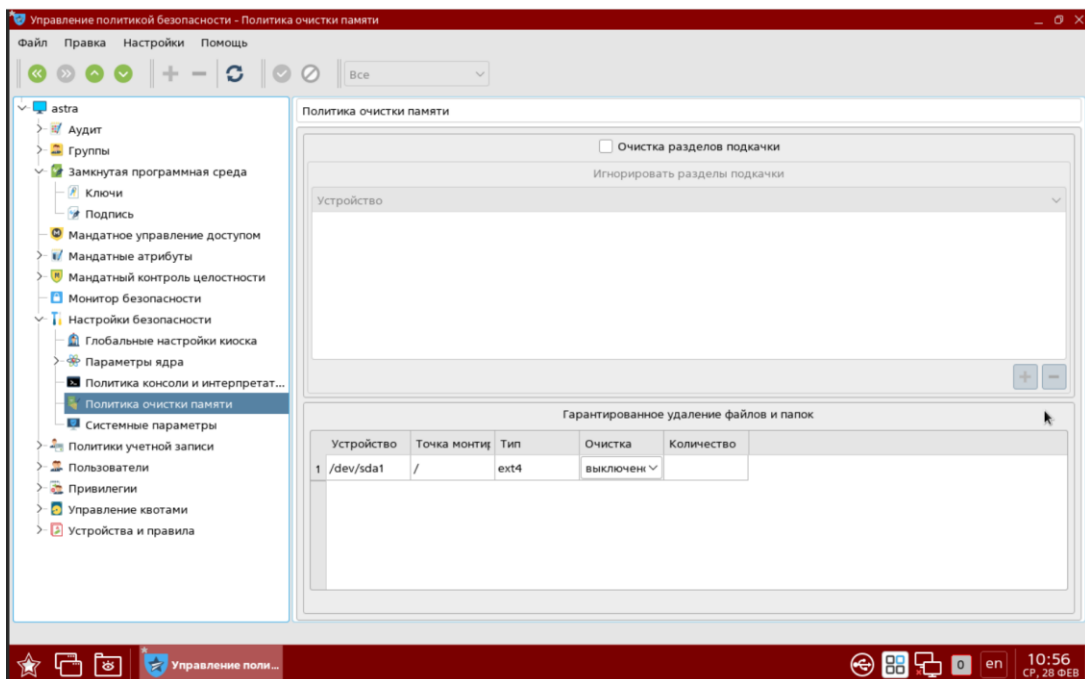


Рисунок 10 – Подраздел «Политика очистки памяти»

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

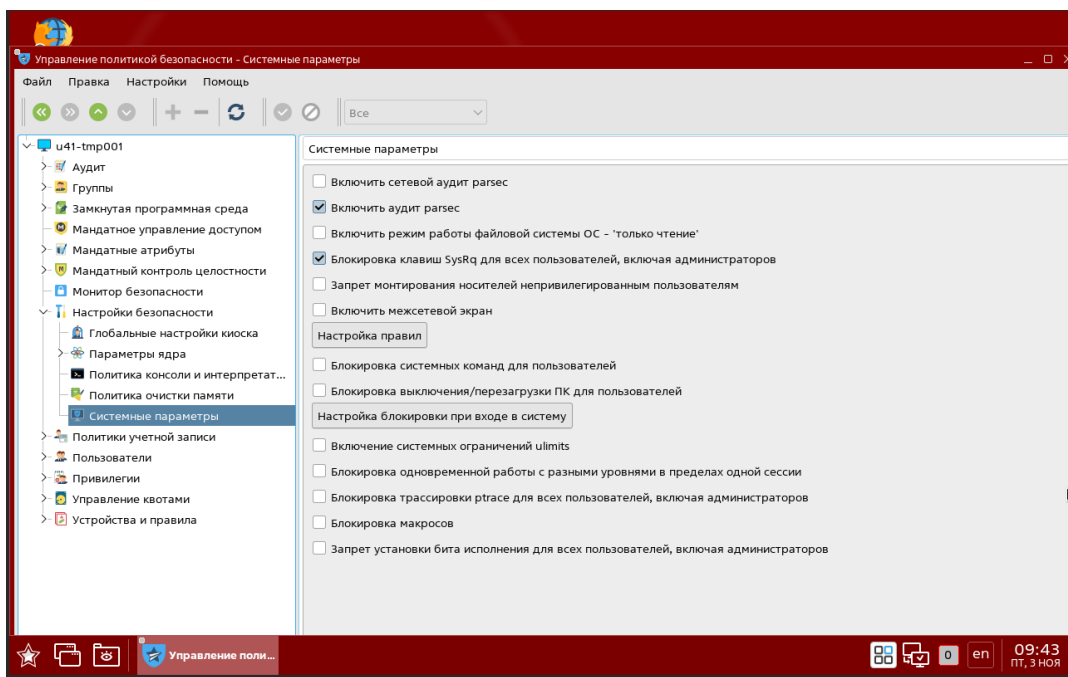


Рисунок 11 – Подраздел «Системные параметры»

Установить флаги в следующих полях:

- «Включить аудит parsec»;
- «Блокировка клавиш SysRq для всех пользователей, включая администраторов».

10) Перейти в подраздел «Политика консоли и интерпретаторов» (рис. 12).
Установить флаг в поле «Включить ввод пароля для sudo».

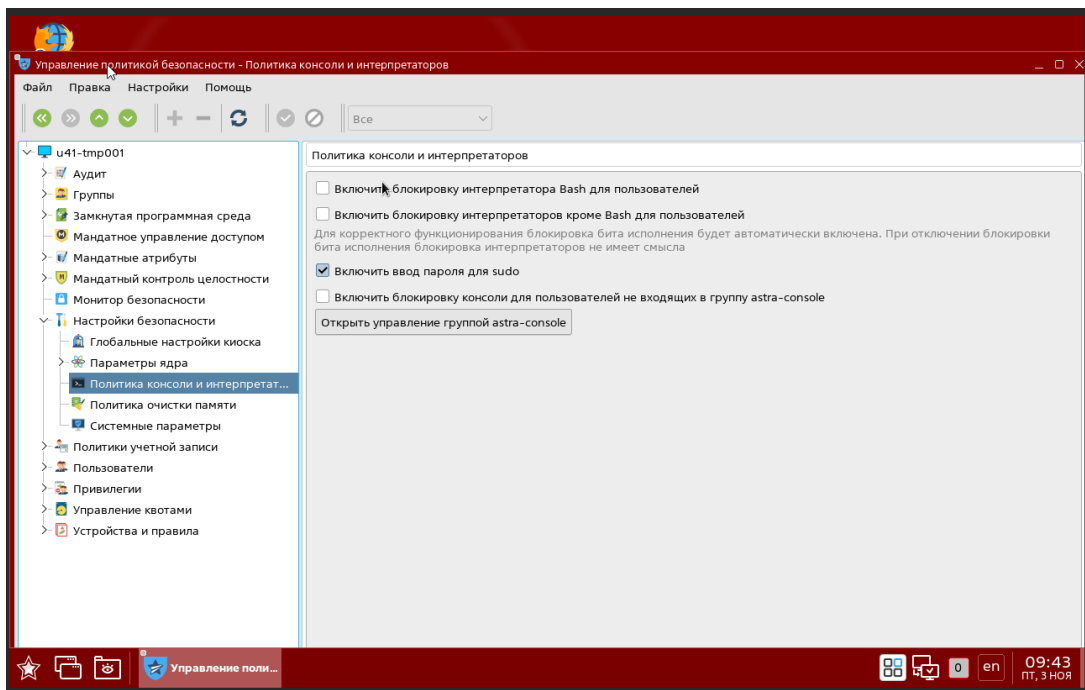


Рисунок 12 – Подраздел «Политика консоли и интерпретаторов»

11) Настройка политик безопасности для ОС Astra Linux SE тип защиты «Максимальный» («Смоленск») завершена.

3.3.2 Настройка политик безопасности ОС для типа защиты «Усиленный» («Воронеж»)

Перед установкой ПК «Efros DO» необходимо выполнить следующие настройки ОС Astra Linux SE для типа защиты «Усиленный» («Воронеж»):

- 1) После ввода логина и пароля, при выборе атрибутов безопасности для учетной записи из раскрывающегося списка необходимо выбрать уровень целостности «Высокий» (рис. 13).

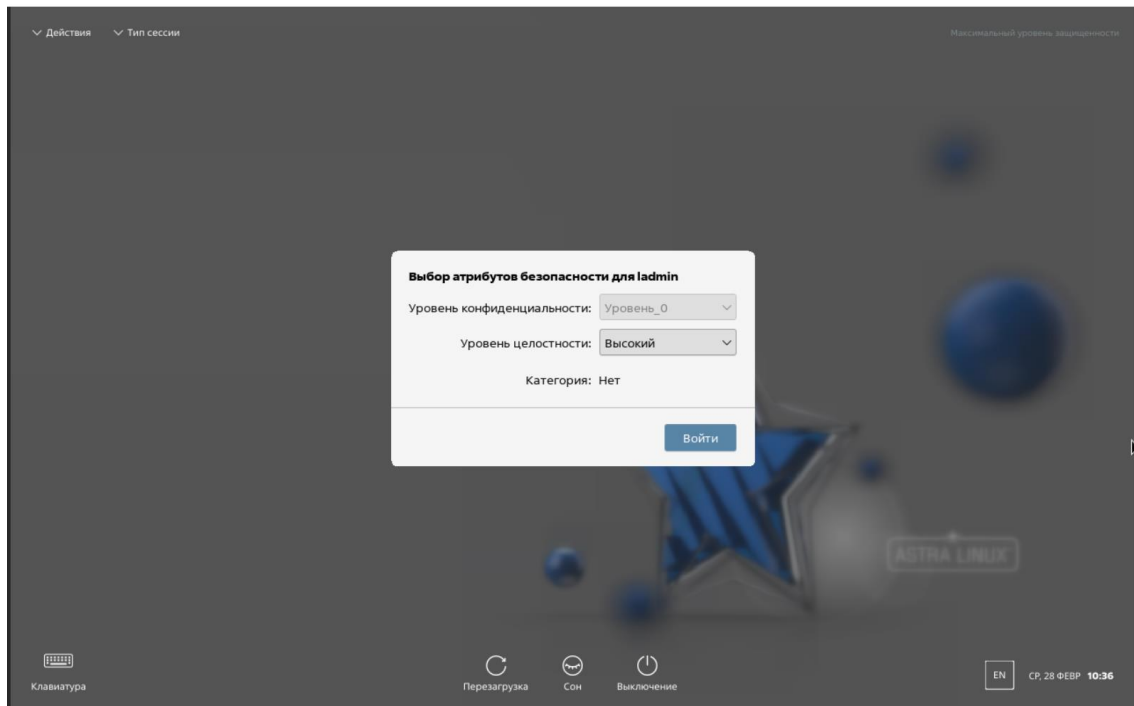


Рисунок 13 – Выбор атрибутов безопасности

2) Перейти в меню «Пуск» → «Системные» → «Политика безопасности» (рис. 14).

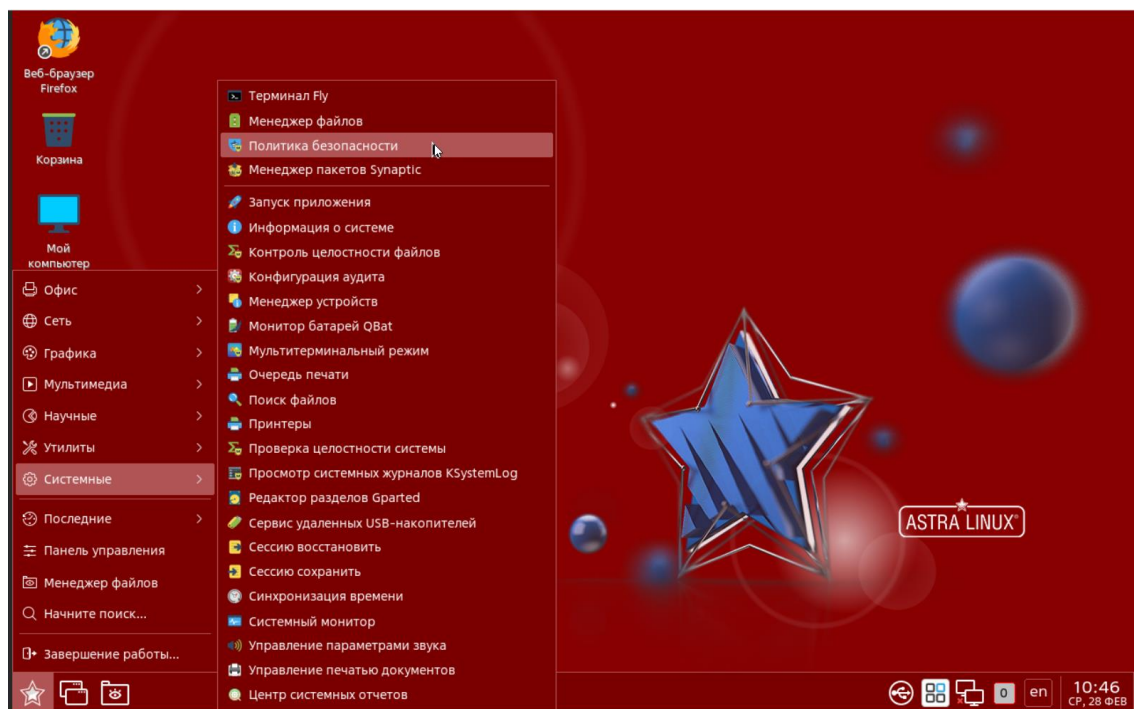


Рисунок 14 – Вкладка «Политики безопасности»

3) Ввести пароль администратора ОС (рис. 15).

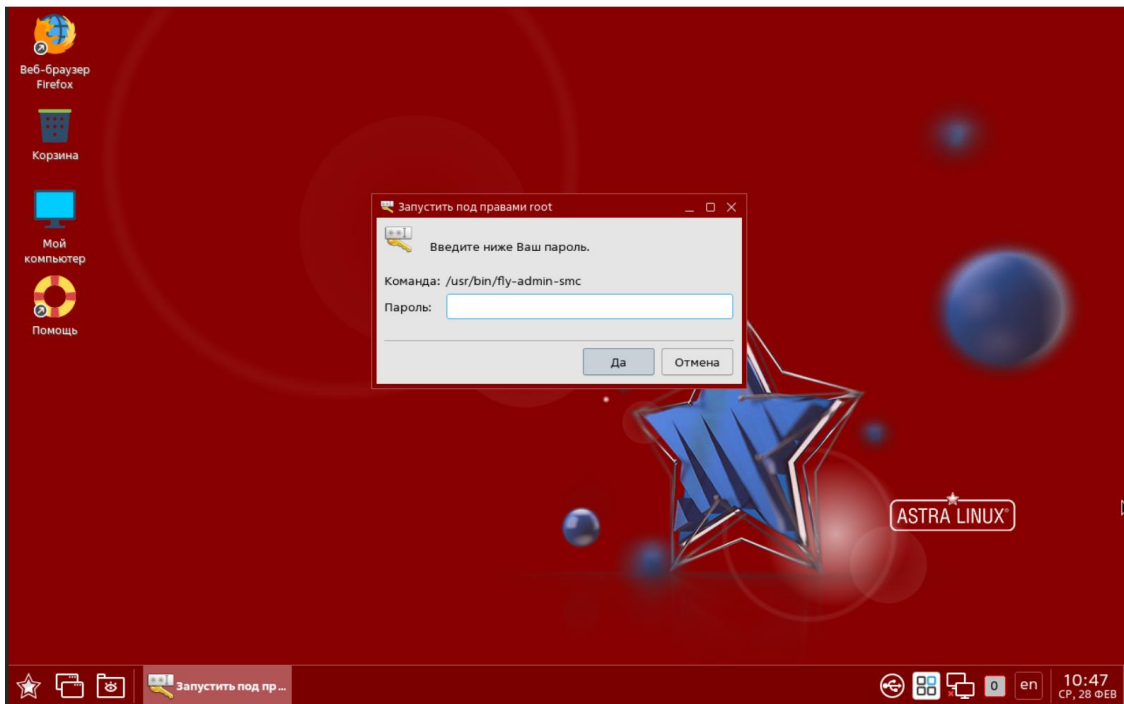


Рисунок 15 – Ввод пароля администратора ОС

- 4) Откроется окно «Управление политикой безопасности – Локальная политика» (рис. 16).

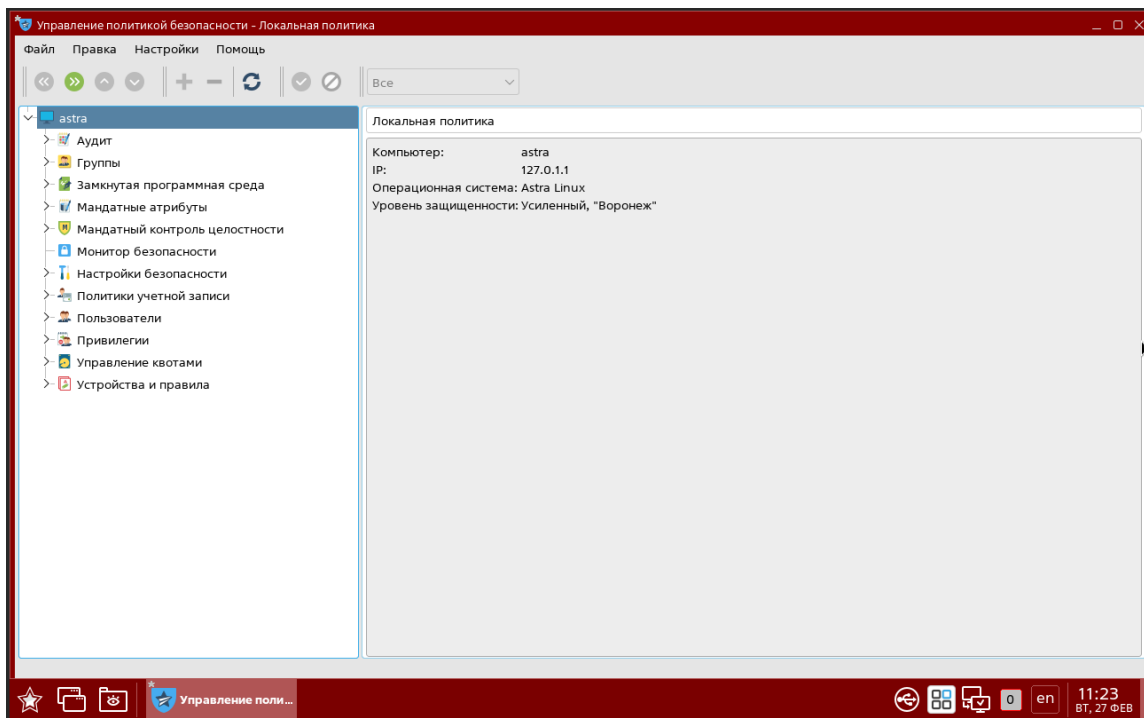


Рисунок 16 – Окно «Управление политикой безопасности – Локальная политика»

- 5) Перейти в раздел «Замкнутая программная среда» (рис. 17).

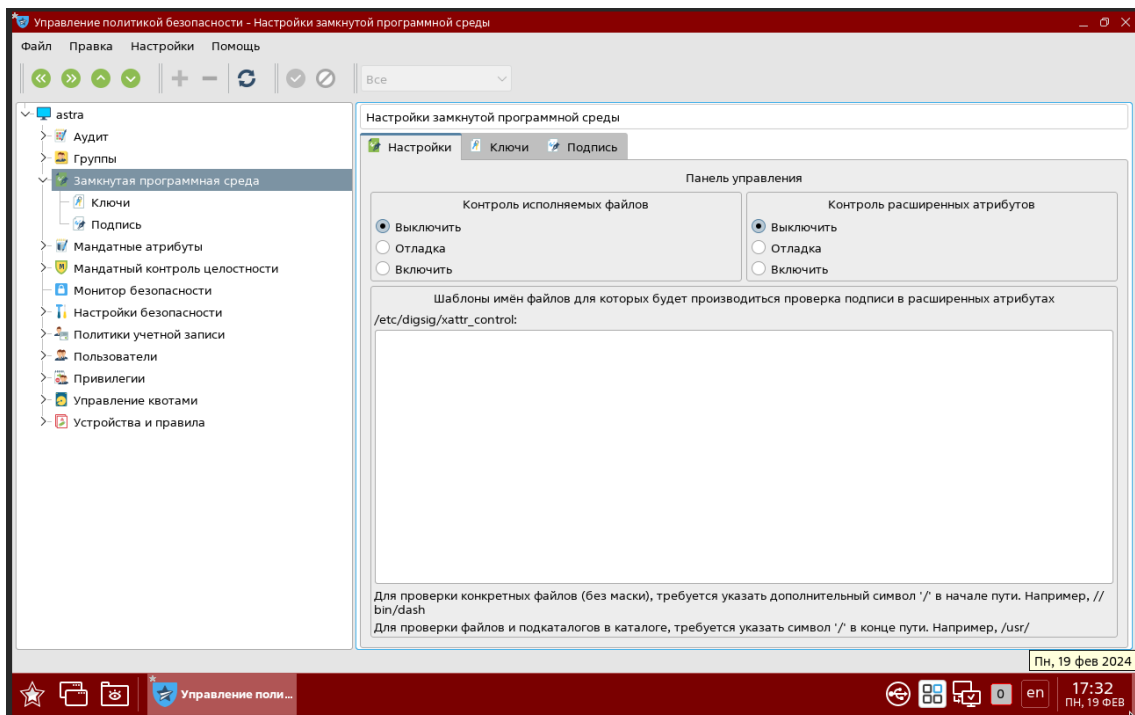


Рисунок 17 – Раздел «Замкнутая программная среда»

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 ПО параметру DIGSIG_ELF_MODE необходимо установить значение 2: **DIGSIG_ELF_MODE=2**.

6) В разделе «Мандатные атрибуты» изменять настройки не требуется.

7) Перейти в раздел «Мандатный контроль целостности» (рис. 18).

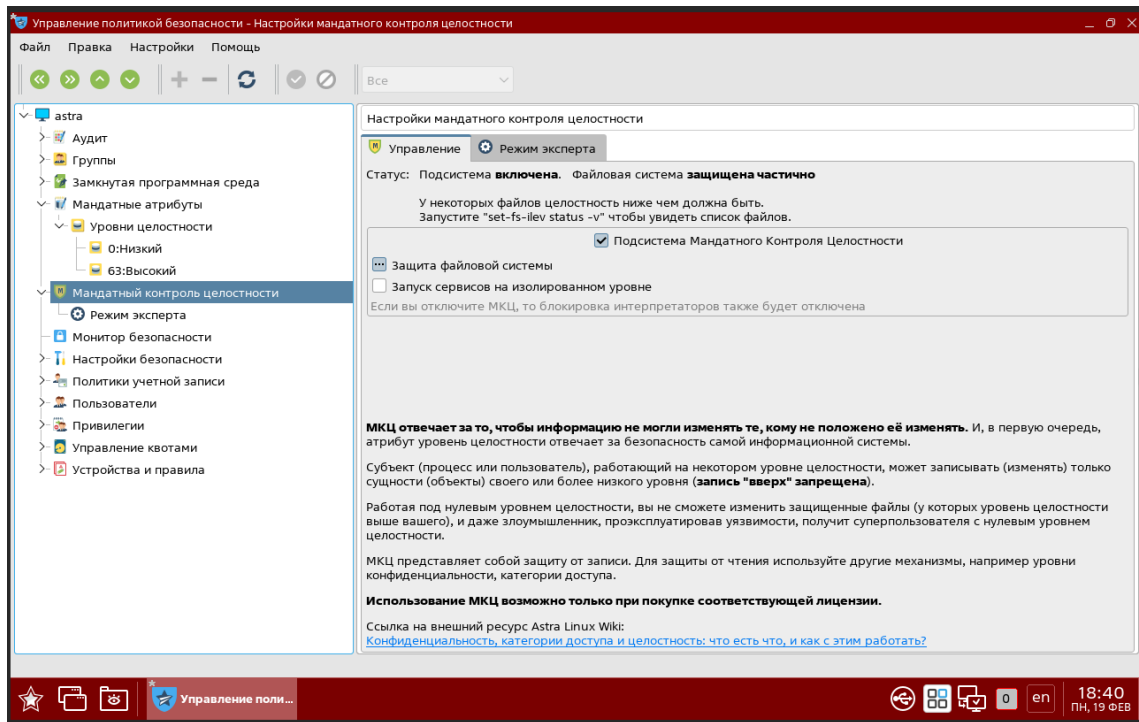


Рисунок 18 – Раздел «Мандатный контроль целостности»

Убедиться, что в поле «Подсистема Мандатного Контроля Целостности» проставлен флаг.

- 8) Перейти в подраздел «Политика очистки памяти». Флаг в поле «Очистка разделов подкачки» должен отсутствовать (рис. 19).

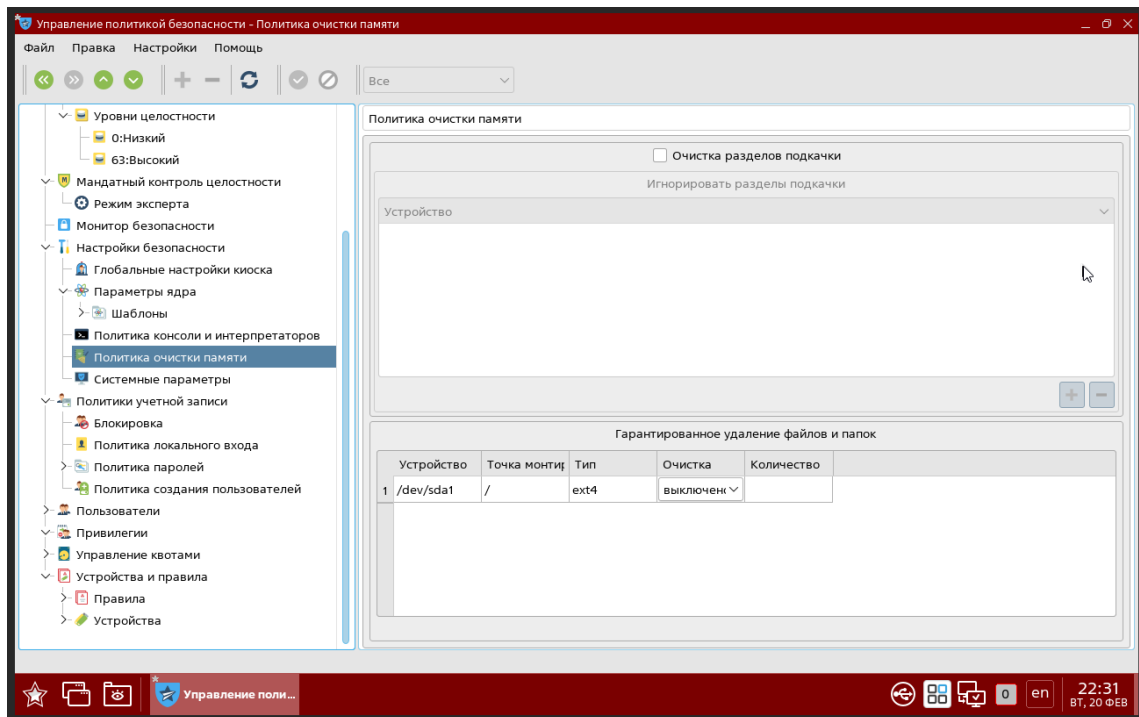


Рисунок 19 – Подраздел «Политика очистки памяти»

- 9) Перейти в подраздел «Системные параметры» (рис. 20).

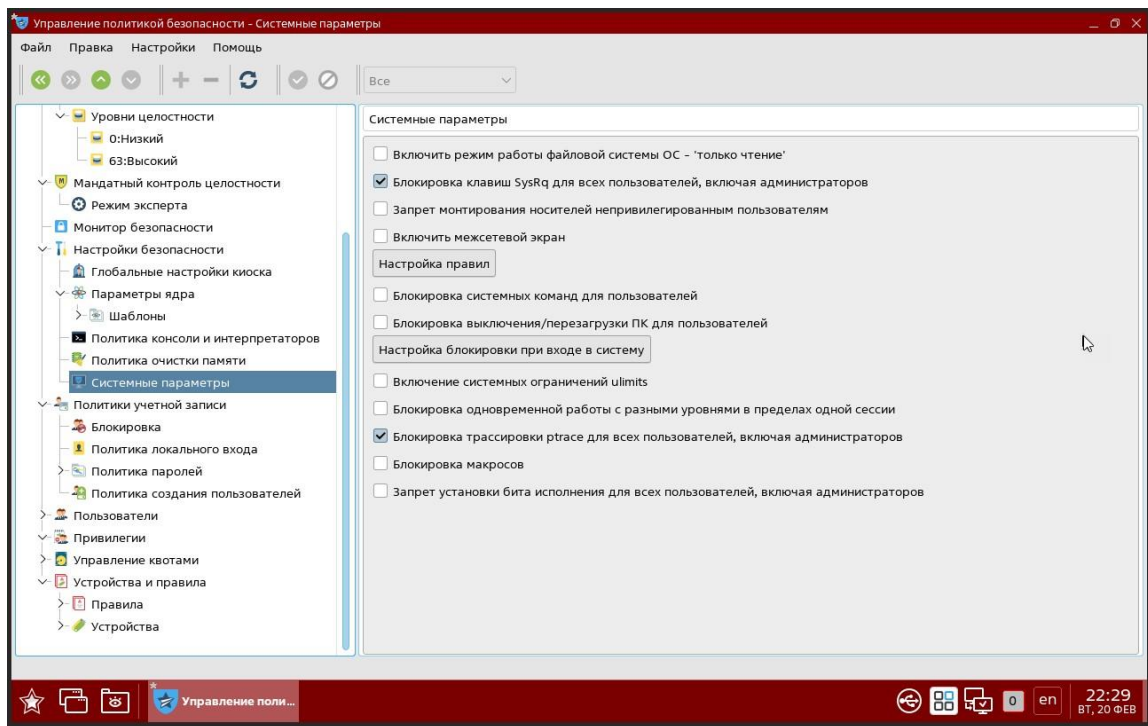


Рисунок 20 – Подраздел «Системные параметры»

Установить флаги в следующих полях:

- «Блокировка клавиш SysRq для всех пользователей, включая администраторов»;
- «Блокировка трассировки ptrace для всех пользователей, включая администраторов».

10) Перейти в подраздел «Политика консоли и интерпретаторов» (рис. 21). Установить флаг в поле «Включить ввод пароля для sudo».

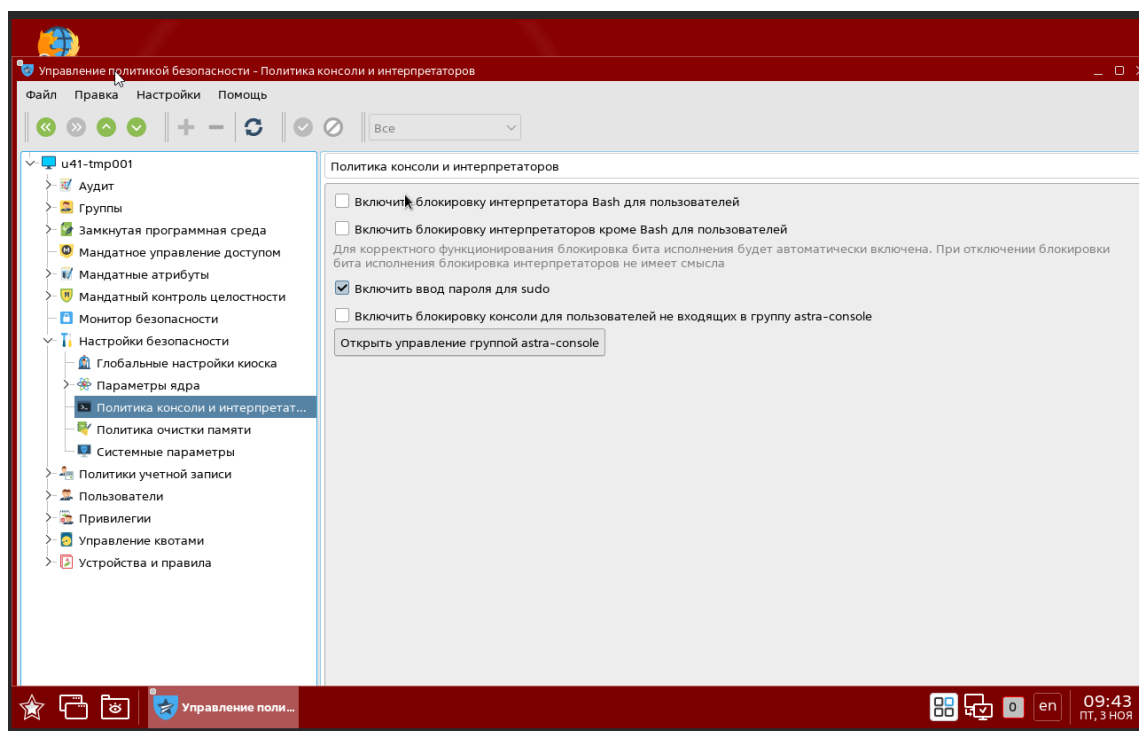


Рисунок 21 – Подраздел «Политика консоли и интерпретаторов»

11) Настройка политик безопасности для ОС Astra Linux SE тип защиты «Усиленный» («Воронеж») завершена.

3.3.3 Настройка политик безопасности ОС для типа защиты «Базовый» («Орел»)



Для ОС Astra Linux SE тип защиты «Базовый» («Орел») дополнительные настройки не требуются.

3.3.4 Установка ПК «Efros DO»

Для установки ПК «Efros DO» необходимо скопировать на ЭВМ в домашнюю директорию (например, в */tmp/distrib*) архивы и скрипт с диска, входящие в комплект поставки в соответствии с таблицей 3.

Существует два способа установки комплекса – с использованием встроенной СУБД (по умолчанию), или с подключением к внешней СУБД.

Для установки комплекса необходимо выполнить следующие действия:

-  Команды необходимо вводить от имени суперпользователя **root** либо используя команду **sudo**.
-  На некоторых операционных системах (Astra Linux Special Edition 1.7.4+, РЕД ОС 7.3.3, Альт 10 Server) в момент установки комплекса инсталляционный скрипт проверяет настройки ОС и версию **cggroups**. При необходимости, скрипт вносит изменения в конфигурацию **systctl**, после чего требуется перезагрузка ОС.

Перезагрузка ОС выполняется пользователем. После этого требуется запустить установочный скрипт еще раз.

1) Для установки комплекса:

- со встроенной БД (например, СУБД PostgreSQL) – запустить скрипт **deploy.sh** без дополнительных аргументов, с правами администратора (рис. 22);

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

Рисунок 22 – Запуск скрипта **deploy.sh** без дополнительных аргументов

- с подключением к внешней БД (например, СУБД «Jatoba») необходимо запустить скрипт с аргументом **--dbfree** (рис. 23).

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

Рисунок 23 – Запуск скрипта **deploy.sh** с аргументом **--dbfree**

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».

2) 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 24 – Процесс установки. Параметры внешней СУБД

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

3) 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. 25). 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 25 – Процесс установки. Данные для настройки внутренней сети docker

4) Установка программного комплекса завершена, при успешном завершении проверки отобразится сообщение в соответствии с рис. 26.

```
[+] 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 26 – 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. 27);
- *./edoctl --stop* – остановка всех сервисов (рис. 28);
- *./edoctl --start* – запуск всех сервисов;
- *./edoctl --restart* – перезапуск сервисов (рис. 29);
- *./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# ./doctl --ps
NAME                COMMAND                SERVICE                STATUS                PORTS
edo-acs-service     */docker-entrypoint... 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 */etc/passwd edo-email-sender-service running (healthy)     80/tcp
edo-flow-collector  */docker-entrypoint... edo-flow-collector    running               80/tcp
edo-flow-collector-dhcp */app/bin/goflow... edo-flow-collector-dhcp running               0.0.0.0:67→67/udp
edo-flow-collector-sflow */docker-entrypoint... edo-flow-collector-sflow running (unhealthy)   80/tcp
edo-flow-service     */bin/bash -c 'while...' edo-flow-service      running (healthy)     80/tcp
edo-gateway-service  */Voltron.Gateway.W... edo-gateway-service   running (healthy)     80/tcp
edo-guest-portal-service */docker-entrypoint... edo-guest-portal-service running (healthy)     5003/tcp
edo-identity-service */./SC.Identity.Api... edo-identity-service  running (healthy)     80/tcp
edo-infr-kafka       */etc/confluent/dock... edo-infr-kafka        running (healthy)     9092/tcp
edo-infr-zookeeper   */etc/confluent/dock... edo-infr-zookeeper    running (healthy)     2889/tcp
edo-knowledge-base-service */./KnowledgeBaseServ... edo-knowledge-base-service running (healthy)     80/tcp
edo-license-service  */./SC.License.Api... edo-license-service   running (healthy)     80/tcp
edo-metrics-collector */./SC.EventsCollecto... edo-metrics-collector running (healthy)     80/tcp
edo-metrics-service  */./SC.AnalyzeMetrics... edo-metrics-service   running               80/tcp
edo-proxy-service    */docker-entrypoint... edo-proxy-service     running (healthy)     0.0.0.0:443→443/tcp, 0.0.0.0:5802→5802/tcp
edo-radius           */lib/systemd/system... edo-radius            running (unhealthy)   0.0.0.0:1812-1813→1812-1813/udp
edo-report-portal-service */./Reporting.WebApi... edo-report-portal-service running (healthy)     80/tcp
edo-schedule-service */./Voltron.Schedule... edo-schedule-service  running (healthy)     80/tcp
edo-so-service       */./SC.SecurityObjec... edo-so-service        running (healthy)     80/tcp
edo-store-opensearch */./opensearch-docker... edo-store-opensearch  running (healthy)     127.0.0.1:5805→9200/tcp
edo-tacacs           */lib/systemd/system... edo-tacacs            running               0.0.0.0:49→49/tcp
edo-task-portal-service */./TaskPortal.WebApi... edo-task-portal-service running (unhealthy)   80/tcp
edo-vulnerability-collector */./SC.VulnerabilityS... edo-vulnerability-collector running (healthy)     80/tcp
edo-web-service      */./Voltron.WebApi... edo-web-service       running (healthy)     80/tcp
    
```

Рисунок 27 – Просмотр запущенных сервисов

```

root@u41ft63:/opt/efros-do# ./doctl --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 28 – Остановка всех сервисов

```

root@u41ft63:/opt/efros-do# ./doctl --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 29 – Перезапуск всех сервисов

- После установки доступен просмотр списка запущенных сервисов их состояния и параметров.

 В случае отображения неверного состояния сервисов необходимо перезагрузить комплекс. Для этого выполнить следующие шаги:

1. Остановить комплекс, выполнив команду:

```
sudo /opt/efros-do/edoctl --down
```

2. Перезагрузить docker, выполнив команду:

```
sudo systemctl restart docker
```

3. Запустить комплекс, выполнив команду:

```
sudo /opt/efros-do/edoctl --start
```

б) 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 подразделом 3.5 руководства;
- настроить ПК «Efros DO» в соответствии с руководством пользователя.

3.4 Перенастройка сети

Для настройки сетевого интерфейса docker0 и подсети, в которой работают контейнеры комплекса, необходимо выполнить следующие действия:

- 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.

3.5 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. 30), в котором необходимо указать в качестве

старого пароля значение «\$Qwerty123456», дважды указать новый пароль и нажать кнопку «Сменить пароль».



Рисунок 30 – 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. 31).

Возможны два варианта проведения активации комплекса:

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

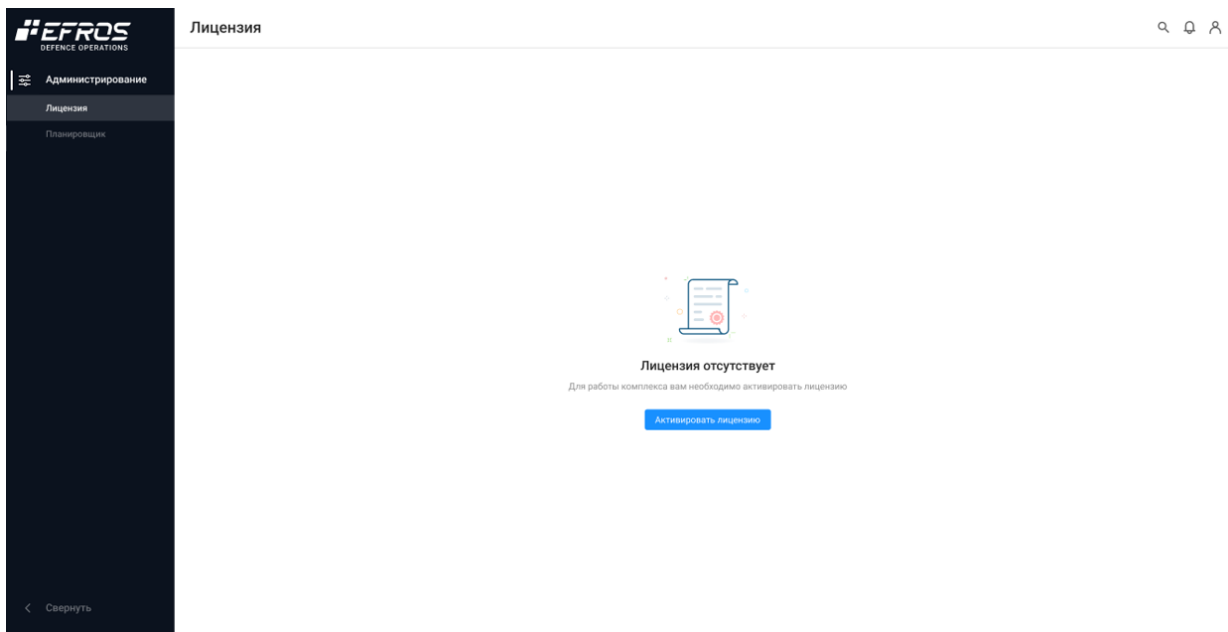


Рисунок 31 – Подраздел «Лицензия»

3.5.1 Online активация комплекса

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

Для online активации ПК «Efros DO» необходимо нажать на кнопку «Активировать лицензию» (см. рис. 31). При подключении к сети Интернет и к серверу лицензирования ООО «Газинформсервис» появится диалоговое окно (рис. 32):

- 1) В окне необходимо указать ключ лицензии, полученный при покупке комплекса.

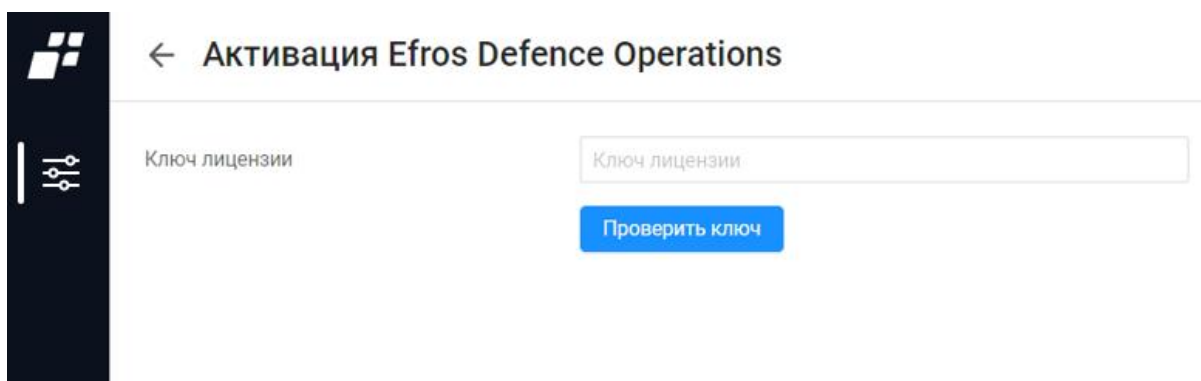
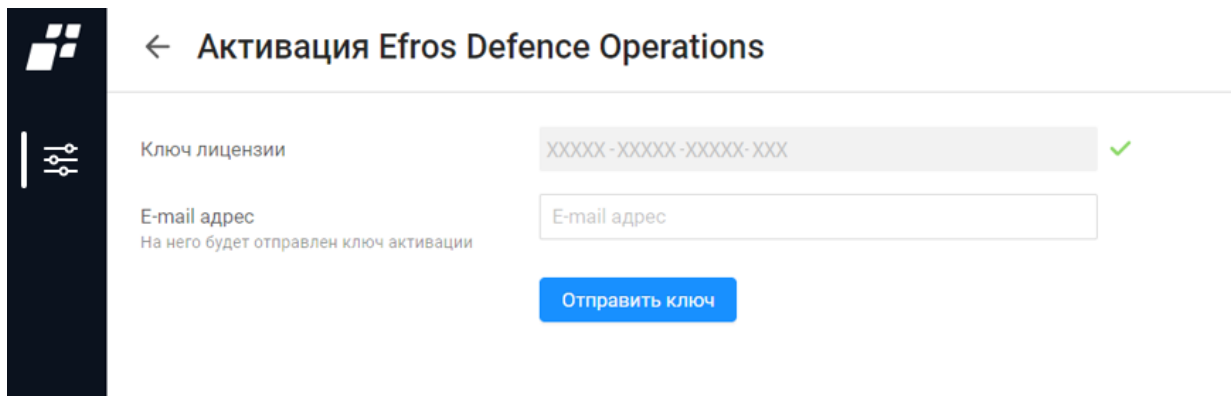


Рисунок 32 – Окно online активации комплекса. Проверка ключа

- 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. 33).



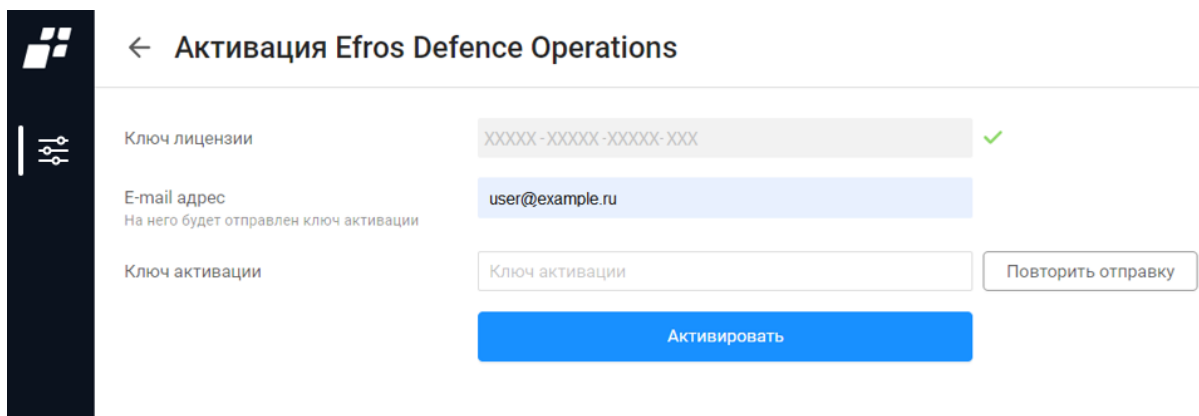
The screenshot shows a web interface for activating Efros Defence Operations. On the left is a dark sidebar with a logo and a settings icon. The main area has a title '← Активация Efros Defence Operations'. Below the title are two input fields: 'Ключ лицензии' with a placeholder 'XXXXX - XXXXX - XXXXX - XXX' and a green checkmark, and 'E-mail адрес' with a placeholder 'E-mail адрес' and a subtext 'На него будет отправлен ключ активации'. A blue button labeled 'Отправить ключ' is positioned below the email field.

Рисунок 33 – Окно online активации комплекса. Отправка ключа

4) 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. 34) и нажать кнопку «Активировать». Если ключ не был использован в течение 20 минут, то по истечении срока необходимо нажать кнопку «Повторить отправку». На указанную почту придет новое письмо с новым ключом активации лицензии.



The screenshot shows the same web interface as Figure 33, but with the 'E-mail адрес' field filled with 'user@example.ru'. A new field 'Ключ активации' with a placeholder 'Ключ активации' has been added below the email field, along with a button 'Повторить отправку'. A large blue button labeled 'Активировать' is now at the bottom of the form.

Рисунок 34 – Указание необходимых данных для активации

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

После успешного завершения активации лицензии откроется окно с данными лицензии в соответствии с рис. 35, в поле «Информация о лицензии» отобразится статус лицензии «Активная».

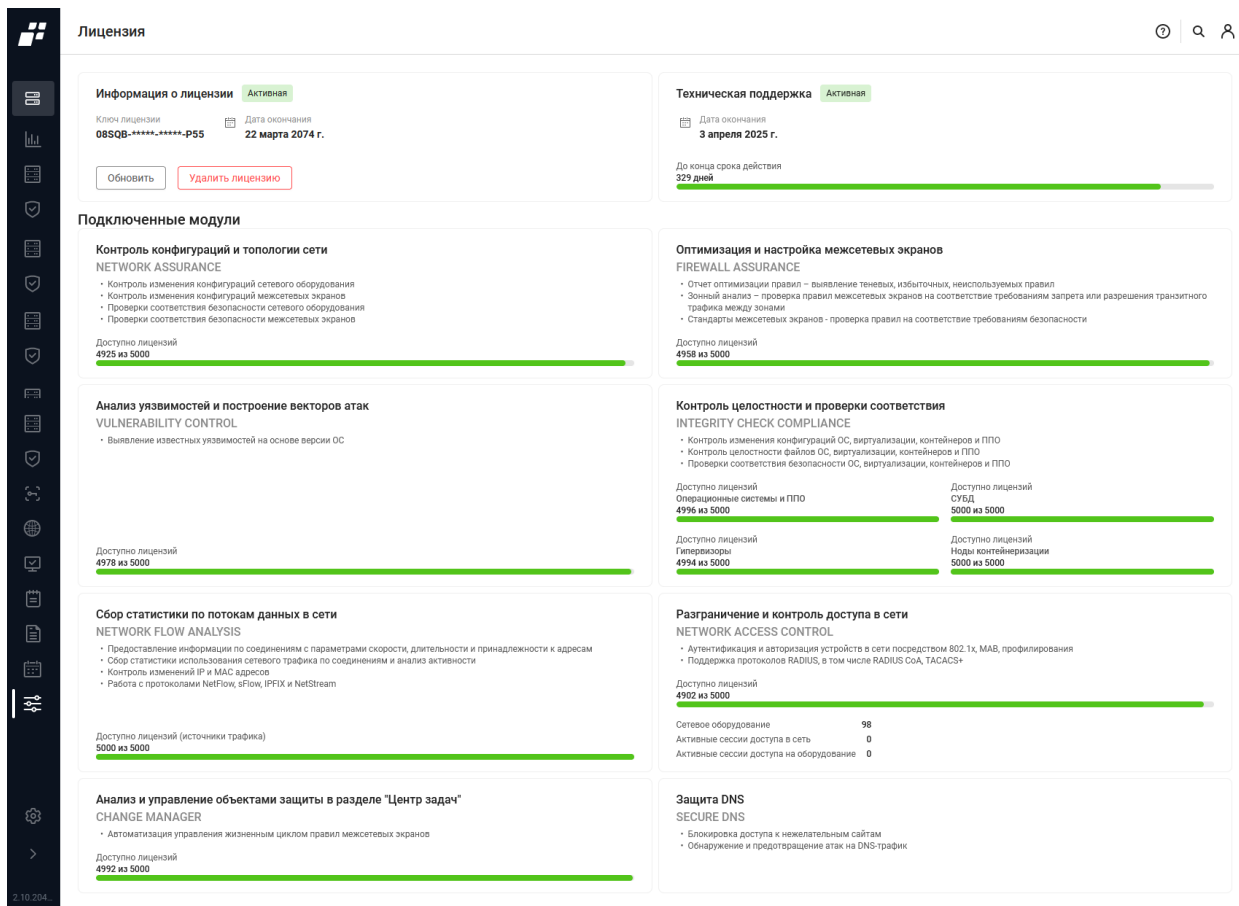


Рисунок 35 – Активация комплекса завершена

3.5.2 Offline активация комплекса

Проведение offline активации осуществляется при отсутствии подключения к сети Интернет либо если связь с сервером лицензирования ООО «Газинформсервис» не установлена. В таком случае, при нажатии кнопки «Активировать лицензию», появится соответствующее окно (рис. 36).

Для offline активации ПК «Efros DO» необходимо выполнить следующие действия:

- 1) Нажать кнопку «Активировать лицензию» (см. рис. 31). Появится диалоговое окно, приведенное на рис. 36.

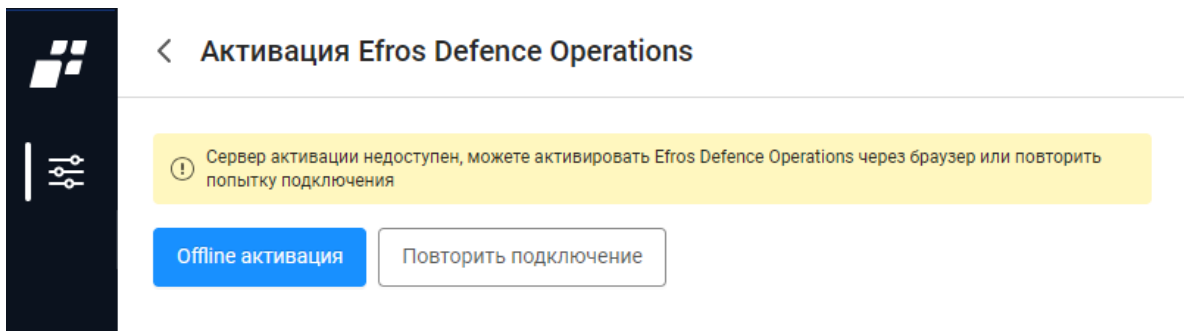


Рисунок 36 – Окно активации

- 2) Нажать кнопку «Offline активация», откроется окно ввода параметров offline активации программного комплекса (рис. 37).

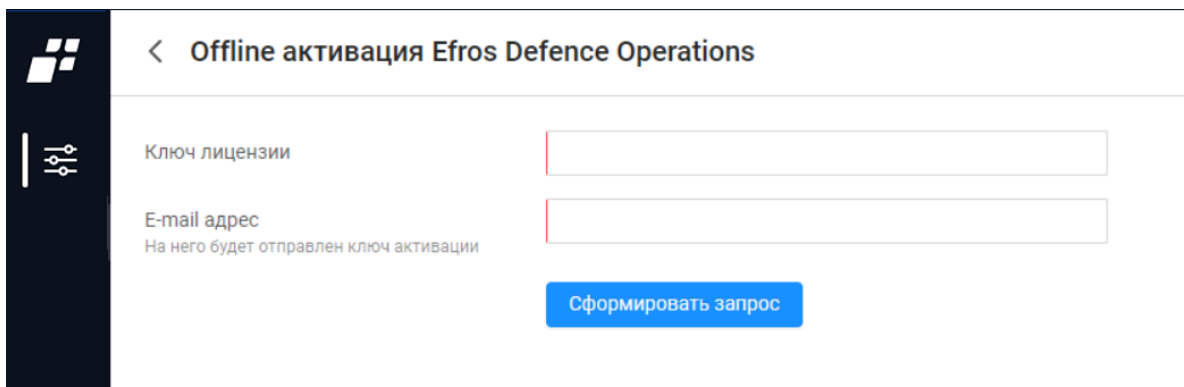


Рисунок 37 – Окно ввода параметров offline активации

- 3) 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. 38).

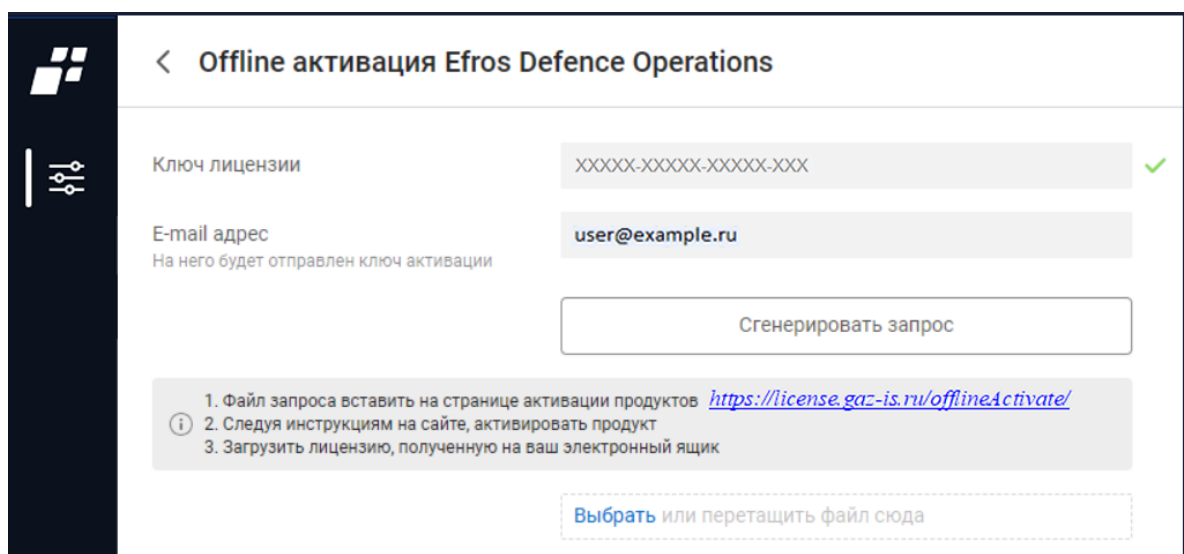


Рисунок 38 – Формирование файла с запросом на лицензию для offline активации

- 4) 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. 39).

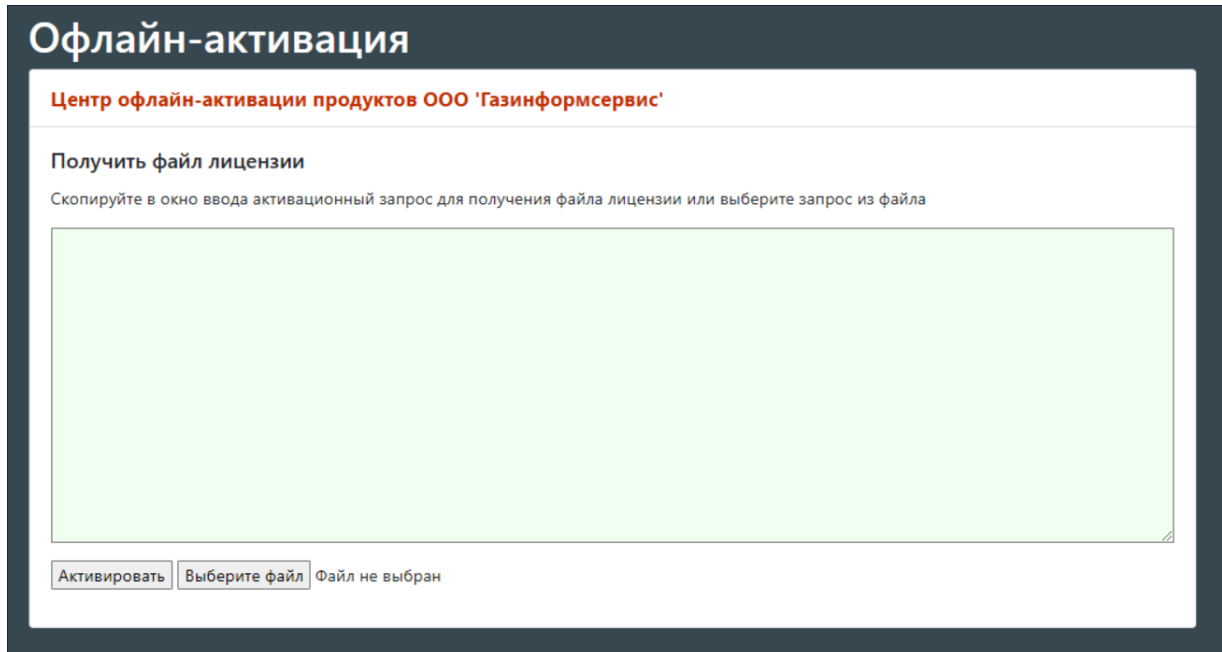


Рисунок 39 – Центр активации продуктов

- 5) Открыть ранее сгенерированный файл **request.json** и скопировать содержимое файла в соответствующее окно (см. рис. 39) либо воспользоваться кнопкой «Выберите файл», затем нажать кнопку «Активировать». Будет отправлено письмо на электронную почту, указанную для запроса, с ключом активации (рис. 40).

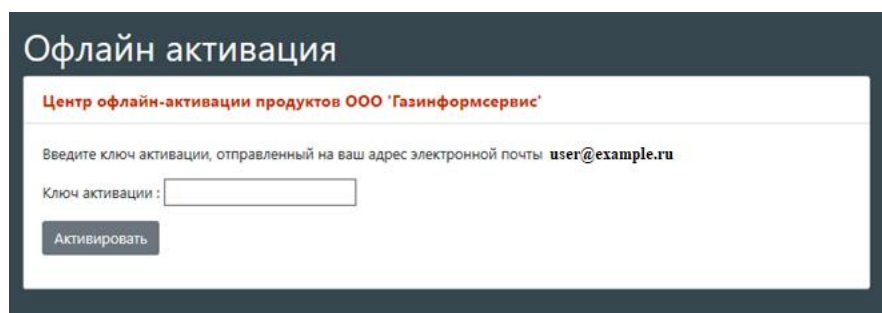


Рисунок 40 – Окно для ввода ключа активации

- 6) 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. 41).
- 7) Перейти на ЭВМ, на которой необходимо активировать комплекс, и в окне offline активации (см. рис. 38) с помощью кнопки «Загрузить лицензию», загрузить

полученный файл лицензии **license.bin**. Автоматически откроется вкладка с активированной лицензией. Offline активация комплекса завершена (рис. 42).

После успешного завершения активации лицензии откроется окно с данными лицензии в соответствии с рис 42, в поле «Информация о лицензии» отобразится статус лицензии «Активная».

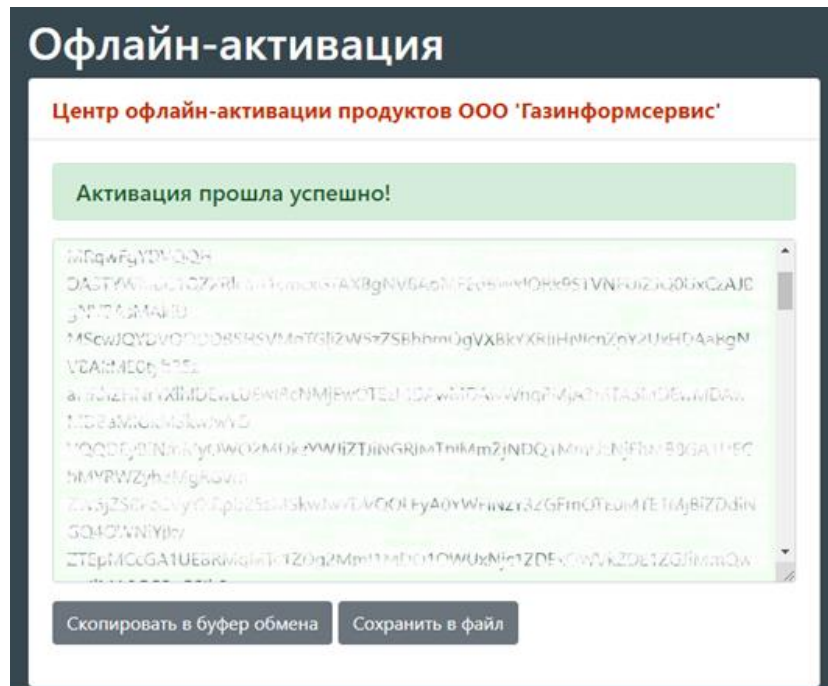


Рисунок 41 – Успешное прохождение активации

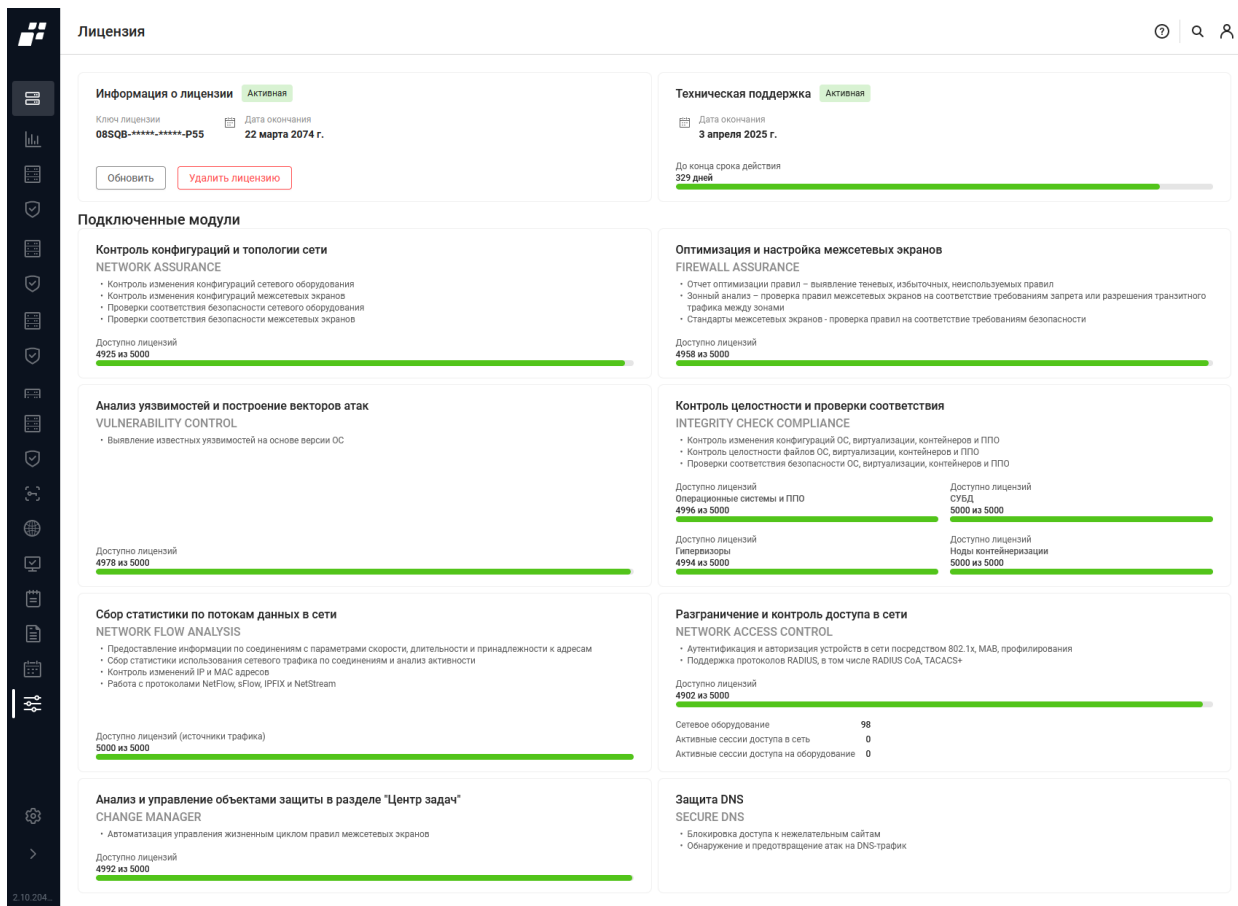


Рисунок 42 – Завершение прохождения offline активации

3.5.3 Реактивация лицензии комплекса

Для осуществления переноса лицензии необходимо после установки комплекса на другую ЭВМ, выполнить следующие действия:

- 1) Перейти в диалоговое окно активации комплекса (Администрирование/Лицензия) и указать ключ лицензии, полученный при покупке комплекса. Нажать кнопку «Активировать лицензию», появится сообщение в соответствии с рис. 43.

Активация Efros Defence Operations

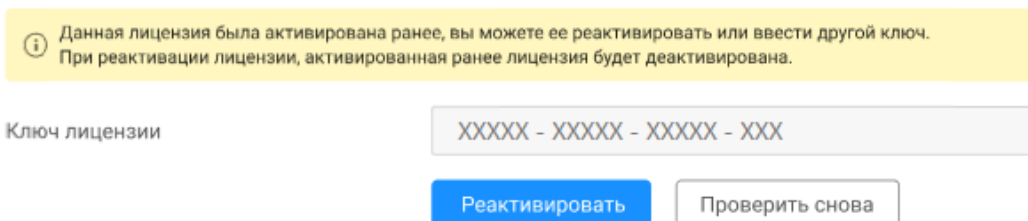

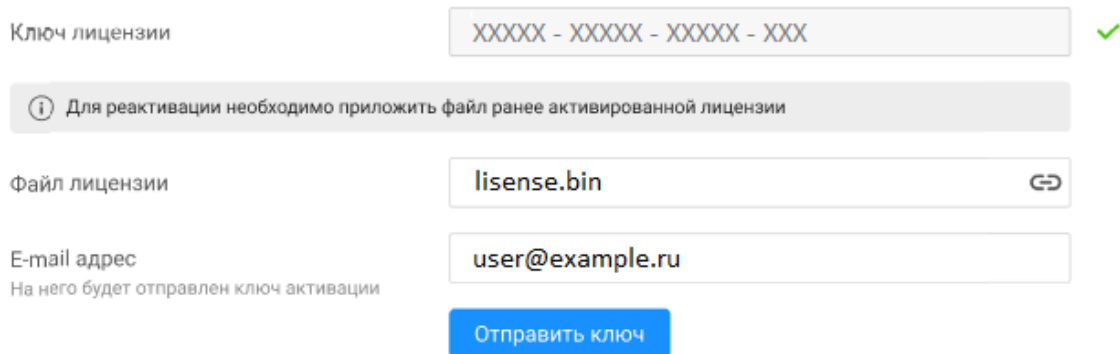




Рисунок 43 – Повторная активация лицензии


- 2) Нажать кнопку «Реактивировать». При наличии устойчивого подключения к сети Internet, дальнейшая активация комплекса осуществится online. При успешном завершении проверки введенного ключа активации напротив поля появится галочка «».

← Активация Efros Defence Operations





Ключ лицензии 

 Для реактивации необходимо приложить файл ранее активированной лицензии

Файл лицензии 

E-mail адрес
На него будет отправлен ключ активации

Рисунок 44 – Ввод данных

- 3) Приложить файл **license.bin**, который был получен ранее при активации комплекса на другой ЭВМ.
 - 4) Указать электронную почту и нажать кнопку «Отправить ключ» (см. рис. 44).
-  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».
- 5) На указанный адрес электронной почты будет отправлен ключ активации продукта.
-  Активацию комплекса необходимо провести в течение 20 минут после формирования запроса на активацию (рис. 45).
- 6) Ввести ключ активации, полученный по электронной почте, в соответствующее поле (см. рис. 45) и нажать кнопку «Активировать». Перенос ключа активации лицензии завершен.

← Активация Efros Defence Operations

Ключ лицензии XXXXX - XXXXX - XXXXX - XXX ✓

ⓘ Для реактивации необходимо приложить файл ранее активированной лицензии

Файл лицензии lisense.bin ↗

E-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 45 – Ввод ключа активации

Реактивация лицензии возможна также в offline режиме. Алгоритм действий аналогичен проведению offline активации комплекса (см. п.3.5.2).

3.6 Удаление изделия

Для удаления приложения необходимо выполнить одну из следующих команд:

- команду **edoctl --uninstall** для частичного удаления комплекса (без потери БД) (рис. 46);
- команду **edoctl --purge-all** для полного удаления комплекса (рис. 47).

В процессе удаления на экране будет отображаться информация об удалении файлов и каталогов в соответствии с рисунками 48, 49.

```
root@u41ft66:/opt/efros-do# edoctl --uninstall
```

Рисунок 46 – Запуск команды для частичного удаления

```
root@u41ft66:/opt/efros-do# edoctl --purge-all
```

Рисунок 47 – Запуск команды для полного удаления

```
Хотите продолжить? [Д/Н]
(Чтение базы 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-acs-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-acs-service, edo-identity-service, edo-ci-service, edo-flow-service, edo-flow-collector-sflow, edo-flow-collector, e
do-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           ...
Removing edo-metrics-service     ...
Removing edo-web-service          ... done
Removing edo-tacacs              ... done
Removing edo-radius               ... done
Removing edo-acs-service          ... done
Removing edo-identity-service     ...
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 48 – Процесс удаления файлов и каталогов

```
Deleted: sha256:688f65ce3a33d5aae47eb089c6f608c4026364ddaba08f87f9f94b4c22b995dc
Deleted: sha256:291f6e44771a7b4399b0c6fb40ab4fe0331ddf76eda11080f052b003d96c7726
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: sha256:7d3ffff76bebeec000934e06652b732d8af9e94a6770e7f603dc538da3e139472
Deleted: sha256:f642031e18cfbb570bfff4d1a12665f8cea1e7601de8bf2f8335ce49bba2b5222
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: sha256:124ff6469e3d01eb72c58afa0668a5a19f7bf0318355e98847a4b4e28fcddeba
Deleted: sha256:7c1b2a63d63d4e8a4bc26812347923d30df54e09fd069ba09633cdc590e6fd37
Deleted: sha256:cf7c6836cab0ee5a22bf97d37d3cc5ba22658f8248de66d9e045bbb3ed4fcb
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 49 – Процесс удаления файлов и каталогов (продолжение)

3.7 Кластеризация

ПК «Efros DO» работает в режимах геораспределенного и отказоустойчивого кластера, то есть распределенной ИТ-инфраструктуры на базе нескольких территориально удаленных дата-центров.

Такое решение позволяет обеспечить высокую надежность работы комплекса, который сохраняет работоспособность даже в случае выхода из строя одного из дата-центров.

Если один сервер кластера выходит из строя, остальные серверы автоматически перенимают его функции, обеспечивая надежный и бесперебойный доступ к ресурсам и данным.

При восстановлении работоспособности сервера происходит согласование серверов кластера, службы ПК «Efros DO» и кластер продолжают работать в штатном режиме. Кластерная версия ПК «Efros DO» выполнена на базе kubernetes-инфраструктуры.





 Кластерная версия ПК «Efros DO» поставляется по запросу.

В таблице 5 приведены технические требования к кластерной версии ПК «Efros DO».

Таблица 5 – Технические требования к кластерной версии ПК «Efros DO»


Поле	Параметр		
Количество серверов со специальным ПО (нодов)	3		
Требования к ПО			
ОС	Astra Linux Special Edition (v. 1.7.4) РЕД ОС (v. 7.3)		
Поддерживаемые СУБД	СУБД Jatoba (v. 5.4.1); СУБД PostgreSQL 13; компонент jaDog (v.2.1.0)		
Прикладное ПО	Confluent Kafka (v. 5.5.0); OpenSearch (v. 1.3.7); Kubernetes (v. 1.27); Metallb (v. 4.5.1); NGINX Ingress Controller (v. 4.8.3)		
Требования для кластера Kubernetes			
Подключение	Порт	Протокол	Направление
Сервер NTP	123	udp	в обе стороны
Связь между нодами	6443	tcp	входящий
Плагин Flannel	8285	udp	входящий
Внешнее подключение (порт относится к виртуальному IP-адресу)	8443	tcp	входящий
kube-apiserver, etcd	2379-2380	tcp	входящий
Kubelet API	10250, 10256	tcp	входящий
kube-scheduler	10259	tcp	входящий
kube-controller-manager	10257	tcp	входящий
NodePort Services	30000-32767	tcp	входящий
Требования к аппаратному обеспечению для одного нода			
Процессор	16 ядер (от 2 ГГц)		
Оперативная память	32 Гб (64)		
Жесткий диск	100 Гб SSD для внешней базы; 300 Гб SSD для внутренней базы		
Сетевая карта	1 Гбит/с		
Требования к аппаратному обеспечению для кластера СУБД			
Количество дата-центров	2		
Количество нодов в дата-центре	2		
Требования к аппаратному обеспечению для одного нода в дата-центре			
Процессор	16 ядер (от 2 ГГц)		
Оперативная память	32 Гб (64)		

Поле	Параметр
Жесткий диск	100 Гб SSD для внешней базы; 300 Гб SSD для внутренней базы
<p>Дополнительные требования:</p> <ol style="list-style-type: none"> 1. Требования для функциональных модулей, Windows-агента, агента ПК «Efros DO» и суппликанта ПК «Efros DO» приведены в таблице 2. 2. Для доступа к кластеру СУБД извне необходимо открыть порт tcp 5432 в обе стороны между кластером СУБД (каждой виртуальной машины (VM)) и комплексом. 3. Для корректной работы Healthcheck необходимо открыть порт tcp 54321 в обе стороны между кластером БД (каждой VM) и комплексом. 4. Для корректной работы кластера необходимо открыть порты tcp 12345, 54321, 5432 между VM кластера (в т.ч. между подсетями различных дата-центров), udp 12346. 5. Для организации отказоустойчивости используется keepalived, в основе которого используется протокол VRRP. Данному протоколу необходим доступ с нод 1 и нод 3 до 224.0.0.18 зарезервированного IP-адреса, который используется для multicast передачи пакетов 	

-  Установка кластера ПК «Efros DO» происходит на 3 VM (нод 1, нод 2, нод 3).
-  Запускать установку необходимо с отдельного хоста. Требования:
 - ОС Astra Linux (v. 1.7.4) доступ по SSH к нод 1 – 3, 40 Гб места на диске. После установки данная нода не будет использоваться, все файлы с нее разрешается удалить;
 - РЕД ОС (v. 7.3) доступ по SSH к нод 1 – 3, 40 Гб места на диске. После установки данная нода не будет использоваться, все файлы с нее разрешается удалить.
-  Скрипты необходимо запускать с правами администратора.
-  Кластерная версия ПК «Efros DO» устанавливается на чистую ОС. При выполнении процедуры обновления кластерной версии комплекса необходимо предварительно удалить старую версию комплекса со всех используемых VM, а также выполнить удаление БД комплекса (внутренней и внешней).
Порядок удаления кластера для Astra Linux SE приведен в п. 3.7.1.4 документа, для РЕД ОС – в п. 3.7.2.3.


3.7.1 Кластеризация на Astra Linux SE

3.7.1.1 Предварительные настройки

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

Перед установкой кластера необходимо выполнить следующие шаги по настройке:

- 1) Определить **hostname edo-cluster-{номер ноды}**, например: edo-cluster-1, edo-cluster-2, edo-cluster-3.

 Идентификатор **hostname** должен быть задан буквами нижнего регистра (строчными буквами).

- 2) Для каждого хоста задать статический IP-адрес. Это можно сделать в файле **/etc/network/interfaces**. Пример приведен ниже:

```
auto eth0
iface eth0 inet static
    address 10.116.41.43/24
    gateway 10.116.41.1
    dns-nameservers 10.116.1.111
```

- 3) Далее выполнить команду:

```
systemctl restart networking.service
```

- 4) Необходимо выделить один IP-адрес, который будет использоваться как виртуальный. Адрес не должен быть привязан к какому-либо хосту и находиться в той же подсети, что и хосты.



- 5) Должно быть однозначное сопоставление IP-адреса и **hostname**. Если хосты не добавлены в **dns**, то это можно сделать в файле **/etc/hosts**. Пример файла для хоста **edo-cluster-1** с IP-адресом 10.116.41.43 приведен ниже:

```
127.0.0.1    localhost
127.0.1.1    edo-cluster-1
10.116.41.43 edo-cluster-1
```



```
10.116.41.44 edo-cluster-2
10.116.41.45 edo-cluster-3
```

3.7.1.2 Установка кластера

-  Рекомендуется проводить установку кластера с отдельного хоста, который будет находиться в той же подсети, что и хосты будущего кластера. А также иметь к ним доступ по SSH.
-  Команды необходимо вводить от имени суперпользователя **root** либо используя команду **sudo**.

Для установки кластера необходимо выполнить следующие шаги:

- 1) Распаковать архив **efros-do-cluster.tar.gz** в произвольную директорию следующей командой:

```
mkdir -p /opt/distr && tar -xvf efros-do-cluster.tar.gz -C
/opt/distr
```

- 2) Перейти в каталог с распакованными файлами и отредактировать файлы **.env** и **inventory**, используя образцы **.env.example**, **inventory.example**:

```
cd /opt/distr
cp -v .env.example .env
cp -v inventory.example inventory
```

- 3) Определить переменные, связанные с адресами нод и именами учетных записей для доступа к ним с помощью редактора **nano**:

— файл **inventory**:

- отредактировать значения **ansible_host** (IP-адрес основного интерфейса eth0), **ansible_user**, **ansible_become_pass** не меняя структуру файла. Пример приведен ниже:

```
[master]
master_1  ansible_host=10.100.200.101  ansible_user=admin
ansible_become_pass=MySudoPassword
```


```
master_2  ansible_host=10.100.200.102  ansible_user=admin
ansible_become_pass=MySudoPassword
master_3  ansible_host=10.100.200.103  ansible_user=admin
ansible_become_pass=MySudoPassword

[all:vars]
ansible_connection=ssh
ansible_private_key_file=/root/.ssh/id_rsa
```

— файл *.env*:

- в блоке «High Ability Settings» задать виртуальный IP-адрес для **Control Plane** в переменной **CONTROL_PLANE_IP** и имя сетевого интерфейса в переменной **KEEPALIVED_INTERFACE**. Пример приведен ниже:


```
#=====
#-----HIGH ABILITY SETTINGS-----
#=====
CONTROL_PLANE_IP="10.100.200.104"
CONTROL_PLANE_PORT="8443"
KEEPALIVED_INTERFACE="eth0"
```

 Необходимо использовать интерфейс, на котором определен IP-адрес текущего хоста из *inventory*. Проверить принадлежность IP-адреса к интерфейсу можно командой *ip a*.

- в блоке «**Database config**» указать параметры подключения к БД. Пример приведен ниже:


```
DB_IP="10.200.200.5"
DB_PORT="5432"
DB_USER="postgres"
DB_NAME="EDodb"

INSTALL_POSTGRESQL="false"
INSTALL_JATOBA="false"
```

 В данной версии комплекса необходимо использовать только внешнюю БД, переменные **INSTALL_POSTGRESQL** и **INSTALL_JATOBA** должны иметь значение «false» (переменные **INSTALL_POSTGRESQL** и **INSTALL_JATOBA** указывают, будет использоваться локальная БД в кластере (значение «**true**») или внешняя (значение «**false**»). При этом только одна из них может быть определена в значении

«*true*»).

- 4) Определить параметры для подключения к СУБД «Jatoba» и к сервису jaDog (кластеризация осуществляется компонентом «jaDog», описанным в документе «Защищенная система управления базами данных «Jatoba». Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»).


 Возможно использование СУБД «Jatoba» в исполнении standalone. При этом шаг 4 пропускается.

- 5) Задать параметры сервера NTP для синхронизации времени на узлах кластера. Это можно выполнить через переменную **NTP_SERVER**:


```
NTP_SERVER="NTP.SERVER"
```

Можно указать несколько серверов NTP разделяя их пробелами.

- 6) Запустить скрипт `./__install.sh`. Для просмотра описания этапов выполнить скрипт **install.sh** без параметров установки. Процесс установки состоит из 8 этапов:
 - s0 – подготовительный этап. Проверяется наличие файлов .env и inventory. На хост устанавливаются зависимости (docker), загружается образ с инсталляционным модулем. Запускается контейнер с установщиком ПК «Efros DO»;
 - s1 – настройка доступа к нодам кластера, генерируются SSH-ключи и копируются на хосты кластера, которые описаны в **inventory**;

 Проверить содержимое файла **./result_check.log** на соответствие хостов требованиям описанным в таблице 5. В случае наличия ошибок привести хосты в соответствие с требованиями.

- s2 – внутри docker-контейнера запускается сценарий (роль **install_deps**) по установке всех зависимостей на ноды (deb-пакеты и утилиты);
- s3 – загрузка образов компонентов кластера;
- s4 – создание кластера **Kubernetes** с помощью утилиты **Kubeadm**;

 При установке кластера на подготовленные ЭВМ необходимо последовательно выполнить шаги установки с s0 по s4. После шага s4 необходимо зайти на ноду **master-1** и выполнить команду **sudo kubectl get nodes**. У всех нод должен появиться статус **STATE Ready**, это может занять некоторое время. Затем

продолжить выполнение шагов с s5 по s8. Все шаги выполняются из скрипта `./__install.sh`.

- s5 – установка в кластер дополнительных компонентов – **Certmanager**;
- s6 – загрузка образов ПК «Efros DO»;
- s7 – задание пароля для доступа к базе данных и установка ПК «Efros DO»;
- s8 – удаление контейнера установки.

7) После установки перейти на **master-1** и выполнить команду **kubectl get po -n edo**. Команда выведет список подов. У всех сервисов, кроме двух, должен быть статус **Running**. У сервисов **edo-radius** и **edo-tacacs** должен быть статус **Init** до тех пор, пока комплекс не пройдет активацию (рис. 50).

```
ladmin@edo-cluster-1:~$ sudo kubectl get po -n edo
NAME                                READY   STATUS    RESTARTS   AGE
edo-acs-service-c7587786d-r84fn      1/1     Running   0           2m23s
edo-agent-service-5ff56866c9-fzs6g  1/1     Running   0           2m27s
edo-ci-service-84ccc5fc66-w2blt      1/1     Running   1 (116s ago) 2m27s
edo-email-sender-service-586ffcdd76-955sx  1/1     Running   0           2m27s
edo-flow-collector-579b5ff5fc-rvlpq  1/1     Running   0           31s
edo-flow-service-9cdfd89b7-fvgjw     1/1     Running   0           2m24s
edo-gateway-service-76b67f74bf-8k95w  1/1     Running   0           2m27s
edo-gateway-service-76b67f74bf-b4g9g  1/1     Running   0           2m27s
edo-gateway-service-76b67f74bf-w5slh  1/1     Running   0           2m27s
edo-guest-portal-service-7f7f4d669c-gs9pr  1/1     Running   0           2m27s
edo-hostpath-provisioner-84f95d95cb-zm9nn  1/1     Running   0           2m26s
edo-identity-service-55d9c9bb5d-2rt7d  1/1     Running   1 (2m24s ago) 2m27s
edo-infr-kafka-0                      1/1     Running   0           2m17s
edo-infr-zookeeper-5d49c79694-7z99t    1/1     Running   0           2m27s
edo-ingress-nginx-controller-7976495df7-8l9z2  1/1     Running   0           2m25s
edo-k8s-operator-service-74b55d66d9-zvkv5  1/1     Running   0           2m26s
edo-knowledge-base-service-645676bcd-b-qnhjj  1/1     Running   0           2m26s
edo-license-service-f8f4c948c-vnmg2    1/1     Running   0           2m26s
edo-metrics-collector-54bd96c78-p2dkf   1/1     Running   4 (98s ago) 2m26s
edo-metrics-service-595c8df8df-qmrv9   1/1     Running   0           2m27s
edo-proxy-service-67cfb84fb4-j6btm     1/1     Running   0           2m27s
edo-radius-7549d49c7b-wrp9h            0/1     Init:0/1  0           2m24s
edo-report-portal-service-5c69c947b5-dfz7r  1/1     Running   0           2m24s
edo-schedule-service-656776cbc9-6fxtl   1/1     Running   0           2m25s
edo-so-service-666cb96cf-nwbbc         1/1     Running   0           2m25s
edo-store-minio-0                      1/1     Running   0           2m27s
edo-store-opensearch-0                 1/1     Running   0           2m27s
edo-tacacs-7d5cfcd997-kcmzj            0/1     Init:0/1  0           2m27s
edo-task-portal-service-559cf5f757-zzkmr  1/1     Running   0           2m25s
edo-vulnerability-collector-8db7487b-v2wz4  1/1     Running   0           2m25s
edo-web-service-54489859f4-jgsmd       1/1     Running   1 (2m24s ago) 2m27s
```

Рисунок 50 – Статусы сервисов

8) Затем необходимо перейти на главную страницу ПК «Efros DO» https://{VIRTUAL_IP}. Например: <https://10.100.200.104>.

- i** Если пароль от БД был введен неверно, на **master-1** необходимо выполнить скрипт, который обновит значение поля **password** в **efros-posgresqlbit-postgresql secret**.

```
sudo kubectl create secret generic efros-posgresqlbit-  
postgresql -n edo \  
--from-literal=password={мой_пароль} \  
--save-config \  
--dry-run=client -o yaml | \  
sudo kubectl apply -f -
```

Для проверки отказоустойчивости необходимо выполнить следующие действия:

- 1) Зайти на веб-интерфейс https://{VIRTUAL_IP}. Проверить доступ к ПК «Efros DO».
- 2) Выключить одну из нод, подключившись к ней напрямую по SSH и выполнив команду:

```
sudo poweroff
```

- 3) Проверить доступность веб-интерфейса комплекса: в течении 5 минут работоспособность должна восстановиться.
- 4) Включить ранее выключенную ноду.

3.7.1.3 Возможные ошибки и способы их устранения

Возможная ошибка №1

При создании кластера **Kubernetes** с помощью утилиты **Kubeadm** (шаг -s4) возможны проблемы инициализации кластера или присоединения узлов. Перед повторным запуском необходимо выполнить шаги по удалению **kubernetes** кластера.

Одна из ошибок при установки может иметь следующий текст:

```
kubeadm_init : Launch kubeadm init from bash script]  
[ERROR CRI]: container runtime is not running: output:  
time="2024-06-10T16:02:02+03:00" level=fatal msg="validate  
service connection: validate CRI v1 runtime API for endpoint  
\\\"unix:///run/containerd/containerd.sock\\\"": rpc error:  
code = Unimplemented desc = unknown service  
runtime.v1.RuntimeService\\\"\\n, error: exit status 1\\n\\
```

Для решения нужно выполнить рестарт сервиса **containerd** на каждом из хостов следующей командой:

```
sudo systemctl restart containerd
```

После можно выполнить проверку командой:

```
sudo crictl ps
```

Возможная ошибка №2

После установки комплекса у некоторых сервисов, развернутых на master_1, могут появиться ошибки вида **image pull failed: Back-off pulling image**.

Для устранения данной проблемы необходимо выполнить следующие действия:

- 1) Загрузить образы на ноду следующей командой:

```
sudo nerdctl load -i /opt/images/edo/{имя образа}.tar.gz
```

- 2) После загрузки необходимо выполнить перезапуск сервиса командой:

```
kubectl rollout restart -n edo deployment/{имя сервиса}
```

Возможная ошибка №3

Проблема с сервисом **edo-radius**. **0/3 nodes are available: 3 node(s) didn't match Pod's node affinity/selector.preemption: 0/3 nodes are available: 3 Preemption is not helpful for scheduling**.

Для устранения данной проблемы необходимо выполнить следующие действия:

- 1) Добавить лейблы **type=master-node** на master-ноды:

```
kubectl label nodes {имя ноды} type=master-node
```

- 2) После загрузки необходимо выполнить перезапуск сервиса **edo-radius** командой:

```
kubectl rollout restart -n edo deployment/edo-radius
```

3.7.1.4 Удаление кластера


Для удаления ПК «Efros DO» из **kubernetes** кластера необходимо выполнить следующую команду:


```
helm uninstall --namespace edo efros
```

Для удаление **kubernetes** кластера необходимо выполнить следующие команды:

```
sudo docker exec -it edo-installer /opt/edospray/__reset-cluster.sh master_3
sudo docker exec -it edo-installer /opt/edospray/__reset-cluster.sh master_2
sudo docker exec -it edo-installer /opt/edospray/__reset-cluster.sh master_1
```

3.7.2 Кластеризация на РЕД ОС

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

 Команды, указанные ниже, необходимо выполнить на всех 3 хостах, кроме отдельных шагов.

3.7.2.1 Предварительные настройки


Перед установкой кластера необходимо выполнить настройку хостов, настройку master-ноды и настроить параметры управления кластером.

3.7.2.1.1 Настройка хостов

Для настройки хостов необходимо выполнить следующие шаги:

- 1) Определить **hostname edo-cluster-{номер ноды}**, например: edo-cluster-1, edo-cluster-2, edo-cluster-3.
- 2) Задать **hostname** можно командой:

```
hostnamectl set-hostname edo-cluster-1
```

 Хосты должны находиться в одной подсети.

❗ Идентификатор **hostname** должен быть задан буквами нижнего регистра (строчными буквами).

- 3) Необходимо выделить один IP-адрес, который будет использоваться как виртуальный. Адрес не должен быть привязан к какому-либо хосту и находиться в той же подсети, что и хосты.
- 4) Должно быть однозначное сопоставление IP-адреса и **hostname**. Если хосты не добавлены в **dns**, то это можно сделать в файле **/etc/hosts**.
- 5) Переменная **\$HOSTNAME** должна иметь тоже значение, что выводится при команде **hostname**. Если значения не совпадают, то требуется перезайти на хост по SSH (рис. 51)

```
[root@edo-cluster-1 ~]# hostname
edo-cluster-1
[root@edo-cluster-1 ~]# echo $HOSTNAME
edo-cluster-1
```

Рисунок 51 – Совпадение значений имен хоста

3.7.2.1.2 Настройка master-нод

Для настройки master-нод необходимо выполнить следующие шаги:

- 1) Для работы **kubelet** отключить **swap**. Для разового отключения **swap** выполнить команду:

```
swapoff -a
```

Для блокирования **swap** после загрузки сервера выполнить команду:

```
swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
```

- 2) Отключить **SELinux**, выполнив команду:

```
setenforce 0 && sed -i --follow-symlinks
's/SELINUX=enforcing/SELINUX=disabled/g'
/etc/sysconfig/selinux
```

- 3) Создать файл для автозагрузки модулей ядра, необходимых для работы сервиса **containerd**. Это можно сделать в файле **/etc/network/interfaces**. Для этого выполнить команду:


```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

Ввести текст в файл:

```
overlay  
br_netfilter
```

Загрузить модули в ядро. Для этого ввести в консоль:

```
modprobe overlay  
modprobe br_netfilter
```

Проверить доступность модулей, выполнив команду:

```
lsmod | egrep "br_netfilter|overlay"
```

4) Создать конфигурационный файл для работы сети внутри **kubernetes**. Для этого выполнить команду:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

Ввести текст в файл:

```
net.bridge.bridge-nf-call-iptables = 1  
net.ipv4.ip_forward = 1  
net.bridge.bridge-nf-call-ip6tables = 1
```

Применить параметры командой:

```
sysctl --system
```

5) Установить необходимые пакеты, выполнив команду:

```
dnf install kubernetes kubernetes-kubeadm cri-tools tc
ipvsadm ebtables socat conntrack git curl wget runc
containerd ntp
```

6) Настроить проброс портов в **iptables**, выполнив команду:

```
iptables -P FORWARD ACCEPT
```

7) Установить настройки по умолчанию для конфигурации контейнера:

```
containerd config default | sudo tee
/etc/containerd/config.toml
```

8) Для разрешения использования **cgroup** необходимо переключить флаг параметра **systemdCgroup** в конфигурационном файле **/etc/containerd/config.toml**:

```
sed -i 's/SystemdCgroup \= false/SystemdCgroup \= true/g'
/etc/containerd/config.toml
```

9) Далее запустить службу **containerd** и добавить ее в автозагрузку:

```
systemctl enable --now containerd
```

10) Добавить службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

11) Добавить службу **ntp** в автозагрузку для синхронизации времени на нодах:

```
systemctl enable --now ntpd.service
```

12) Выполнить команду для создания файла конфигурации **/etc/crictl.yaml**:

```
cat << EOL > /etc/crictl.yaml
runtime-endpoint: "unix:///run/containerd/containerd.sock"
timeout: 0
```

```
debug: false  
EOL
```

13) Загрузить образы контейнеров, необходимых **kubeadm** для инициализации ноды кластера:

```
kubeadm config images pull --kubernetes-version 1.28.9 --cri-  
socket /run/containerd/containerd.sock
```

14) Загрузить образы для **keepalived** и **haproxy** для создания отказоустойчивого кластера на **master 1** и **master 3** ноды.

```
crictl pull osixia/keepalived:2.0.20  
crictl pull haproxy:2.2.32-bullseye
```

15) Создать следующие папки для добавления конфигураций для **keepalived** и **haproxy** кластера на **master 1** и **master 3** нодах:

```
mkdir -p /etc/keepalived;  
mkdir -p /etc/haproxy;  
mkdir -p /etc/kubernetes/manifests;
```

16) Добавить конфигурацию для **haproxy**, предварительно указав IP-адреса нод в команде. Команду нужно выполнить на **1** и **3** нодах:

```
cat << EOL > /etc/haproxy/haproxy.cfg  
frontend kubernetes-master-lb  
    bind *:8443  
    mode tcp  
    option tcplog  
    default_backend kubernetes-master  
  
backend kubernetes-master  
    mode tcp  
    option tcp-check
```

```
balance roundrobin
default-server inter 10s downinter 5s rise 2 fall 2
slowstart 60s maxconn 250 maxqueue 256 weight 100
server edo-cluster-1 10.116.41.182:6443 check
server edo-cluster-2 10.116.41.183:6443 check
server edo-cluster-3 10.116.41.184:6443 check
EOL
```

17) Добавить манифест для создания статического пода **haproxy**, выполнив следующую команду на **1 и 3 нодах**:

```
cat << EOL > /etc/kubernetes/manifests/haproxy.yaml
apiVersion: v1
kind: Pod
metadata:
  name: haproxy
  namespace: kube-system
spec:
  containers:
  - image: haproxy:2.2.32-bullseye
    name: haproxy
    imagePullPolicy: IfNotPresent
    livenessProbe:
      failureThreshold: 8
      tcpSocket:
        port: 8443
      initialDelaySeconds: 15
      periodSeconds: 10
    volumeMounts:
    - mountPath: /usr/local/etc/haproxy/haproxy.cfg
      name: haproxyconf
      readOnly: true
  hostNetwork: true
  volumes:
```

```
- hostPath:
  path: /etc/haproxy/haproxy.cfg
  type: FileOrCreate
  name: haproxyconf
status: {}
EOL
```

18) Выбрать виртуальный IP-адрес (далее – VIP) для доступа к кластеру. Данный адрес должен находиться в той же подсети, что и master-ноды, и не должен быть привязан к хосту. Пример IP-адреса:

```
10.116.41.180
```

19) Выполнить команду, приведенную ниже, на **1 и 3 нодах**, чтобы узнать название сетевого интерфейса, через который будет выполняться реализация VIP:

```
ip address show | grep "10.116.41.184"
```

Например, для ноды 3 с IP-адресом 10.116.41.184, название сетевого интерфейса будет «ens18»:

```
inet 10.116.41.184/24 brd 10.116.41.255 scope global
noprefixroute ens18
```

20) Добавить */etc/keepalived/keepalived.conf* файл конфигурации для **keepalived** на **1 ноду** через редактор **nano**, указав VIP и Interface соответствующие значения переменных **\$APISERVER_VIP** и **\$INTERFACE**:

```
nano /etc/keepalived/keepalived.conf
! /etc/keepalived/keepalived.conf
! Configuration File for keepalived
$STATE=MASTER
$INTERFACE=ens18
$ROUTER_ID=51
$PRIORITY=101
$AUTH_PASS=1111
```

```
$APISERVER_VIP=10.116.41.180/24

vrrp_script check_apiserver {
    script "/etc/keepalived/check_apiserver.sh"
    interval 3
    weight -2
    fall 10
    rise 2
}

vrrp_instance VI_1 {
    state ${STATE}
    interface ${INTERFACE}
    virtual_router_id ${ROUTER_ID}
    priority ${PRIORITY}
    authentication {
        auth_type PASS
        auth_pass ${AUTH_PASS}
    }
    virtual_ipaddress {
        ${APISERVER_VIP}
    }
    track_script {
        check_apiserver
    }
}
```

21) Добавить ***/etc/keepalived/keepalived.conf*** файл конфигурации для ***keepalived*** на **3 ноде** через редактор nano, указав VIP и Interface соответствующие значения переменных ***\$APISERVER_VIP*** и ***\$INTERFACE***:



Разница от предыдущего шага в устанавливаемой ноде и в приоритете.

```
nano /etc/keepalived/keepalived.conf
```

```
! /etc/keepalived/keepalived.conf
! Configuration File for keepalived
$STATE=BACKUP
$INTERFACE=ens18
$ROUTER_ID=51
$PRIORITY=100
$AUTH_PASS=1111
$APISERVER_VIP=10.116.41.180/24

vrrp_script check_apiserver {
    script "/etc/keepalived/check_apiserver.sh"
    interval 3
    weight -2
    fall 10
    rise 2
}

vrrp_instance VI_1 {
    state ${STATE}
    interface ${INTERFACE}
    virtual_router_id ${ROUTER_ID}
    priority ${PRIORITY}
    authentication {
        auth_type PASS
        auth_pass ${AUTH_PASS}
    }
    virtual_ipaddress {
        ${APISERVER_VIP}
    }
    track_script {
```

```
        check_apiserver
    }
}
```

22) Добавить на **1 и 3 ноду** скрипт для проверки доступности ноды. Указав VIP на соответствующий виртуальный IP-адрес в команде:

```
cat << EOL > /etc/keepalived/check_apiserver.sh
#!/bin/sh

errorExit() {
    echo "*** $*" 1>&2
    exit 1
}

curl --silent --max-time 2 --insecure https://localhost:8443/
-o /dev/null || errorExit "Error GET
https://localhost:10.116.41.180/"
if ip addr | grep -q 10.116.41.180; then
    curl --silent --max-time 2 --insecure
https://10.116.41.180:8443/ -o /dev/null || errorExit "Error
GET
https:// 10.116.41.180:8443/"
fi
EOL

chmod 755 /etc/keepalived/check_apiserver.sh
```

23) Добавить манифест для создания статического пода **keepalived**, выполнив следующую команду на **1 и 3 нодах**:

```
cat << EOL > /etc/kubernetes/manifests/keepalived.yaml
apiVersion: v1
kind: Pod
metadata:
  creationTimestamp: null
```



```
name: keepalived
namespace: kube-system
spec:
  containers:
  - image: osixia/keepalived:2.0.20
    name: keepalived
    resources: {}
    imagePullPolicy: IfNotPresent
    securityContext:
      capabilities:
        add:
        - NET_ADMIN
        - NET_BROADCAST
        - NET_RAW
    volumeMounts:
    - mountPath: /usr/local/etc/keepalived/keepalived.conf
      name: config
    - mountPath: /etc/keepalived/check_apiserver.sh
      name: check
  hostNetwork: true
  volumes:
  - hostPath:
      path: /etc/keepalived/keepalived.conf
      name: config
  - hostPath:
      path: /etc/keepalived/check_apiserver.sh
      name: check
status: {}
EOL
```

24) Запустить инициализацию master-ноды на **1 ноде**, указав VIP на виртуальный IP-адрес из шага 16. Данная команда выполнит начальную настройку и подготовку основного узла кластера. Ключ **--pod-network-cidr** задает адрес внутренней подсети для кластера:

```
kubeadm init --control-plane-endpoint 10.116.41.180:8443 \  
  --cri-socket /run/containerd/containerd.sock \  
  --kubernetes-version 1.28.9 \  
  --pod-network-cidr 10.244.0.0/16 \  
  --service-cidr 10.96.0.0/16 \  
  --service-dns-domain cluster.local \  
  --node-name $HOSTNAME \  
  --upload-certs --ignore-preflight-errors  
NumCPU,KubeletVersion
```

После успешной инициализации, в конце вывода команды отобразится соответствующее сообщение:

```
Your Kubernetes control-plane has initialized successfully!
```

To start using your cluster, you need to run the following as a regular user:

```
mkdir -p $HOME/.kube  
sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config  
sudo chown $(id -u):$(id -g) $HOME/.kube/config
```

Alternatively, if you are the root user, you can run:

```
export KUBECONFIG=/etc/kubernetes/admin.conf
```

You should now deploy a pod network to the cluster.

Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:

```
https://kubernetes.io/docs/concepts/cluster-administration/addons/
```

You can now join any number of the control-plane node running the following command on each as root:

```
kubeadm join 10.116.41.180:8443 --token
9pej38.xa2cipum2vgqi3w9 \
    --discovery-token-ca-cert-hash
sha256:9c2f79347f83898bda0bba1e54e4806f6e356735c25ec36f8c032d
4d3d4e5837 \
    --control-plane --certificate-key
e4fb5c88456a959b42abc5b76d6d546e9a3ec6ee349a039366621f5456dac
b72
```

Please note that the certificate-key gives access to cluster sensitive data, keep it secret!

As a safeguard, uploaded-certs will be deleted in two hours; If necessary, you can use

"kubeadm init phase upload-certs --upload-certs" to reload certs afterward.

Then you can join any number of worker nodes by running the following on each as root:

```
kubeadm join 10.116.41.180:8443 --token
9pej38.xa2cipum2vgqi3w9 \
    --discovery-token-ca-cert-hash
sha256:9c2f79347f83898bda0bba1e54e4806f6e356735c25ec36f8c032d
4d3d4e5837
```

25) Сохранить строки, приведенные ниже, после успешной инициализации кластера, полученные на прошлом шаге. Они будут использоваться для присоединения 2 других нод:

```
kubeadm join 10.116.41.180:8443 --token
9pej38.xa2cipum2vgqi3w9 \
    --discovery-token-ca-cert-hash
sha256:9c2f79347f83898bda0bba1e54e4806f6e356735c25ec36f8c032d
4d3d4e5837 \
    --control-plane --certificate-key
e4fb5c88456a959b42abc5b76d6d546e9a3ec6ee349a039366621f5456dac
b72
```

3.7.2.1.3 Настройка управления кластером

Настройку параметров управления кластером можно выполнить как для локального пользователя, так и для суперпользователя **root**.

Для управления кластером от имени суперпользователя **root** необходимо выполнить команды:

```
echo "export KUBECONFIG=/etc/kubernetes/admin.conf" >>
/root/.bashrc
source .bashrc
export KUBECONFIG=/etc/kubernetes/admin.conf
```

Для настройки управления кластером необходимо выполнить следующие шаги:

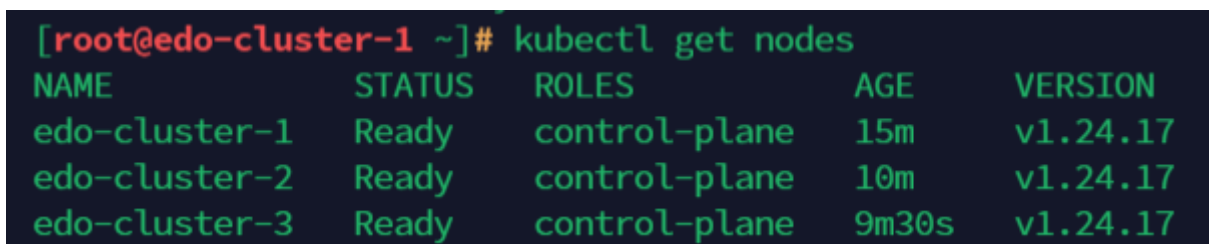
- 1) Установить внутреннюю конфигурацию сети в кластере. Пример с использованием **calico**:

```
kubectl apply -f
https://raw.githubusercontent.com/projectcalico/calico/v3.25.
0/manifests/calico.yaml
```

- 2) Проверить список и статус всех подов в кластере, они должны иметь статус **Running**:

```
kubectl get pod -n kube-system
```

- 3) Запустить команду на **2 ноде**, сохраненную на шаге 25, для присоединения данной ноды к кластеру.
- 4) Запустить команду на **3 ноде**, сохраненную на шаге 25, для присоединения данной ноды к кластеру.
- 5) Проверить, что все ноды перешли в состояние **Ready** (рис. 52).



```
[root@edo-cluster-1 ~]# kubectl get nodes
NAME                STATUS    ROLES    AGE     VERSION
edo-cluster-1      Ready    control-plane   15m    v1.24.17
edo-cluster-2      Ready    control-plane   10m    v1.24.17
edo-cluster-3      Ready    control-plane    9m30s  v1.24.17
```

Рисунок 52 – Ноды в состоянии **Ready**


- 6) Скачать и установить **helm**, используя следующие команды на **1 ноде**:

```
mkdir helm;  
cd helm;  
wget https://get.helm.sh/helm-v3.14.4-linux-amd64.tar.gz;  
tar -xvf helm-v3.14.4-linux-amd64.tar.gz;  
mv linux-amd64/helm /usr/local/bin/helm;  
cd ../;  
rm -rf helm;
```

- 7) Выполнить следующую команду, чтобы разрешить назначать поды на master-ноды:

```
kubectl taint nodes --all node-  
role.kubernetes.io/master:NoSchedule-  
kubectl taint nodes --all node-role.kubernetes.io/control-  
plane:NoSchedule-
```

3.7.2.2 Установка кластера

 Рекомендуется проводить установку кластера с отдельного хоста, который будет находится в той же подсети, что и хосты будущего кластера. А также иметь к ним доступ по SSH.

 Команды необходимо вводить от имени локального пользователя.

Для установки кластера необходимо выполнить следующие шаги:

- 1) Скопировать архив **certmanager.tgz** на **1 ноду** и выполнить распаковку следующей командой:

```
mkdir certmanager;  
tar -xvf certmanager.tgz -C ~/certmanager;  
cd ./certmanager
```

- 2) Установить **certmanager**, запустив следующие команды на **1 ноду**:

```
kubectl create namespace certmanager  
kubectl apply -f cert-manager.crds.yaml
```

```
helm install cert-manager cert-manager-v1.7.1.tgz -f
certmanager.values.yml --namespace certmanager
```

- 3) Скопировать архив с образами ПК «Efros DO» на каждую из нод и распаковать архив:

```
mkdir edo-images;
tar -xvf edo-images.tgz -C ./edo-images;
```

- 4) Установить **nerdctl** для загрузки образов ПК «Efros DO»:

```
mkdir nerd;
cd nerd;
wget
https://github.com/containerd/nerdctl/releases/download/v1.7.
6/nerdctl-1.7.6-linux-amd64.tar.gz;
tar -xvf nerdctl-1.7.6-linux-amd64.tar.gz;
mv nerdctl /usr/local/bin/;
cd ../;
rm -rf nerd;
```

- 5) С помощью редактора **nano** создать скрипт **load_local_images.sh** со следующим содержанием:

```
#!/bin/bash

echo "Image folder: ${1}"

for f in ${1}/*tar.gz; do
    nerdctl load -i "$f";
    sync;
    sysctl -w vm.drop_caches=3;
done;
```

- 6) Загрузить образы ПК «Efros DO» на каждую ноду, выполнив следующие команды

на каждой из нод:

```
chmod +x ./load_local_images.sh;  
./load_local_images.sh ./edo-images/;
```

7) Выполнить следующие команды для предварительной настройки хостов под использование внутренней базы:

```
sysctl -w vm.max_map_count=262144  
echo fs.inotify.max_user_instances=524288 | sudo tee -a  
/etc/sysctl.conf && sudo sysctl -p
```

8) Распаковать архив с **edo helm-chart** на **1 ноду**:

```
mkdir edo-helm;  
tar -xvf efros-do.tgz -C ./edo-helm;
```

9) В папке с **edo helm-chart** отредактировать **values.yaml** под требуемую среду:

```
namespace: edo  
  
#Database installations  
# включить внутреннюю базу postgres  
installPostgreSQL: true  
installjatoba: false  
# включить внутреннее хранилище для volumes  
installStorageProv: true  
  
storageclass: local-storage  
  
#license_server_url: http://10.80.2.11  
# сервер лицензирования  
license_server_url: https://license.gaz-is.ru  
# временная зона сервера  
timezone: "Europe/Moscow"
```

```
ingress:
  enabled: true

serviceAccount:
  create: false


global:
  # Удаленный репозиторий, в случае использования закрытого
  # контура поле должно быть пустым
  repository:
    # Флаг локальной установки, в случае использования
    # закрытого контура должно быть true
    localInstall: true
    # Политика скачивания образа, в случае использования
    # закрытого контура должно быть true
    imagePullPolicy: "IfNotPresent"

VoltronDB:
  # Адрес базы, в случае использования внутренней базы
  # оставить неизменным
  DatabaseAddress: "efros-posgresqlbit-pgpool"
  # Порт подключения к базе
  DatabasePort: "5432"
  # Имя базы, при использовании внутренней базы оставить
  # неизменным
  DatabaseName: "postgres"
  # Имя пользователя, при использовании внутренней базы
  # оставить неизменным
  DatabaseUserId: "postgres"

# Для radius, tacacs, gateway и extIP указать VIP
addresspool:
  radius: "10.116.41.180"
  tacacs: "10.116.41.180"
```



```
gateway: "10.116.41.180"  
extIP:  
  - "10.116.41.180"  
eci: ""  
flow_dhcp: ""  
flow_sflow: ""  
flow_collector: ""
```


-  Рекомендуется проводить установку кластера с отдельного хоста, который будет находиться в той же подсети, что и хосты будущего кластера. А также иметь к ним доступ по SSH.

10) Выполнить команду для установки **helm-chart** в папке **edo-helm**:

```
cd edo-helm;  
helm install efros ./ -f ./values.yaml --namespace edo --  
create-namespace
```

11) Дождаться, когда все поды edo перейдут в состояние **Running**.

3.7.2.3 Удаление кластера

-  Команды, указанные ниже, необходимо выполнить на всех 3 хостах, кроме отдельных шагов.

Для удаления ПК «Efros DO» из **kubernetes** кластера необходимо выполнить следующие действия:

- 1) Сбросить настройки **kubeadm** и компонентов **Kubernetes**. Для этого выполнить команду:

```
kubeadm reset -f
```

- 2) Удалить все образы во всех namespaces (пространства имен) **nerdctl**, выполнив следующую команду:


```
for namespace in $(nerdctl namespace ls -q); do
```

```
nerdctl --namespace $namespace rmi -f $(nerdctl --namespace $namespace images -q)
```

Done

3) Удалить все конфигурационные файлы и данные, выполнив следующую команду:

```
rm -rf /etc/cni/net.d /etc/containerd /etc/kubernetes/  
/var/lib/kubelet/ /var/lib/containerd/ /etc/cni/  
/etc/keepalived/ /etc/haproxy/ /var/lib/etcd/
```

 Конфигурационные файлы и данные **keepalived** и **haproxy** удаляются только на **1 и 3 нодах**, на 2 ноде их не должно быть.

4) Остановить службы **kubelet containerd**, выполнив следующую команду:

```
systemctl stop kubelet containerd
```

5) Удалить конфигурационный файл **kube**. Выполняется опционально, если конфигурационный файл был установлен. Для удаления выполнить команду:

```
rm -rf /root/.kube/config
```

6) Завершить все процессы **containerd-shim**, выполнив следующую команду:

```
sudo pkill -f containerd-shim
```

7) Очистить все правила **iptables**, выполнив следующую команду:

```
iptables -F && iptables -t nat -F && iptables -t mangle -F &&  
iptables -X
```

8) Отключить сетевой интерфейс, выполнив следующую команду:

```
ip link set "INTERFACE_NAME" down
```

Примеры параметра "INTERFACE_NAME": tunl0, cali6cc8609202b.

9) Перезагрузить **systemd**, выполнив следующую команду:

```
systemctl daemon-reload
```

10) Перезагрузить систему, выполнив следующую команду:

```
sudo reboot
```

3.8 Windows-агент ПК «Efros DO»

3.8.1 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.

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. 53).

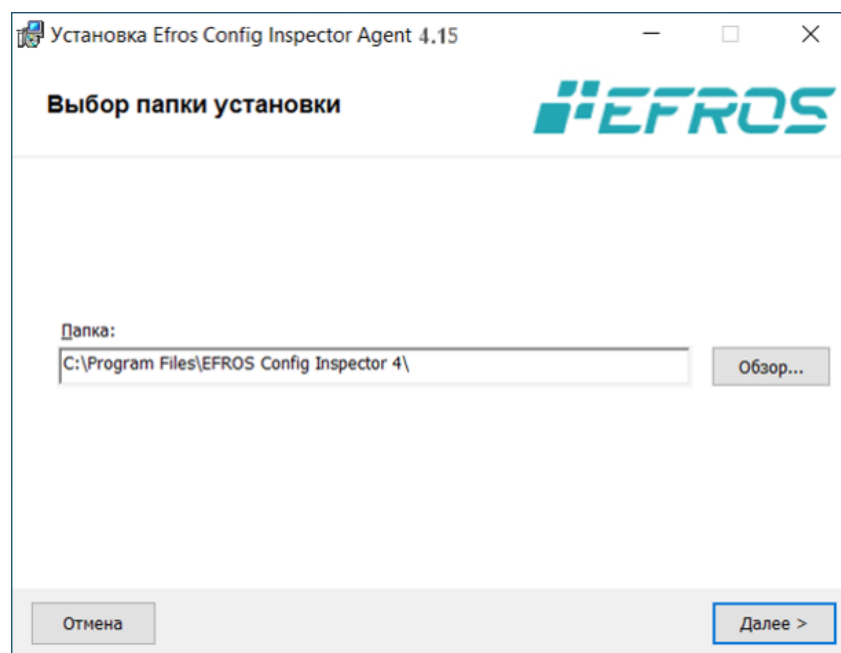


Рисунок 53 – Диалоговое окно выбора папки для установки windows-агента

В диалоговом окне готовности мастера к установке (рис. 54) для запуска процесса установки с заданными ранее параметрами следует нажать кнопку «Установить».

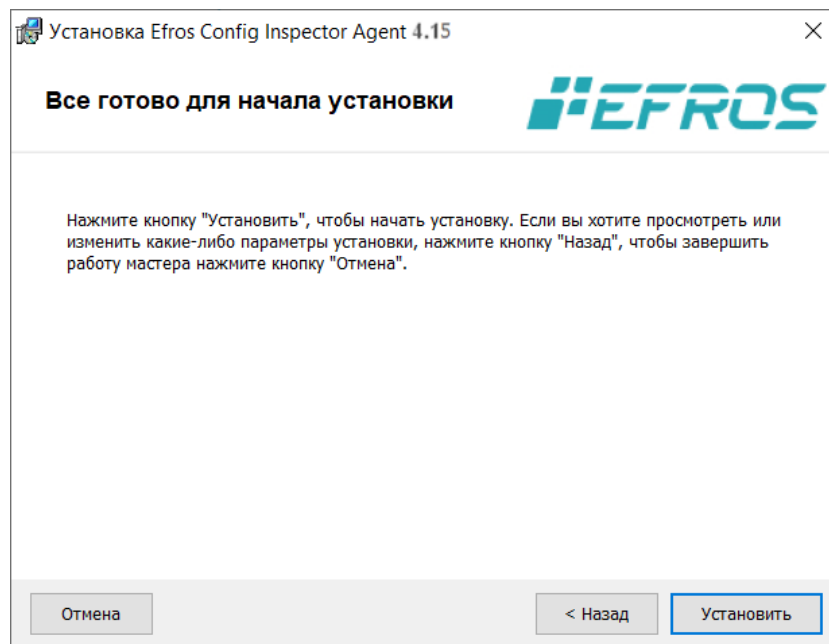


Рисунок 54 – Диалоговое окно готовности к установке

Ход установки windows-агента программного комплекса будет отображаться в окне мастера установки (рис. 55).

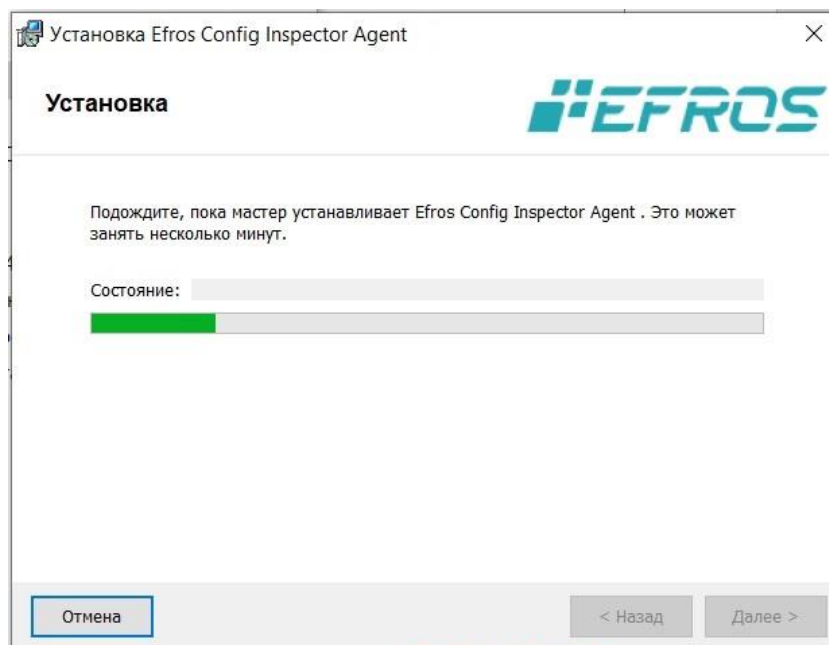


Рисунок 55 – Диалоговое окно процесса установки

После окончания установки windows-агента откроется диалоговое окно завершения работы мастера установки (рис. 56), в котором следует нажать кнопку «Готово».

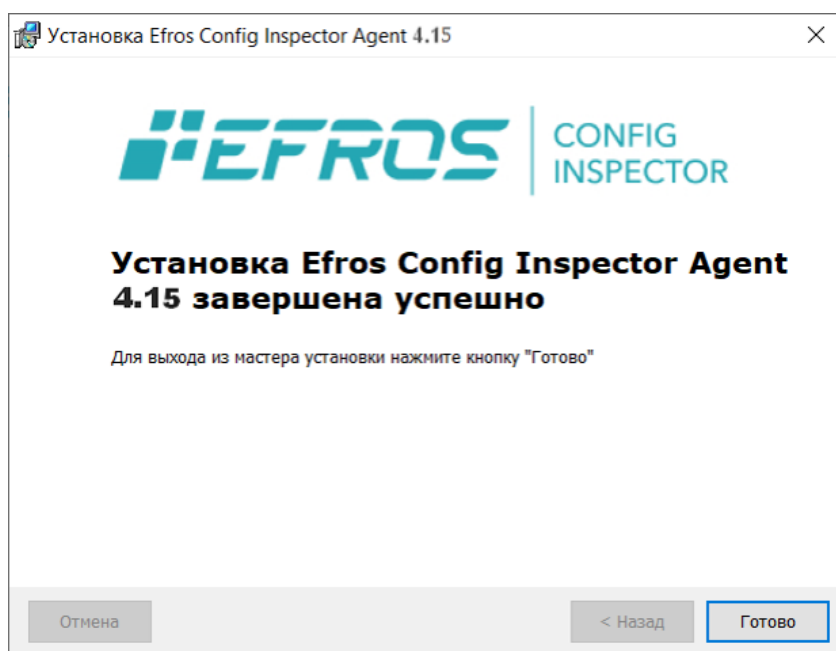


Рисунок 56 – Диалоговое окно завершения работы мастера установки

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 CI Agent Service 4 (C:\Program Files\EFROS Config Inspector 4\Agent\WASetup.exe)**.

3.8.2 Настройка параметров службы windows-агента

Вызов окна настройки параметров службы EFROS CI Agent Service 4 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. 57). Состав и описание полей вкладки «Службы» приведены в таблице 6.

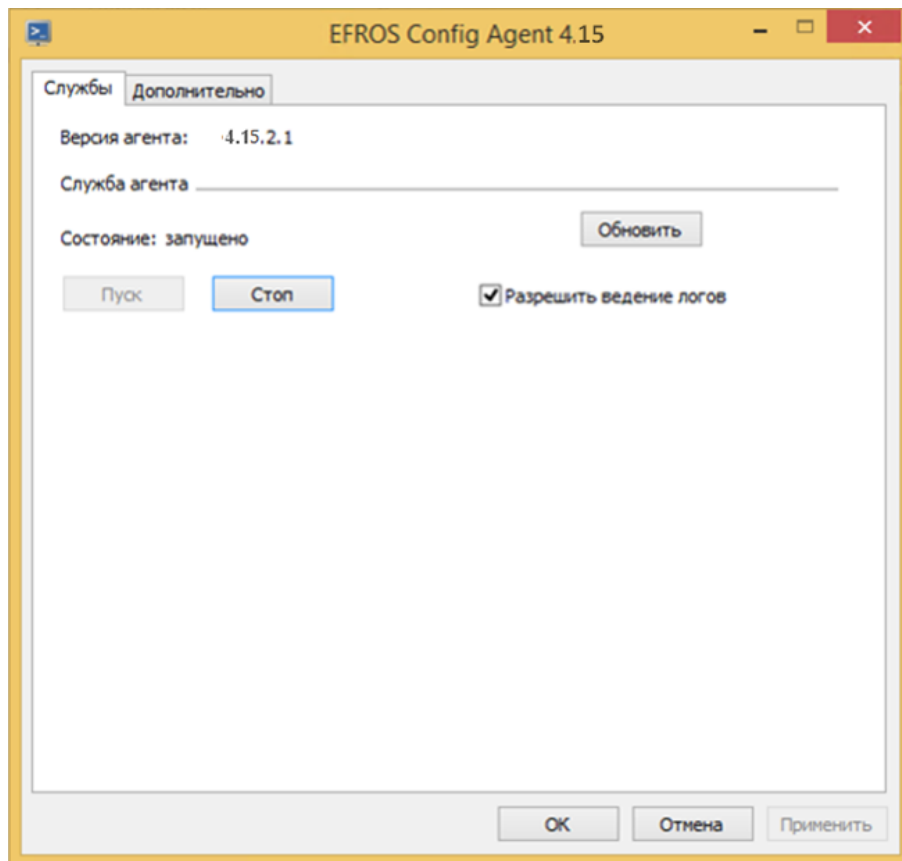


Рисунок 57 – Вкладка «Службы» окна настройки параметров службы EFROS CI Agent Service 4

Таблица 6 – Состав и описание полей вкладки «Службы» окна настройки параметров службы EFROS CI Agent Service 4

Поле	Описание
Поле «Версия агента»	Отображает последнюю версию установленного агента
Раздел «Служба агента»	
Поле «Состояние»	Отображает статус агента: — запущено; — остановлено
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

При переходе на вкладку «Дополнительно» отображаются дополнительные настройки

службы (рис. 58). Состав и описание полей вкладки «Дополнительно» приведены в таблице 7.

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.

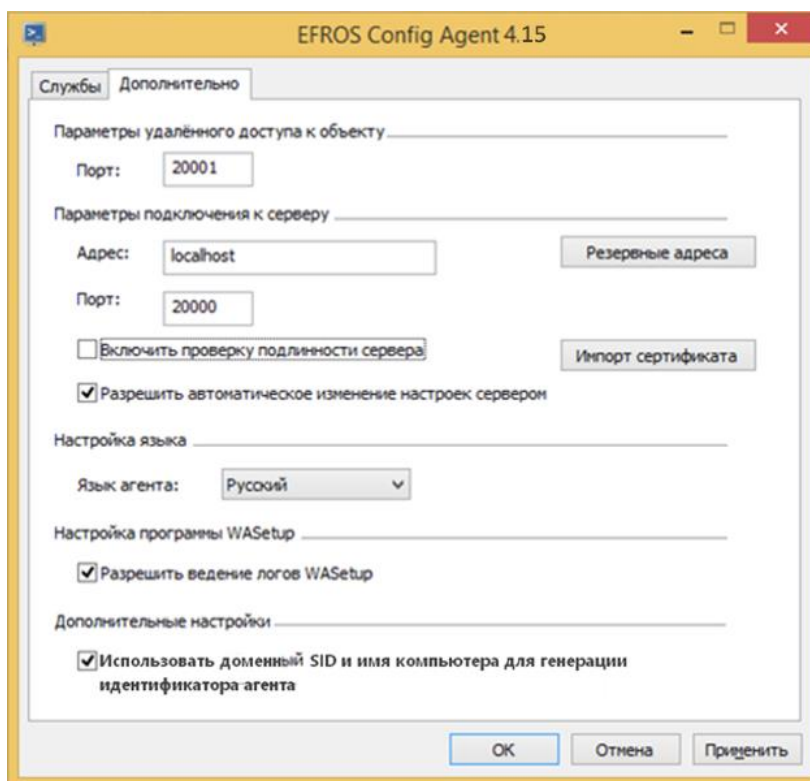


Рисунок 58 – Вкладка «Дополнительно» окна настройки параметров службы EFROS CI Agent Service 4

Таблица 7 – Состав и описание полей вкладки «Дополнительно» окна настройки параметров службы EFROS CI Agent Service 4

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 windows-агенту
Поле «Включить проверку»	При включенном параметре (флаг в поле установлен) происходит проверка серверной части и windows-агента с

Поле	Описание
подлинности сервера»	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»
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»
Настройка языка	
Поле «Язык агента»	Позволяет выбрать язык windows-агента (русский, английский)
Настройка программы WASetup	
Поле «Разрешить ведение логов WASetup»	Включает/отключает ведение логов программы настройки windows-агента WASetup
Дополнительные параметры	
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

3.9 Агент ПК «Efros DO»

Агент ПК «Efros DO» (агент) устанавливается на контролируемые конечные точки.

Агент предназначен для сбора сведений о конечной точке. На основе полученных данных определяется статус соответствия требованиям политики безопасности.

3.9.1 Установка агента ПК «Efros DO» на Windows



Предварительно необходимо настроить подключение конечной точки к серверу ПК «Efros DO» по имени сервера: <https://edo-gateway-service>. Для обеспечения сетевой связанности необходимо зарегистрировать имя сервера «edo-gateway-service» в службе DNS.

Для установки агента ПК «Efros DO» необходимо скопировать на контролируруемую конечную точку с ОС Windows файл ***edo-agent-<версия>.msi*** и запустить его на исполнение.

Откроется окно мастера установки «EDO Agent» (рис. 59).

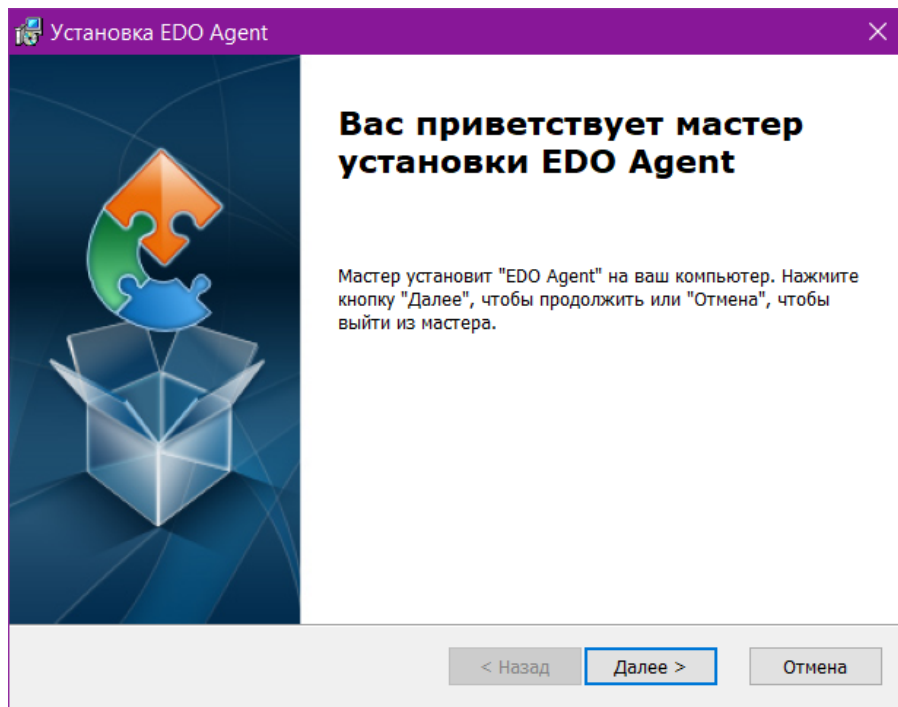


Рисунок 59 – Диалоговое окно мастера установки «EDO Agent»

В диалоговом окне мастера установки нажать кнопку «Далее».

Откроется диалоговое окно выбора папки установки, в котором следует выбрать папку для установки агента или оставить заданную по умолчанию (***C:\Program Files\EDO\Agent***) и нажать кнопку «Далее» (рис. 60).

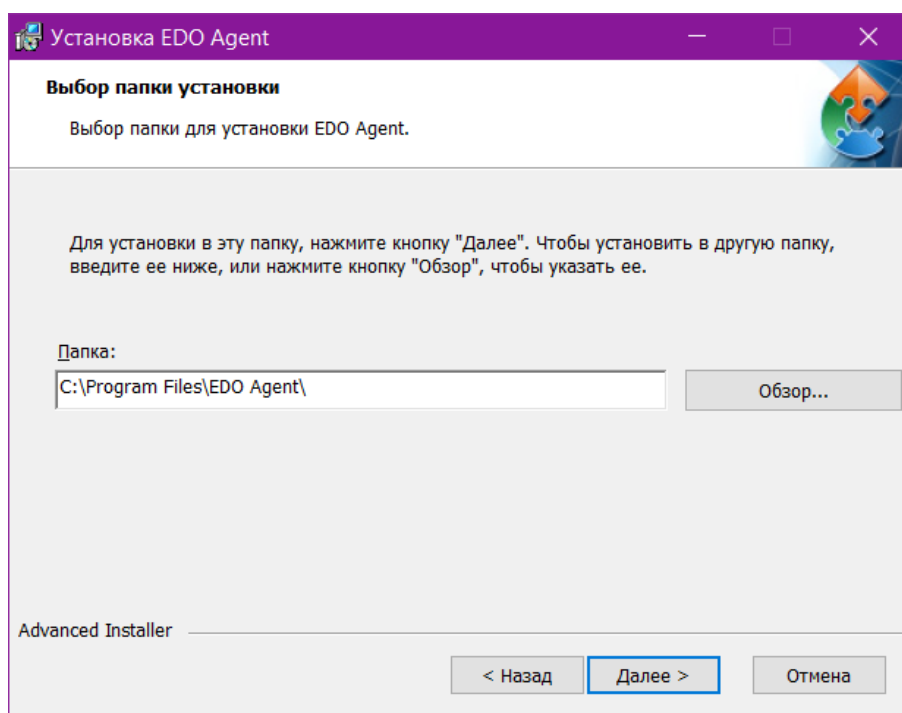


Рисунок 60 – Диалоговое окно выбора папки установки

В диалоговом окне готовности мастера к установке (рис. 61) для запуска процесса инсталляции с заданными ранее параметрами следует нажать кнопку «Установить».

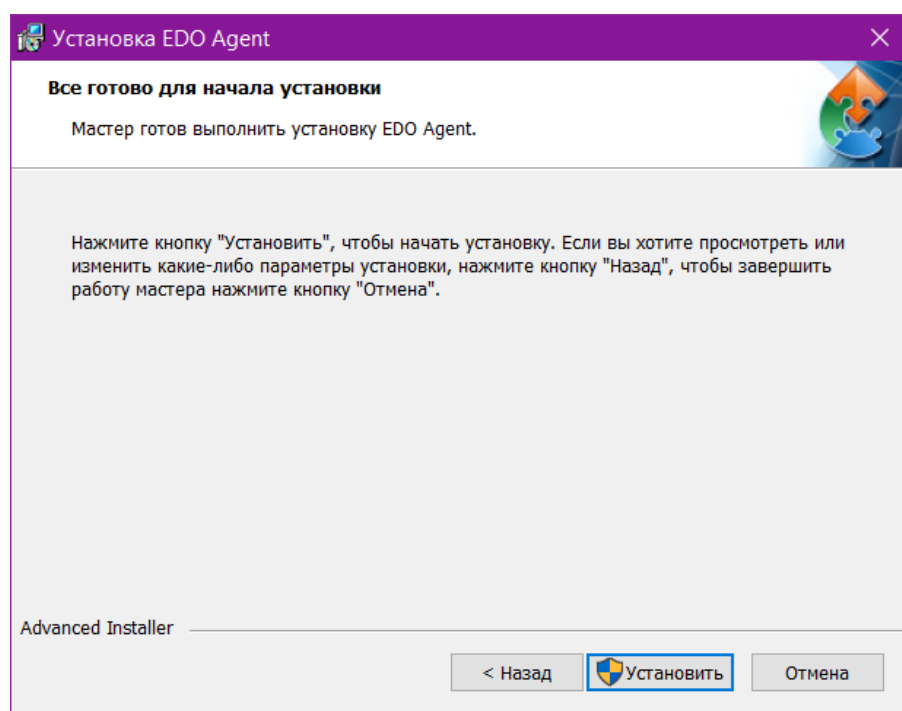


Рисунок 61 – Диалоговое окно готовности к установке

Ход установки «EDO Agent» программного комплекса будет отображаться в окне мастера установки (рис. 62).

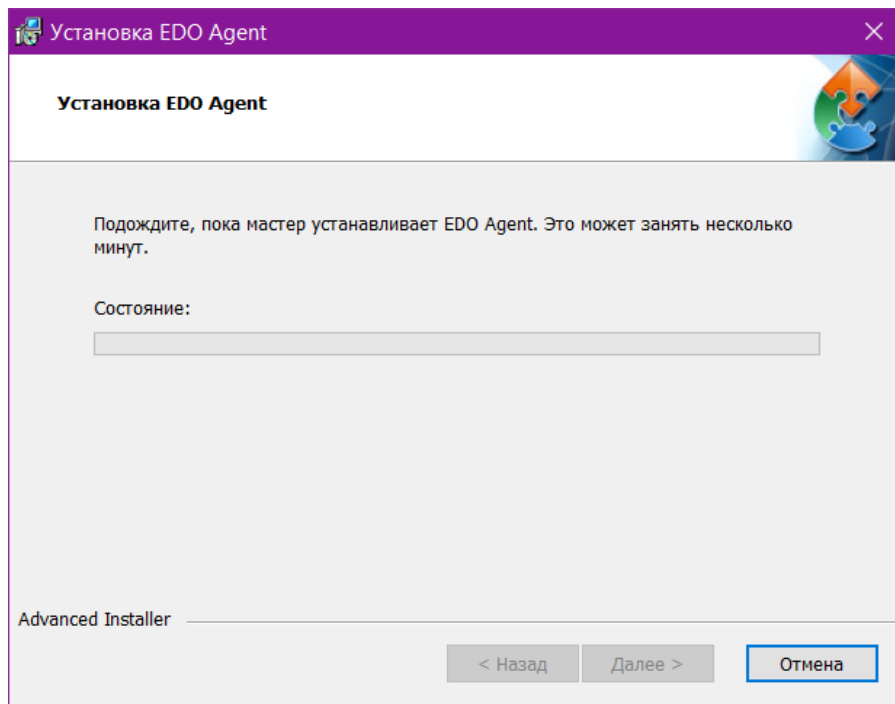


Рисунок 62 – Диалоговое окно процесса установки

i При появлении диалогового окна операционной системы «Разрешить этому приложению вносить изменения на вашем устройстве?» следует нажать кнопку «Да».

После окончания установки «EDO Agent» откроется диалоговое окно завершения работы мастера установки (рис. 63), в котором следует нажать кнопку «Готово».

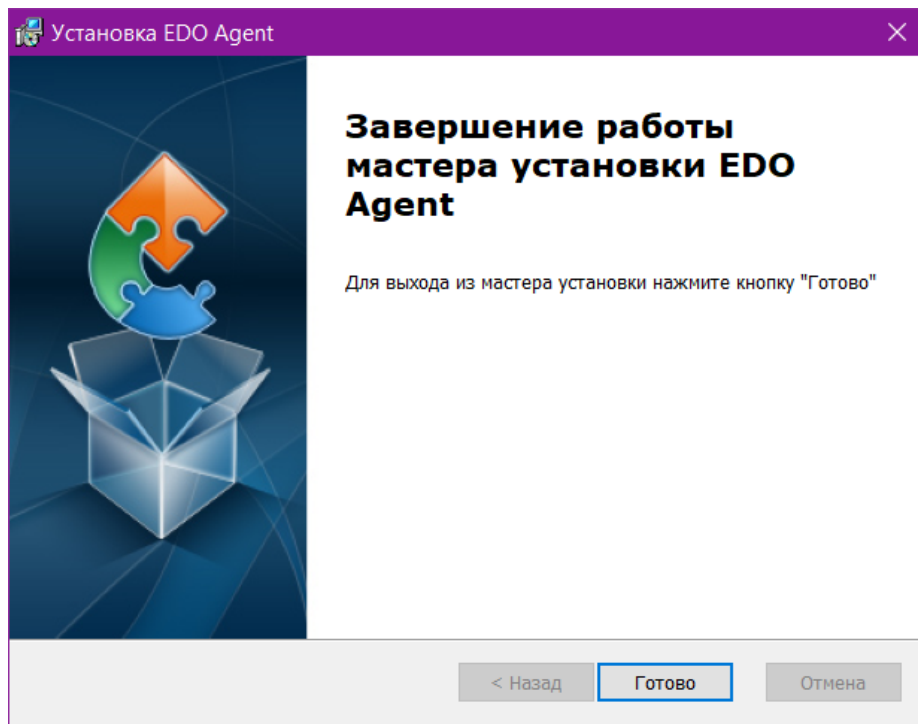


Рисунок 63 – Диалоговое окно завершения работы мастера установки

В окне программы «Службы» появится и автоматически запустится служба «Edo Agent Service» (рис. 64).

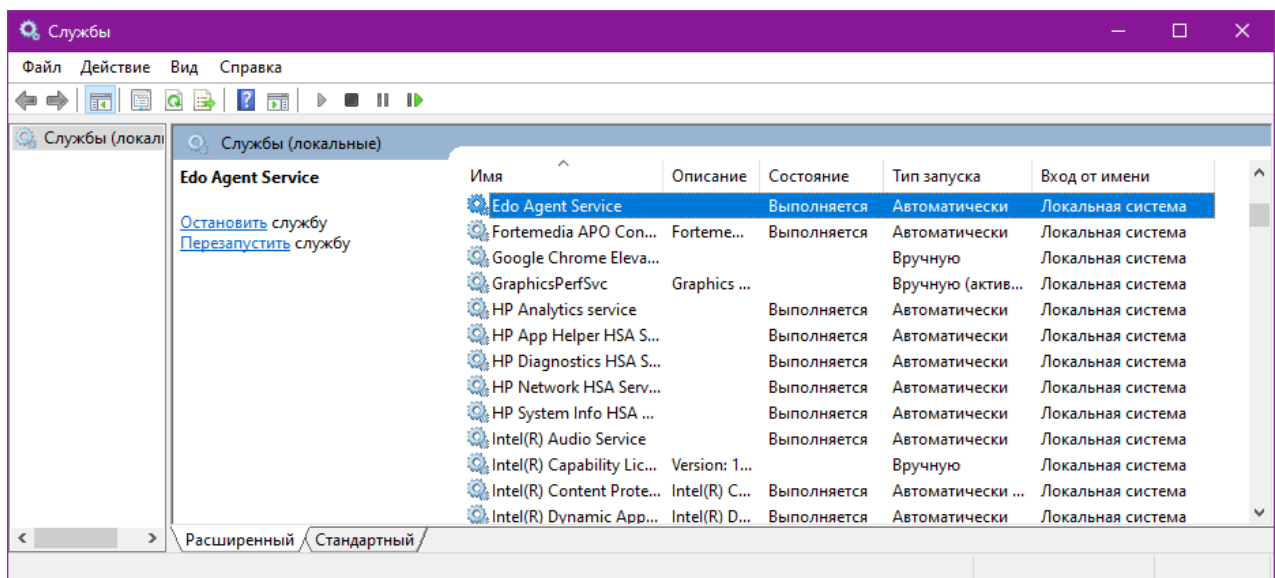



Рисунок 64 – Запущенная служба «Edo Agent Service»

В веб-интерфейсе ПК «Efros DO» в разделе «Объекты сети» → «Агенты» появится соответствующий агент, для которого будут применены проверки текущей политики безопасности.

3.9.2 Удаление агента ПК «Efros DO» на Windows

Для удаления агента ПК «Efros DO» на конечной точке с ОС Windows необходимо выполнить переход «Панель управления» → «Программы» → «Программы и компоненты» («Удаление программы»). В списке программ найти «EDO Agent», выбрать его и нажать кнопку «Удалить».

3.9.3 Установка агента ПК «Efros DO» на Linux

 Предварительно необходимо настроить подключение конечной точки к серверу ПК «Efros DO» по имени сервера: <https://edo-gateway-service>. Для обеспечения сетевой связанности необходимо зарегистрировать имя сервера «edo-gateway-service» в службе DNS.

При установке агента ПК «Efros DO» на контролируруемую конечную точку с ОС Astra Linux Special Edition или ОС Ubuntu необходимо использовать установочный файл **edo-agent-*<версия>.deb***.

При установке агента ПК «Efros DO» на контролируруемую конечную точку с РЕД ОС необходимо использовать установочный файл **edo-agent-*<версия>.rpm***.

Для установки агента необходимо выполнить следующие действия:

- 1) Скопировать на контролируруемую конечную точку необходимый файл.
- 2) В интерфейсе командной строки ввести следующие команды:

```
sudo dpkg -i edo-agent-1.0.0.deb  
systemctl start edo-agent.service
```

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

- 3) Установка агента ПК «Efros DO» завершена.

В веб-интерфейсе ПК «Efros DO» в разделе «Объекты сети» → «Агенты» появится соответствующий агент, для которого будут применены проверки текущей политики безопасности.

3.9.4 Удаление агента ПК «Efros DO» на Linux

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

Для удаления агента ПК «Efros DO» необходимо выполнить следующие действия:

- 1) В интерфейсе командной строки ввести следующие команды:

```
sudo apt-get purge edo-agent
```

- 2) Ввести пароль пользователя ОС.
- 3) Согласиться с выполнением операции.
- 4) Удаление агента ПК «Efros DO» завершено.

3.9.5 Установка агента ПК «Efros DO» на MacOS



Предварительно необходимо настроить подключение конечной точки к серверу ПК «Efros DO» по имени сервера: <https://edo-gateway-service>. Для обеспечения сетевой связанности необходимо зарегистрировать имя сервера «edo-gateway-service» в службе DNS.

При установке агента ПК «Efros DO» на контролируруемую конечную точку с ОС MacOS необходимо использовать установочный файл **edo-agent-<версия>.pkg**.

Для установки агента необходимо выполнить следующие действия:

- 1) Скопировать на контролируруемую конечную точку необходимый файл.
- 2) В интерфейсе командной строки ввести следующие команды:

```
sudo installer -pkg edo-agent-1.0.0.1.pkg -target /  
systemctl start edo-agent.service
```



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

- 3) Установка агента ПК «Efros DO» завершена.

В веб-интерфейсе ПК «Efros DO» в разделе «Объекты сети» → «Агенты» появится соответствующий агент, для которого будут применены проверки текущей политики безопасности.

3.9.6 Удаление агента ПК «Efros DO» на MacOS



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

Для удаления агента ПК «Efros DO» необходимо в интерфейсе командной строки ввести последовательно следующие команды:

```
sudo launchctl stop edo.agent  
sudo launchctl unload /Library/LaunchDaemons/edo.agent.plist
```

```
sudo rm /Library/LaunchDaemons/edo.agent.plist
sudo rm -rf /Applications/EDO/Agent.app
sudo pkgutil --forget gis.edo.agent
```

Удаление агента ПК «Efros DO» завершено.

3.10 Суппликант ПК «Efros DO»

Суппликант ПК «Efros DO» (суппликант) устанавливается на контролируемые конечные точки.

Суппликант предназначен для проверки требований политики безопасности на этапе подключения к корпоративной сети.

3.10.1 Установка суппликанта ПК «Efros DO» на Windows

- ⚠ Предварительно необходимо настроить подключение конечной точки к серверу ПК «Efros DO» по имени сервера: <https://edo-gateway-service>. Для обеспечения сетевой связанности необходимо зарегистрировать имя сервера «edo-gateway-service» в службе DNS.

Для установки суппликанта ПК «Efros DO» необходимо скопировать на контролируемую конечную точку с ОС Windows файл **edo-supPLICANT-*<версия>.msi*** и запустить его на исполнение.

Откроется окно мастера установки «EDO-SupPLICANT» (рис. 65).

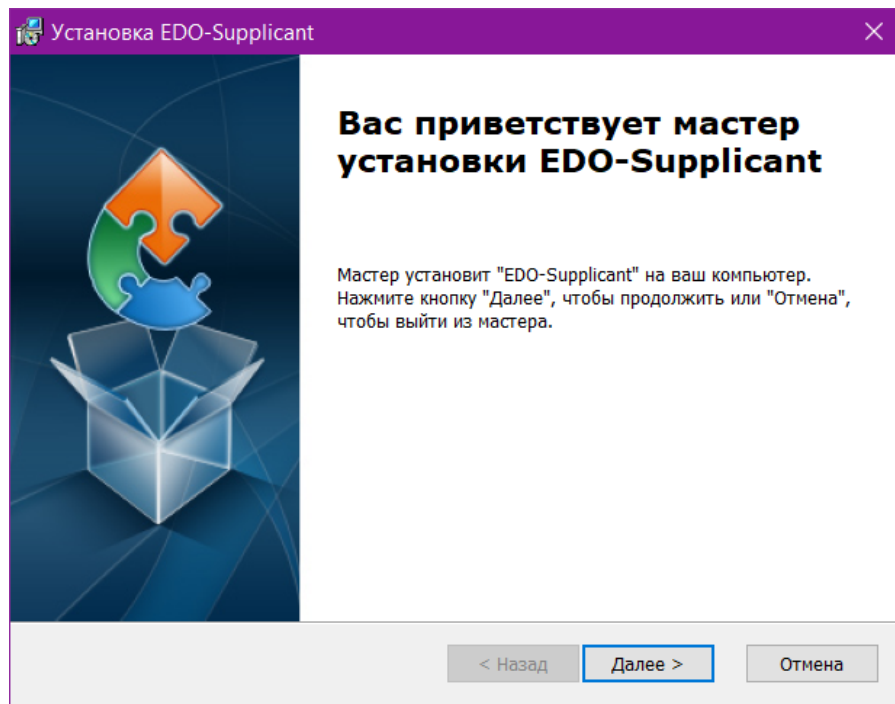


Рисунок 65 – Диалоговое окно мастера установки «EDO-Supplіcant»

В диалоговом окне мастера установки нажать кнопку «Далее».

Откроется диалоговое окно выбора папки установки, в котором следует выбрать папку для установки агента или оставить заданную по умолчанию (**C:\Program Files (x86)\EDO\Supplіcant**) и нажать кнопку «Далее» (рис. 66).

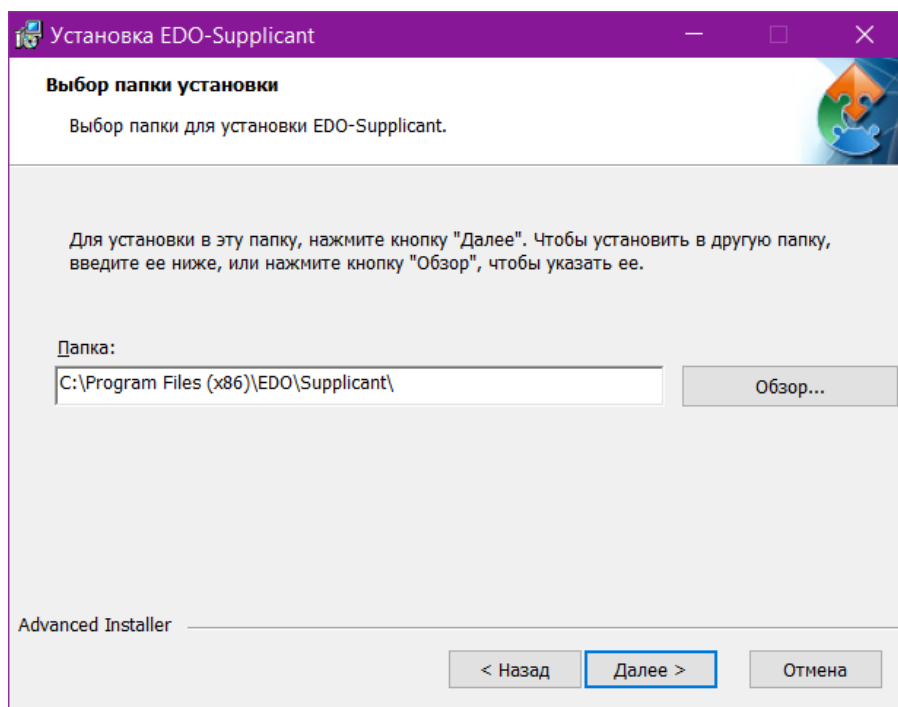


Рисунок 66 – Диалоговое окно выбора папки установки

В диалоговом окне готовности мастера к установке (рис. 67) для запуска процесса инсталляции с заданными ранее параметрами следует нажать кнопку «Установить».

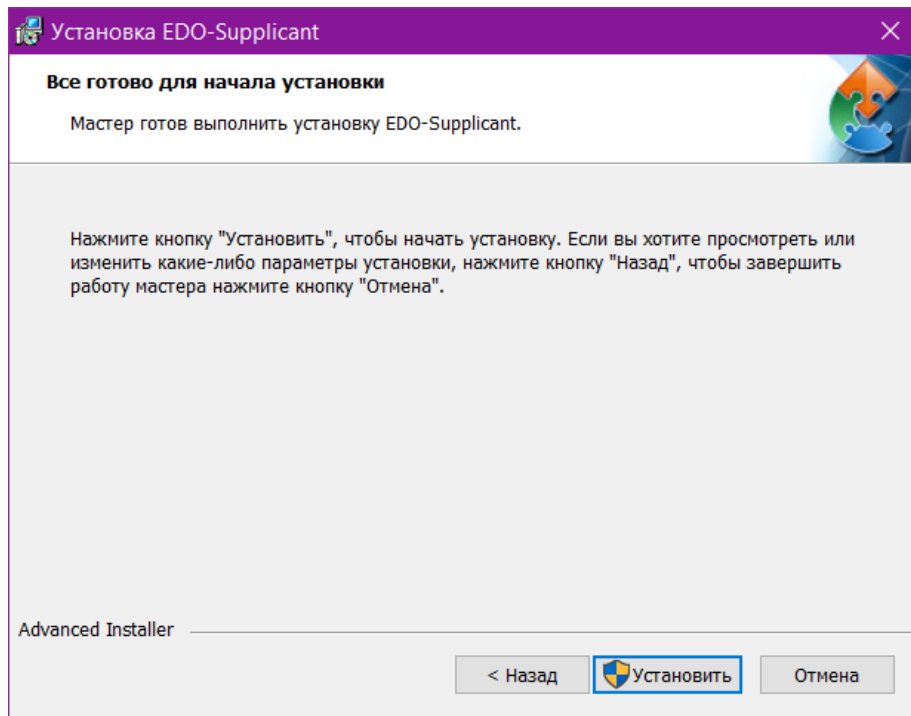


Рисунок 67 – Диалоговое окно готовности к установке

Ход установки «EDO-Suppliant» программного комплекса будет отображаться в окне мастера установки (рис. 68).

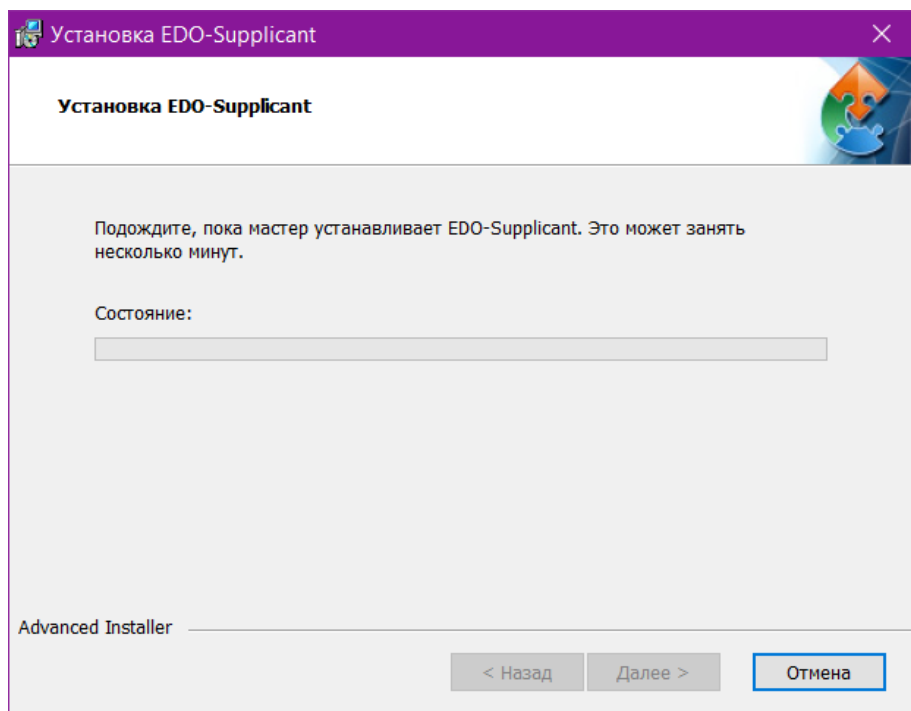



Рисунок 68 – Диалоговое окно процесса установки

-  При появлении диалогового окна ОС «Разрешить этому приложению вносить изменения на вашем устройстве?» следует нажать кнопку «Да».

После окончания установки «EDO-Supplicant» откроется диалоговое окно завершения работы мастера установки (рис. 69), в котором следует нажать кнопку «Готово».

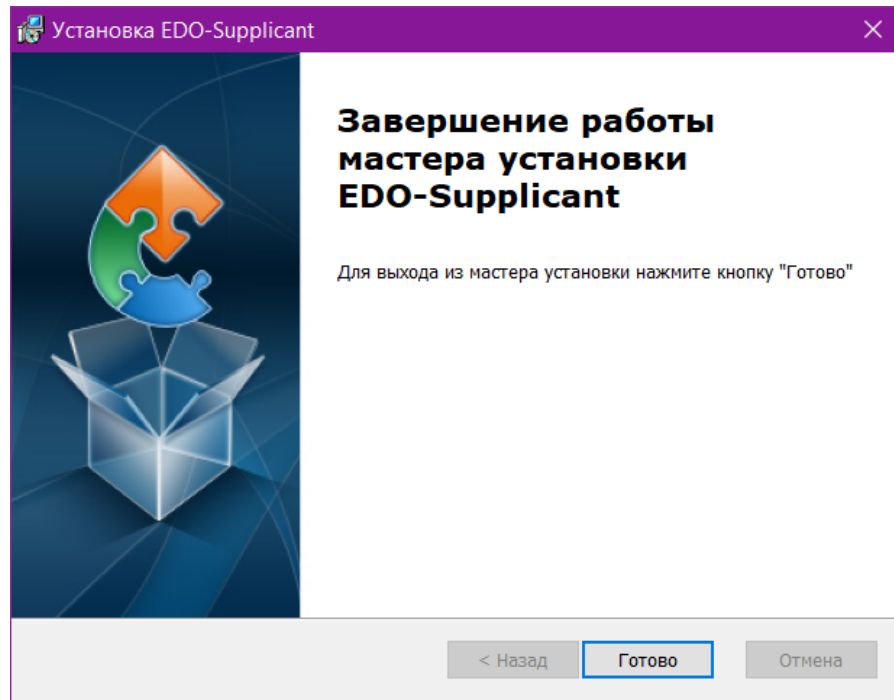



Рисунок 69 – Диалоговое окно завершения работы мастера установки

В окне программы «Службы» появится и автоматически запустится служба «Edo Supplicant Service».

3.10.2 Удаление суппликанта ПК «Efros DO» на Windows

Для удаления суппликанта ПК «Efros DO» на конечной точке с ОС Windows необходимо выполнить переход «Панель управления» → «Программы» → «Программы и компоненты» («Удаление программы»). В списке программ найти «EDO-Supplicant», выбрать его и нажать кнопку «Удалить».

3.10.3 Установка суппликанта ПК «Efros DO» на Linux

-  Предварительно необходимо настроить подключение конечной точки к серверу ПК «Efros DO» по имени сервера: <https://edo-gateway-service>. Для обеспечения сетевой связанности необходимо зарегистрировать имя сервера «edo-gateway-service» в службе DNS.

При установке суппликанта ПК «Efros DO» на контролируемую конечную точку с ОС Astra Linux Special Edition необходимо использовать установочный файл **edo-supplicant-**

<версия>.deb.

При установке суппликанта ПК «Efros DO» на контролируемую конечную точку с РЕД ОС необходимо использовать установочный файл **edo-supPLICANT-<версия>.rpm**.

Для установки суппликанта необходимо выполнить следующие действия:

- 1) Скопировать на контролируемую конечную точку необходимый файл.
- 2) В интерфейсе командной строки ввести следующую команду:

```
sudo apt install ./edo-supPLICANT-1.0.0.deb
```

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

- 3) При наличии нескольких сетевых интерфейсов требуется выбрать необходимый для настройки суппликанта, например, «eth1».
- 4) Установка суппликанта ПК «Efros DO» завершена.

3.10.4 Настройка параметров суппликанта ПК «Efros DO» на Linux

Для настройки суппликанта необходимо выполнить следующие действия:

- 1) Запустить суппликант. Откроется стартовое окно (рис. 70).

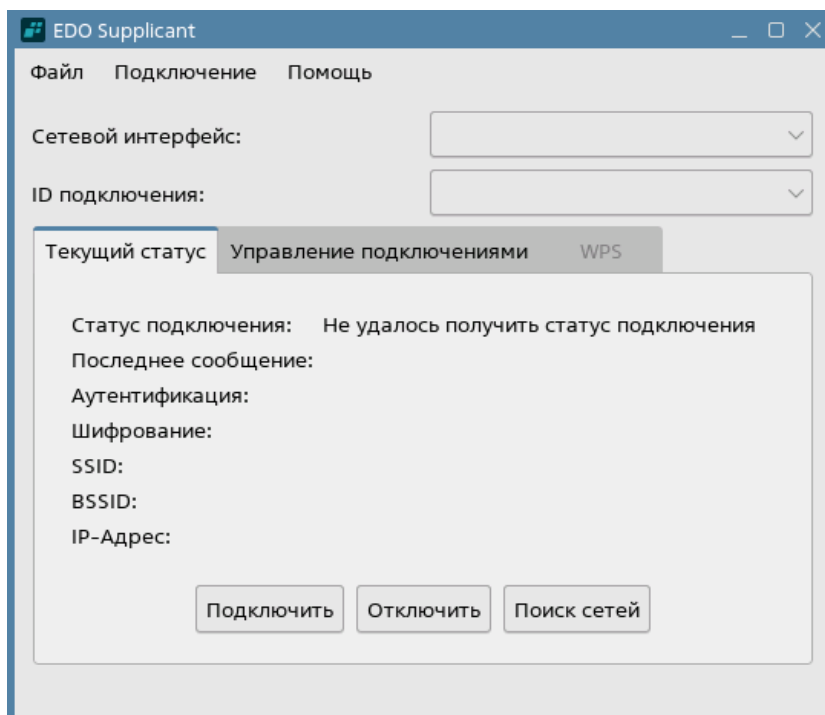


Рисунок 70 – Стартовое окно

- 2) Перейти на вкладку «Управление подключениями» (рис. 71). Для добавления нового

подключения необходимо нажать кнопку «Добавить». Для корректировки существующего подключения необходимо выбрать подключение из существующих и нажать кнопку «Изменить».

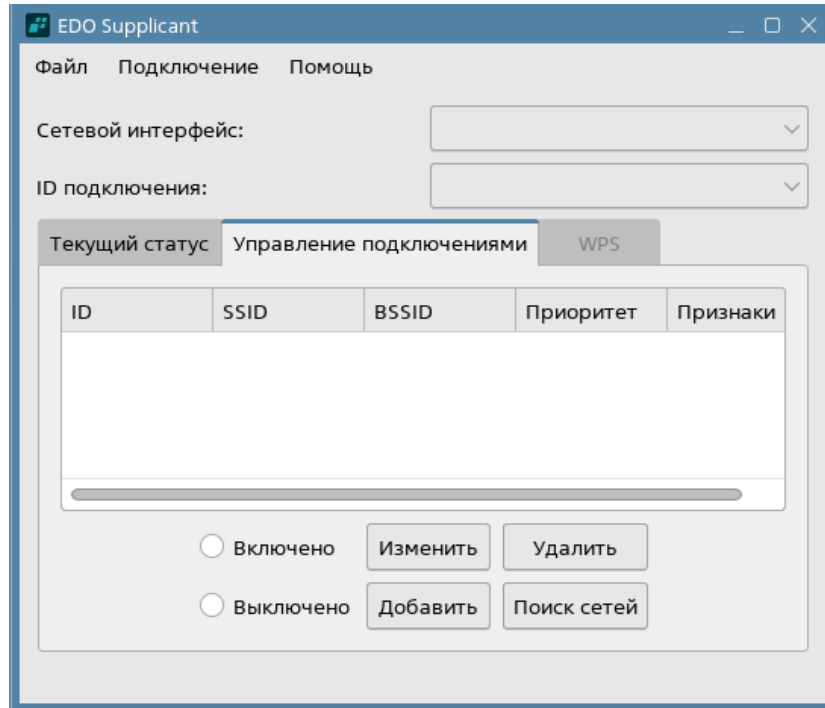


Рисунок 71 – Вкладка «Управление подключениями»

- 3) Откроется окно «Настройка подключения» (рис. 72). Заполнить поля требуемыми параметрами (рис. рис. 73). Состав и описание полей окна приведены в таблице 8.

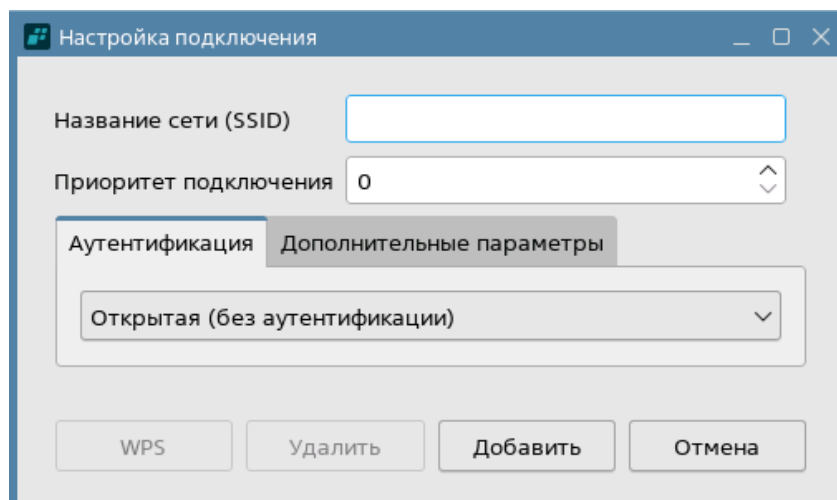


Рисунок 72 – Окно «Настройка подключения»

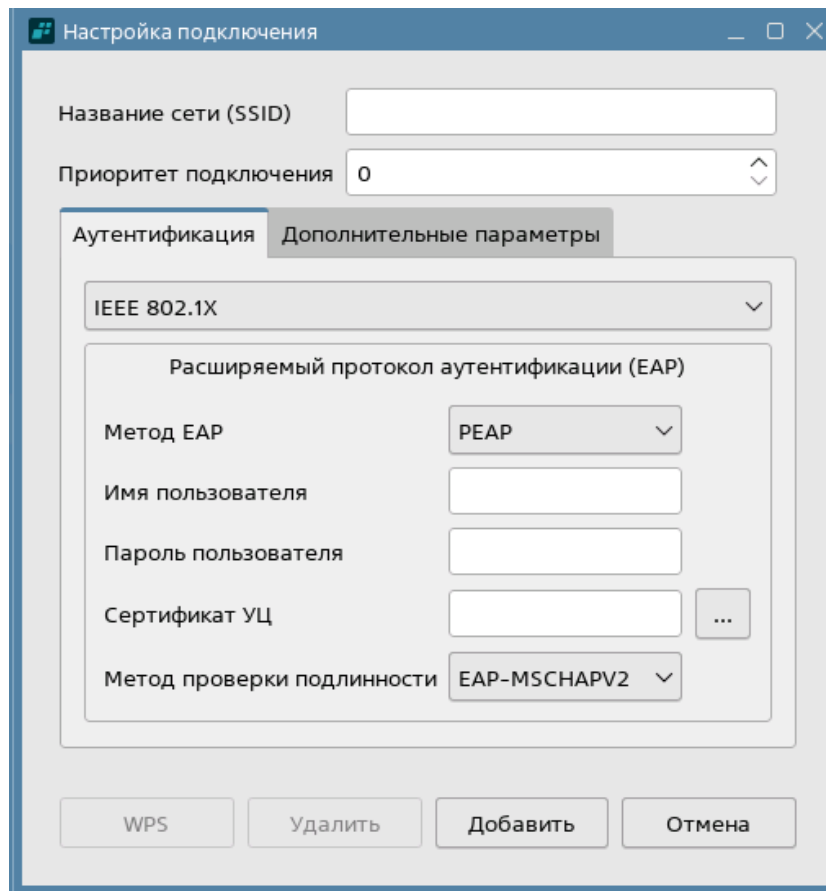


Рисунок 73 – Окно «Настройка подключения»

Таблица 8 – Состав и описание полей окна «Настройка подключения»

Поле	Описание
Поле «Название сети (SSID)»	Текстовое поле для ввода имени беспроводной сети. Для проводной сети поле не заполняется
Поле «Приоритет подключения»	Раскрывающийся список приоритетов подключения: — «0» – основной приоритет у подключения; — «1» – приоритет первого уровня; — «2» – приоритет второго уровня.
Группа полей вкладки «Аутентификация»	
Поле «Аутентификация»	Раскрывающийся список видов аутентификации: — «Открытая (без аутентификации)»; — «WEP (без аутентификации)»; — «WEP (Аутентификация с общим ключом)»; — «IEEE 802.1X» – для проводной сети; — «WPA-Personal (PSK)»; — «WPA-Enterprise (EAP)»; — «WPA2-Personal (PSK)»;

Поле	Описание
	— «WPA2-Enterprise (EAP)». В зависимости от выбора вида аутентификации выводятся дополнительные поля для заполнения
Группа полей для «Расширяемого протокола аутентификации (EAP)» при выборе метода EAP MD5 или TEAP	
Поле «Метод EAP»	MD5
Поле «Имя пользователя»	Поле для ввода логина пользователя, у которого есть доступ в сеть
Поле «Пароль»	Поле для ввода пароля пользователя, у которого есть доступ в сеть
Поле «Метод проверки подлинности»	Выбор отсутствует
Группа полей для «Расширяемого протокола аутентификации (EAP)» при выборе метода EAP TLS	
Поле «Метод EAP»	TLS
Поле «Имя пользователя»	Поле для ввода логина пользователя, у которого есть доступ в сеть
Поле «Пароль пользователя»	Поле для ввода пароля пользователя, у которого есть доступ в сеть
Поле «Сертификат УЦ»	Поле для добавления сертификата удостоверяющего центра в форматах «.pem», «.cer» или «.crt»
Поле «Сертификат клиента»	Поле для добавления сертификата организации, в которой расположена конечная точка с установленным суппликантом, в форматах «.pfx» или «.p12»
Поле «Закрытый ключ»	Поле для добавления закрытого ключа в формате файла «.key»
Поле «Метод проверки подлинности»	Выбор отсутствует
Группа полей для «Расширяемого протокола аутентификации (EAP)» при выборе метода EAP PEAP	
Поле «Метод EAP»	PEAP
Поле «Имя пользователя»	Поле для ввода логина пользователя, у которого есть доступ в сеть
Поле «Пароль пользователя»	Поле для ввода пароля пользователя, у которого есть доступ в сеть
Поле «Сертификат УЦ»	Поле для добавления сертификата удостоверяющего центра в форматах «.pem», «.cer» или «.crt»
*Поле «Сертификат УЦ (этап проверки	Поле для добавления сертификата удостоверяющего центра в форматах «.pem», «.cer» или «.crt»

Поле	Описание
подлинности)»	
*Поле «Сертификат клиента»	Поле для добавления сертификата организации, в которой расположена конечная точка с установленным суппликантом, в форматах «.pfx» или «.p12»
*Поле «Закрытый ключ»	Поле для добавления закрытого ключа в формате файла «.key»
Поле «Метод проверки подлинности»	<p>Раскрывающийся список методов проверки подлинности для метода EAP PEAP/TTLS:</p> <ul style="list-style-type: none"> — «EAP-GTS»; — «EAP-MSCHAPV2»; — «EAP-TLS». <p>Раскрывающийся список методов проверки подлинности для метода EAP FAST:</p> <ul style="list-style-type: none"> — «EAP-FAST MSCHAPV2»; — «EAP-MSCHAPV2»; — «EAP-TLS».
*Данные поля появляются при выборе в поле «Метод проверки подлинности» EAP-TLS	
Элементы управления	
WPS	Недоступна для выполнения действий
Удалить	При нажатии на кнопку введенные данные удаляются
Добавить	При нажатии на кнопку введенные данные сохраняются
Отмена	При нажатии на кнопку введенные данные не сохраняются

- 4) Нажать кнопку «Добавить».
- 5) Добавленное подключение автоматически подключится. На вкладке «Управление подключениями» появится добавленное подключение. На вкладке «Текущий статус» отобразятся данные по подключению (рис. 74).

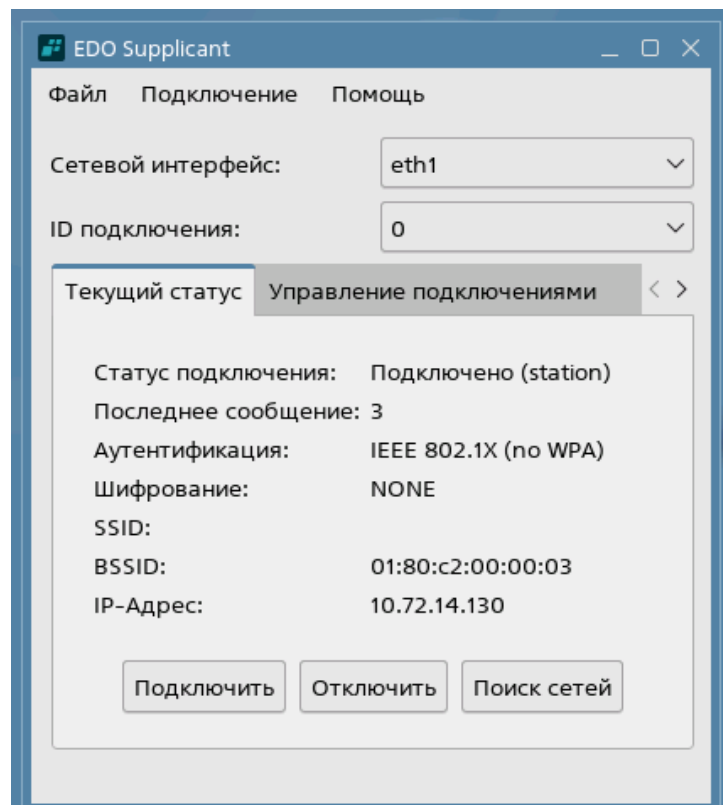


Рисунок 74 – Вкладка «Текущий статус»

3.10.5 Удаление суппликанта ПК «Efros DO» на Linux

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

Для удаления суппликанта ПК «Efros DO» необходимо выполнить следующие действия:

- 1) В интерфейсе командной строки ввести следующую команду:

```
sudo apt-get purge edo-supPLICANT
```

- 2) Ввести пароль пользователя ОС.
- 3) Согласиться с выполнением операции.
- 4) Удаление суппликанта ПК «Efros DO» завершено.

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 запустить скрипт **deploy.sh** 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 данного 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
NTP	–	Network Time Protocol
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