

**ООО «Гефест Технолоджиз»**

ИНН: 7100029285; ОГРН: 1227100014195; КПП: 710001001.

**Программный комплекс автоматизации  
ситуационного центра информационной  
безопасности «Эгида»**

**Пошаговая инструкция по установке  
экземпляра программного обеспечения**

**(для проведения экспертной оценки в Экспертном совете  
при Минцифры России)**

# Оглавление

<b>1. ОБЩИЕ СВЕДЕНИЯ .....</b>	<b>3</b>
<b>2. СИСТЕМНЫЕ ТРЕБОВАНИЯ .....</b>	<b>3</b>
2.1. МИНИМАЛЬНЫЕ АППАРАТНЫЕ ТРЕБОВАНИЯ.....	3
2.2. ПРОГРАММНЫЕ ТРЕБОВАНИЯ.....	3
<b>3. УСТАНОВКА.....</b>	<b>4</b>
<b>4. ЗАПУСК.....</b>	<b>10</b>
<b>5. СОСТАВ МОДУЛЕЙ И КОМПОНЕНТОВ .....</b>	<b>12</b>
5.1. СОБСТВЕННЫЕ КОМПОНЕНТЫ.....	12
5.2. СТОРОННИЕ РЕШЕНИЯ.....	14
5.3. РЕКОМЕНДАЦИИ ПО МОНИТОРИНГУ КОМПОНЕНТ .....	14
<b>6. КОНТАКТЫ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ .....</b>	<b>15</b>

## 1. ОБЩИЕ СВЕДЕНИЯ

Программный комплекс автоматизации ситуационного центра информационной безопасности «Эгида» представляет собой веб-приложение. Серверная часть веб-приложения требует установки необходимой инфраструктуры. Клиентская часть выполняется и отображается веб-браузером.

## 2. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Комплект поставки состоит из OVA-файла (`Aegis.ova`) образа виртуальной машины с развернутой инфраструктурой серверной части программного комплекса автоматизации ситуационного центра информационной безопасности «Эгида». Ниже приведены требования к ПК, используемому для установки программного комплекса из файла образа. Дальнейшая работа с программным комплексом может осуществляться на этом же ПК.

### 2.1. Минимальные аппаратные требования

Для установки и работы программного комплекса требуется ПК следующей конфигурации:

- процессор: 12 ядер;
- ОЗУ: 32 ГБ;
- диск: 100 ГБ свободного пространства.

### 2.2. Программные требования

На ПК требуется наличие установленного дополнительного программного обеспечения:

- Система виртуализации, поддерживающая OVA-файлы. В инструкции ниже используется ОС Windows и система виртуализации Oracle VM VirtualBox, актуальную версию которой можно скачать по адресу: <https://www.virtualbox.org/wiki/Downloads>.
- Веб-браузер (любая из последних двух актуальных версий Google Chrome, Яндекс Браузер, Microsoft Edge или Mozilla Firefox).

### 3. УСТАНОВКА

Установка осуществляется в систему виртуализации VirtualBox импортированием файла образа виртуальной машины из комплекта поставки (Aegis.ova).

Для начала установки запустите систему виртуализации VirtualBox. Чтобы импортировать образ виртуальной машины и запустить ее, выполните следующие действия (ниже представлены снимки экрана из VirtualBox версии 7):

1. Нажмите кнопку «Импортировать» на панели команд (Рисунок 1).

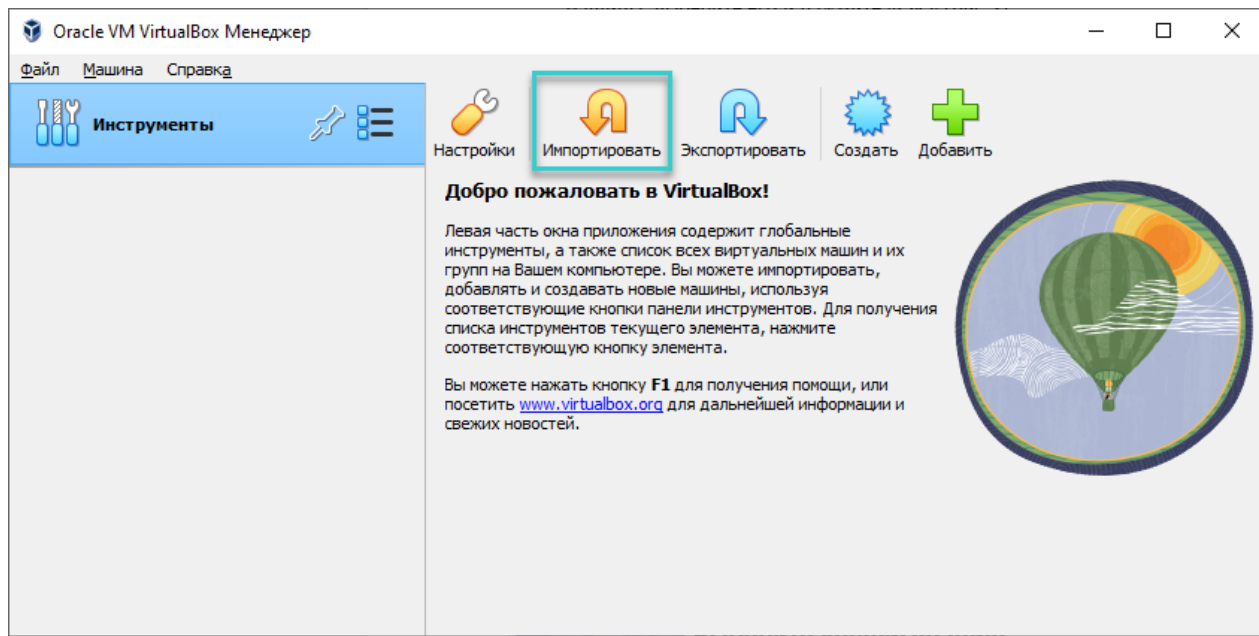
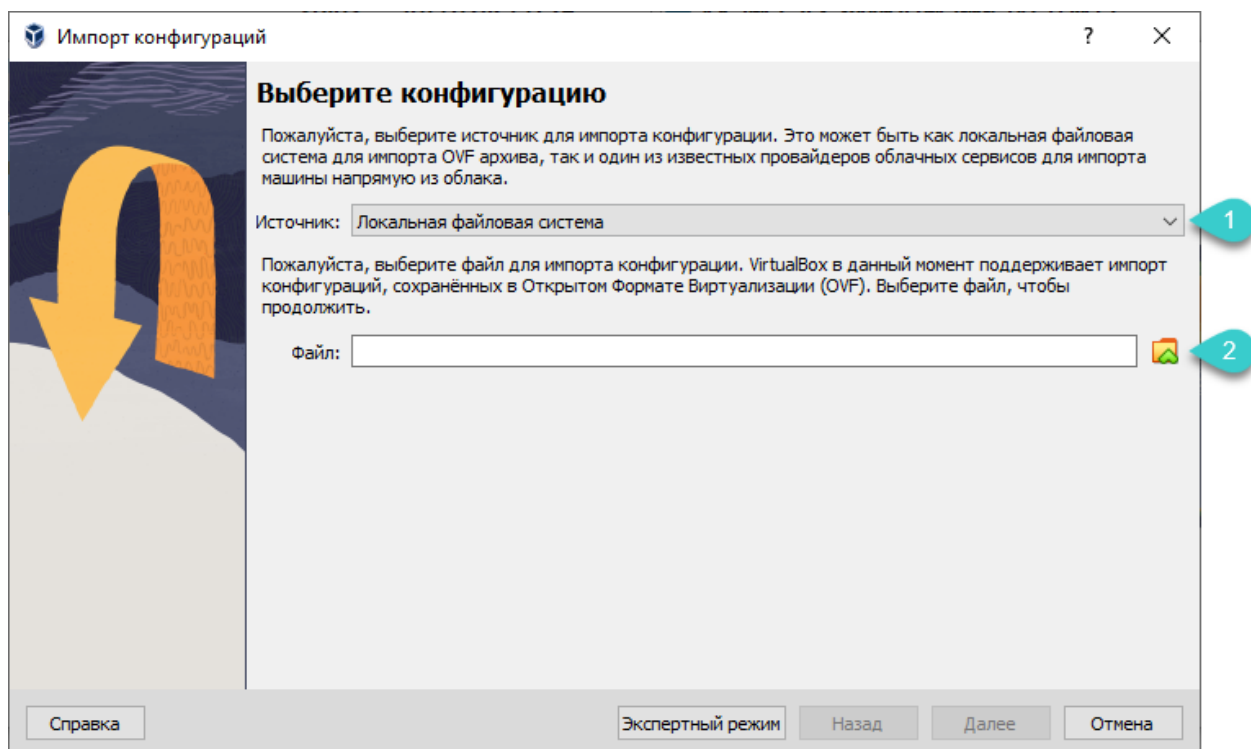


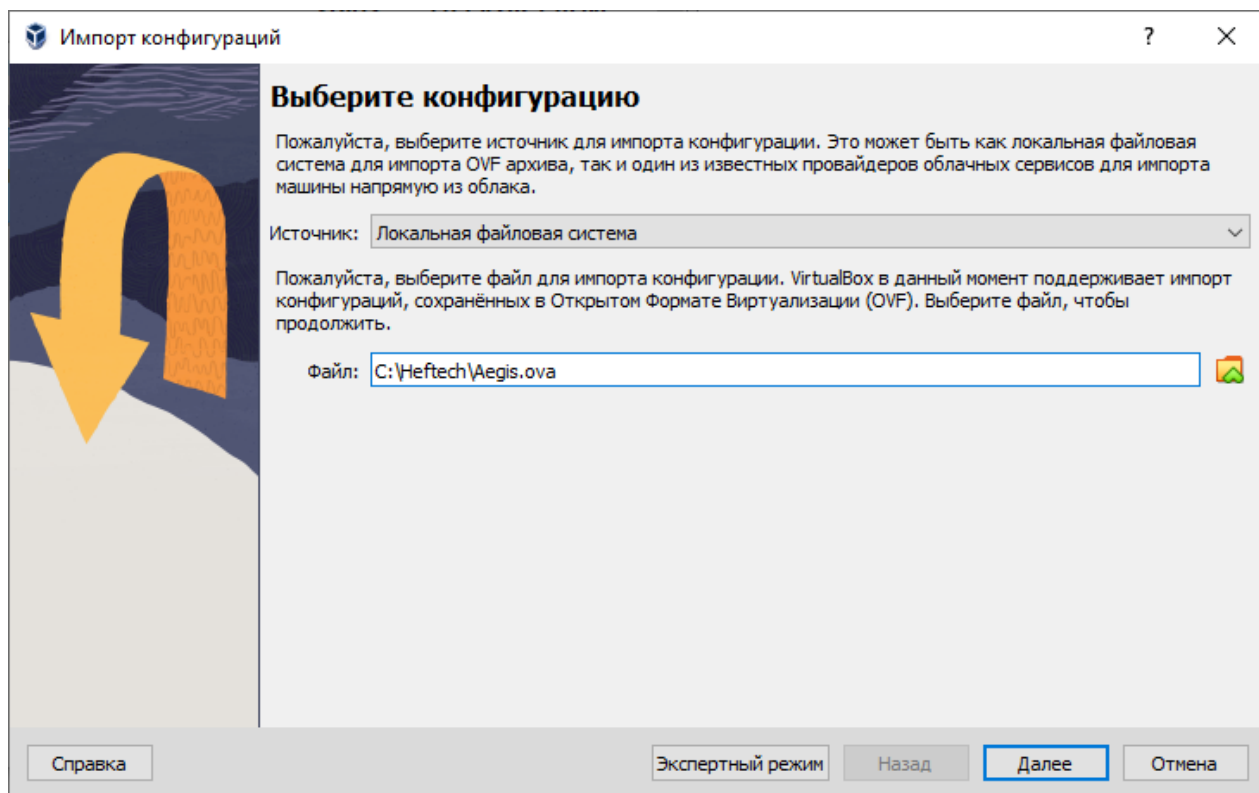
Рисунок 1 – Панель команд (импортирование образа)

2. В открывшемся окне «Импорт конфигураций» выберите в поле «Источник» опцию «Локальная файловая система» и у поля «Файл» нажмите на значок папки (Рисунок 2).



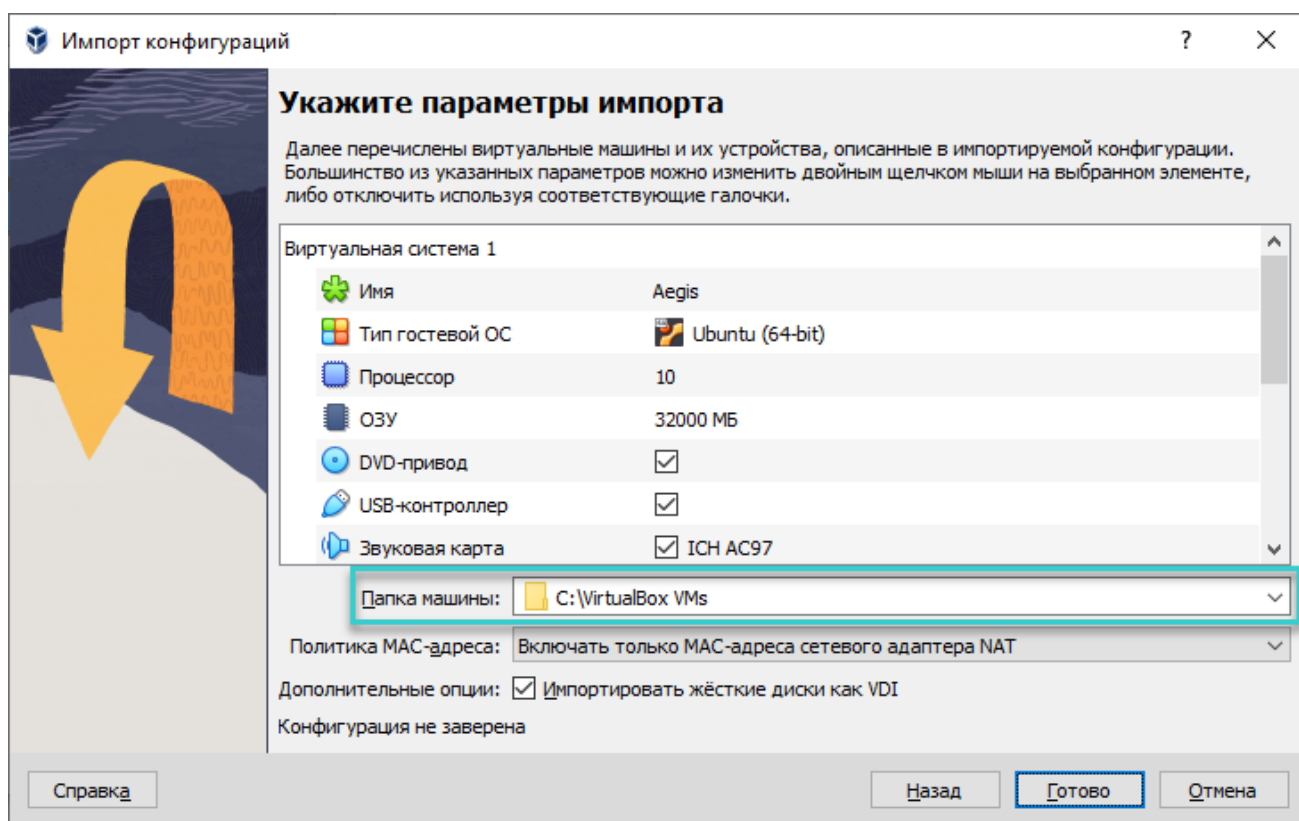
**Рисунок 2 – Выбор конфигурации для импорта**

3. В открывшемся окне «Укажите файл для импорта конфигураций» перейдите в папку с файлом образа виртуальной машины, выберите его и нажмите кнопку «Открыть».
4. В окне «Импорт конфигураций» нажмите кнопку «Далее» (Рисунок 3).



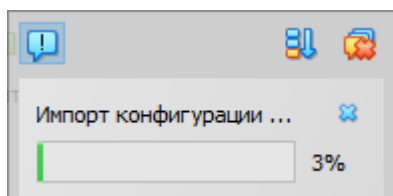
**Рисунок 3 – Выбранная конфигурация для импорта**

5. На открывшейся странице в поле «Папка машины» выберите путь, где будут располагаться файлы импортируемой виртуальной машины. Остальные параметры импорта оставьте без изменения (Рисунок 4) и нажмите кнопку «Готово».



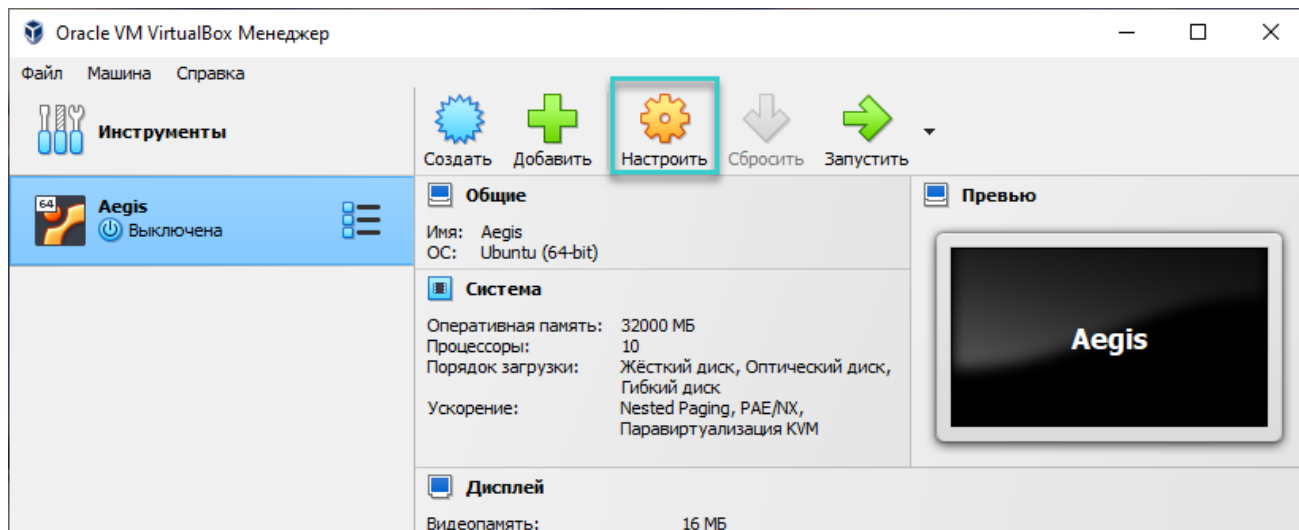
**Рисунок 4 – Параметры импорта**

6. Окно «Импорт конфигураций» закроется, и появится окно с индикацией прогресса импорта (Рисунок 5).



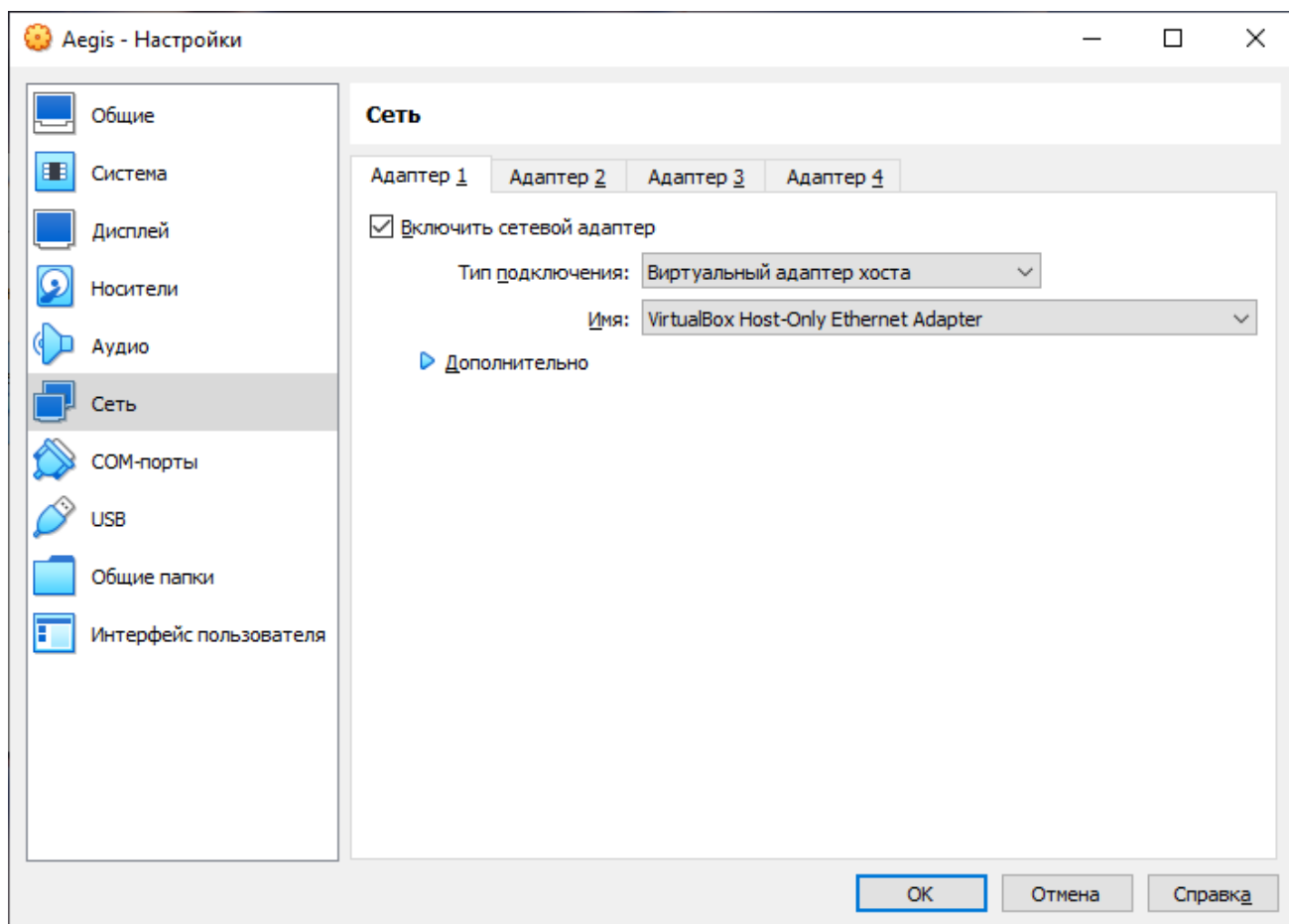
**Рисунок 5 – Индикация прогресса импорта**

7. Дождитесь завершения импорта, затем выберите импортированную машину Aegis в списке виртуальных машин и нажмите значок «Настроить» для изменения ее настроек (Рисунок 6).



**Рисунок 6 – Панель команд (переход в настройки виртуальной машины)**

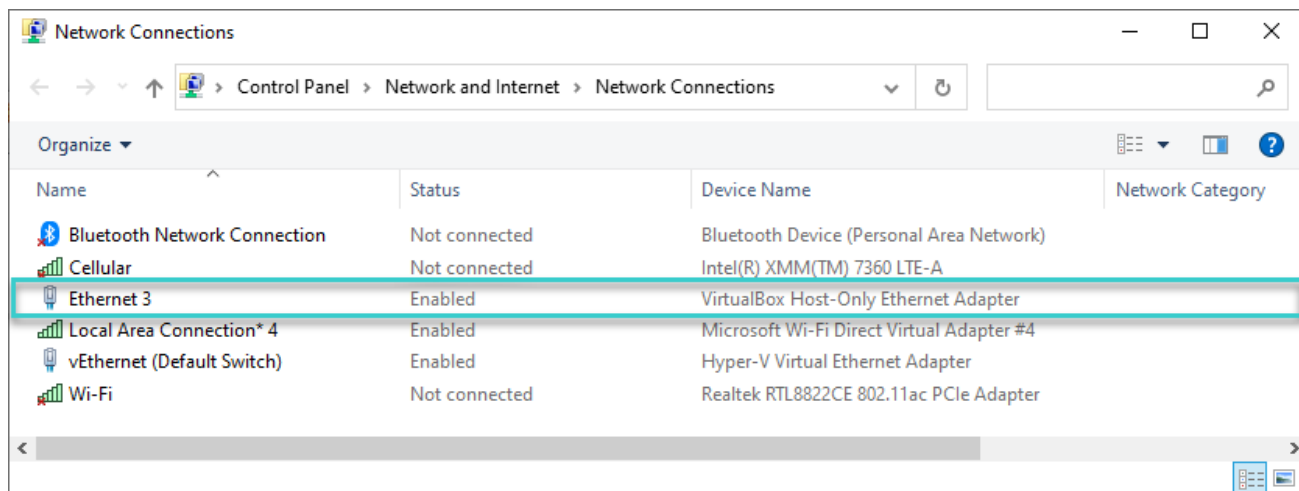
8. В открывшемся окне «Настройки» выберите раздел «Сеть» и убедитесь, что на закладке «Адаптер 1» установлены следующие параметры (Рисунок 7). Нажмите кнопку «ОК», чтобы закрыть окно «Настройки» и применить параметры.



**Рисунок 7 – Сетевые настройки виртуальной машины**

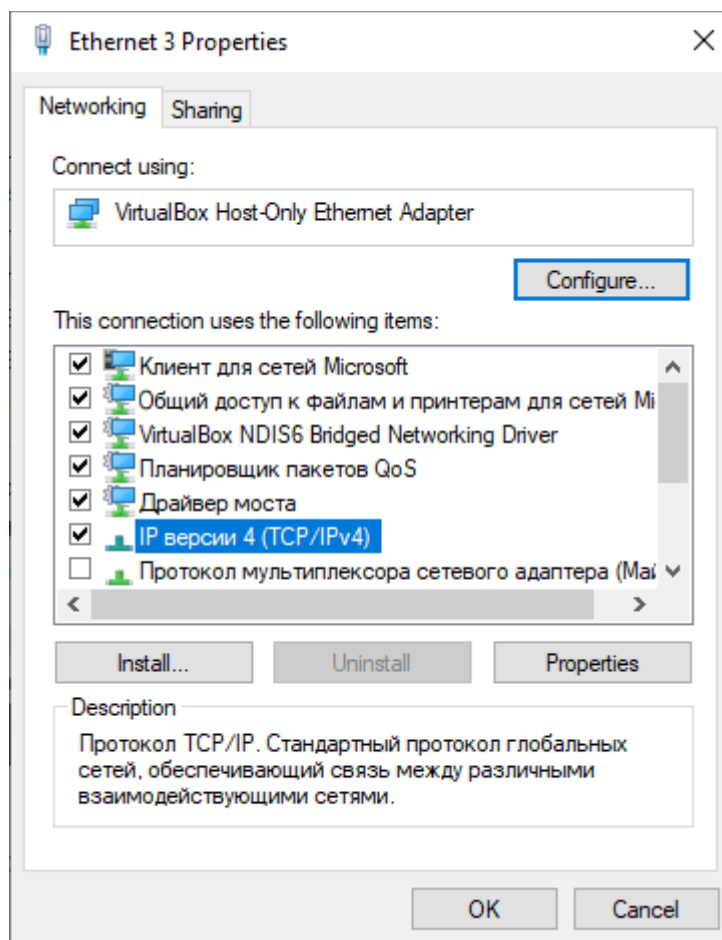
9. В системных настройках ПК пользователя (ниже представлены снимки экрана ОС Windows 10) запустите консоль «Сетевые подключения» | «Network Connections» (полный путь: «Панель управления\Сеть и Интернет\Сетевые подключения» | «Control Panel\Network and

Internet\Network Connections»). В списке подключений найдите сетевой адаптер с именем «VirtualBox Host-Only Ethernet Adapter» в колонке «Имя устройства» | «Device Name» (Рисунок 8) и откройте его свойства, нажав пункт «Свойства» | «Properties» в контекстном меню.



**Рисунок 8 – Сетевые подключения (адаптер виртуальной машины)**

10. В открывшемся окне свойств адаптера, в списке компонентов выберите «IP версии 4 (TCP/IPv4)» и откройте его свойства, нажав кнопку «Свойства» | «Properties» (Рисунок 9).

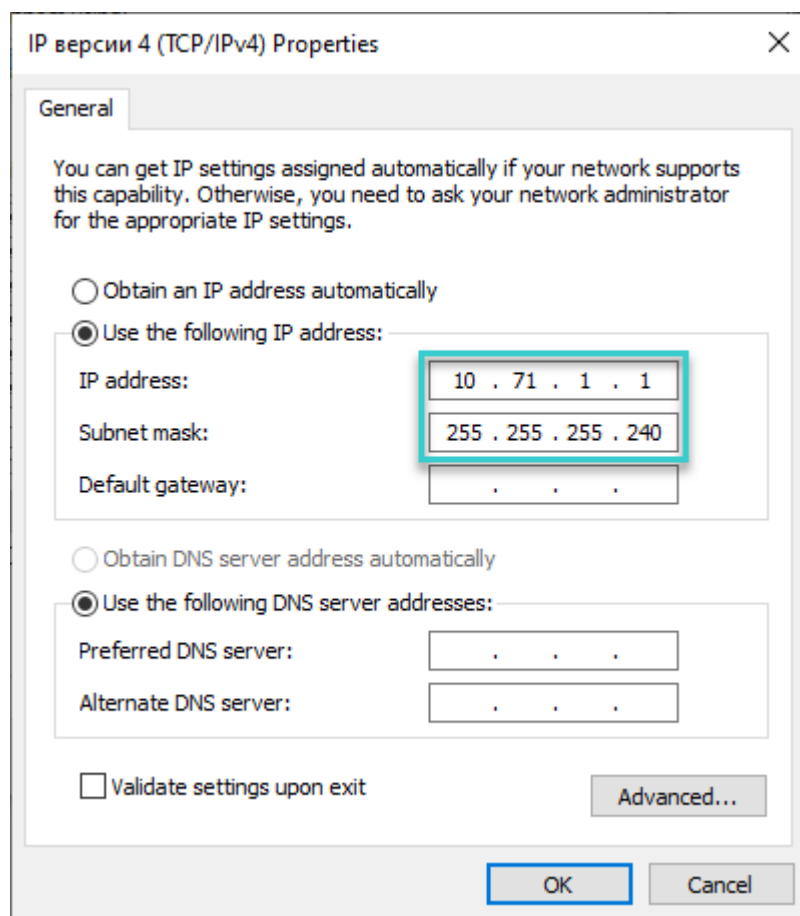


**Рисунок 9 – Свойства адаптера виртуальной машины**



11. В открывшемся окне свойств компонента задайте следующие значения параметров (Рисунок 10):

- «IP address» | «IP-адрес»: 10.71.1.1;
- «Subnet mask» | «Маска подсети»: 255.255.255.240.



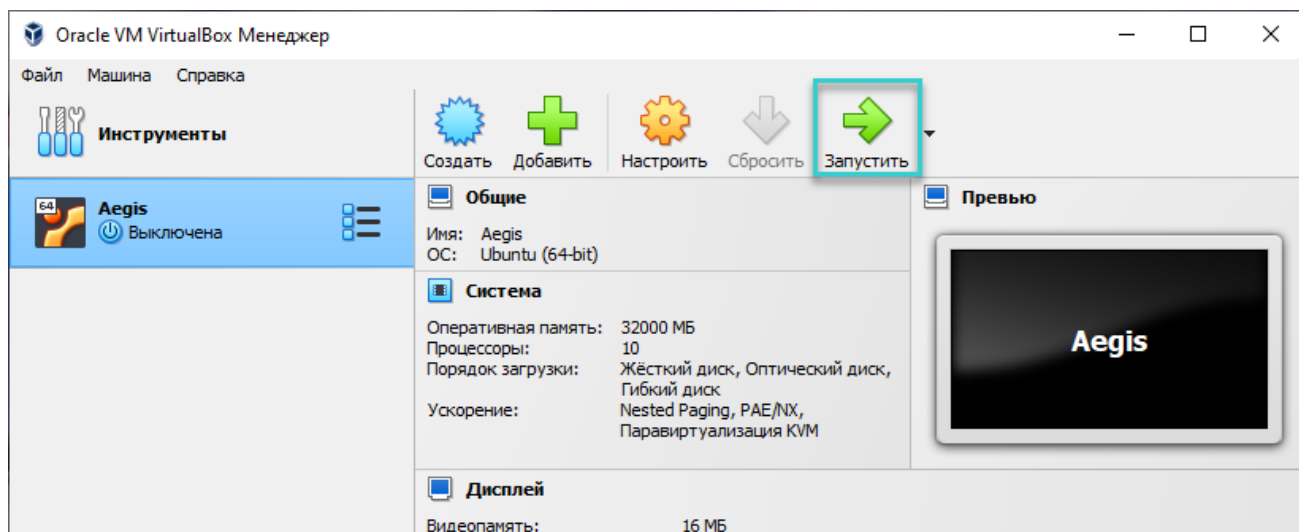
**Рисунок 10 – Свойства компонента «IP версии 4 (TCP/IPv4)»**

12. Нажмите кнопку «ОК», чтобы закрыть окно и применить изменения.

13. Нажмите кнопку «ОК» в окне свойств адаптера, чтобы закрыть это окно и применить изменения.

14. На ПК пользователя добавьте следующую строку в файл hosts, находящийся в папке %SystemRoot%\System32\drivers\etc, и сохраните изменения в этом файле:  
10.71.1.9 siem.aio.local

15. Перейдите в окно приложения «Oracle VM VirtualBox Менеджер» и нажмите значок «Запустить» для старта виртуальной машины Aegis (Рисунок 11).



**Рисунок 11 – Панель команд (запуск виртуальной машины)**

16. В результате успешного старта в консоли виртуальной машины появятся следующие сообщения о запущенной ОС Ubuntu (Рисунок 12).

```
Ubuntu 22.04.1 LTS node1 tty1
node1 login: _
```

**Рисунок 12 – Консоль виртуальной машины (запущена ОС Ubuntu)**

17. Дождитесь завершения инициализации инфраструктуры серверной части Системы (запуска сервисов и инициализации компонент). В зависимости от быстродействия ПК это может потребовать до 40 минут. Индикацией завершения инициализации и готовности к работе служит сообщение «Aegis started» (Рисунок 13).

```
Ubuntu 22.04.1 LTS node1 tty1
node1 login: [ 2258.173784] Aegis started
_
```

**Рисунок 13 – Консоль виртуальной машины (готовность к работе)**

## 4. ЗАПУСК

На ПК пользователя откройте веб-браузер и в адресной строке введите: <https://siem.aio.local/>

Появится окно авторизации программного комплекса (Рисунок 14).

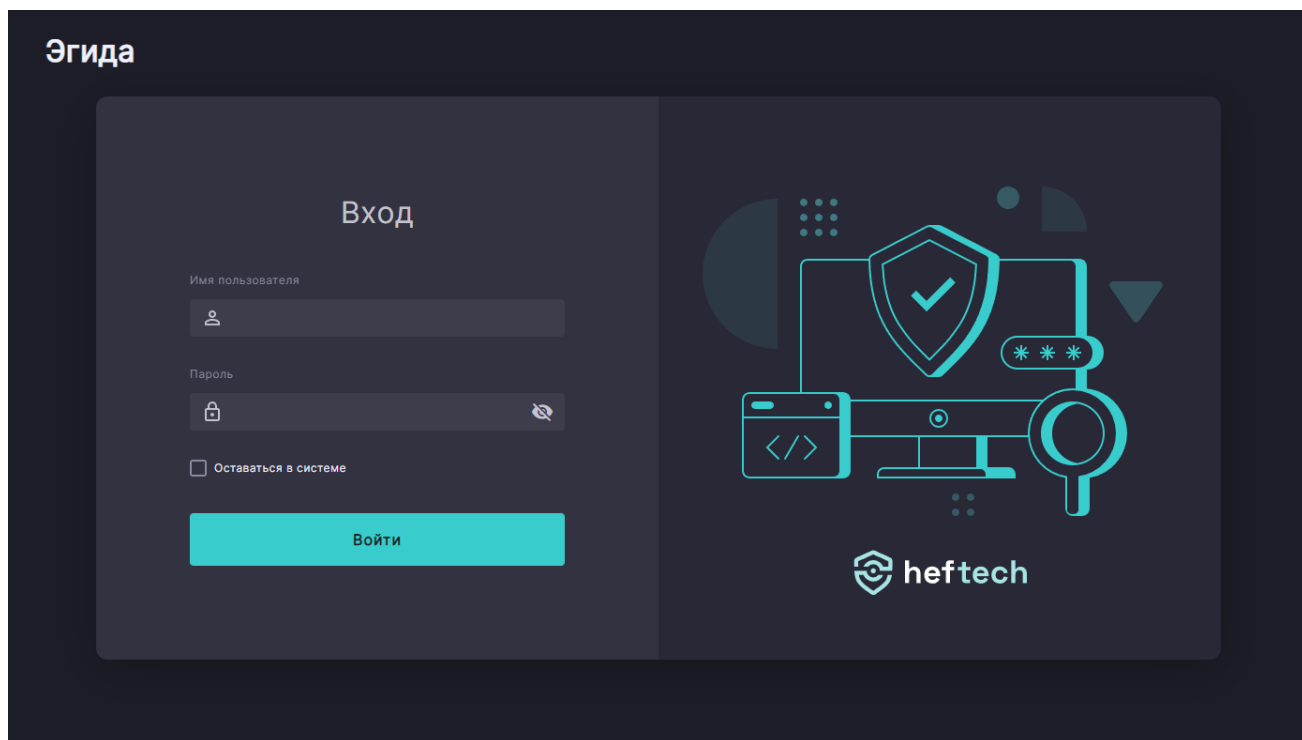


Рисунок 14 – Окно авторизации программного комплекса

Для входа введите следующие учетные данные.

Имя пользователя: siem\_admin

Пароль: aj\_z7ddb2\*\_JpJe4cJd9

Отобразится интерфейс управления программным комплексом.

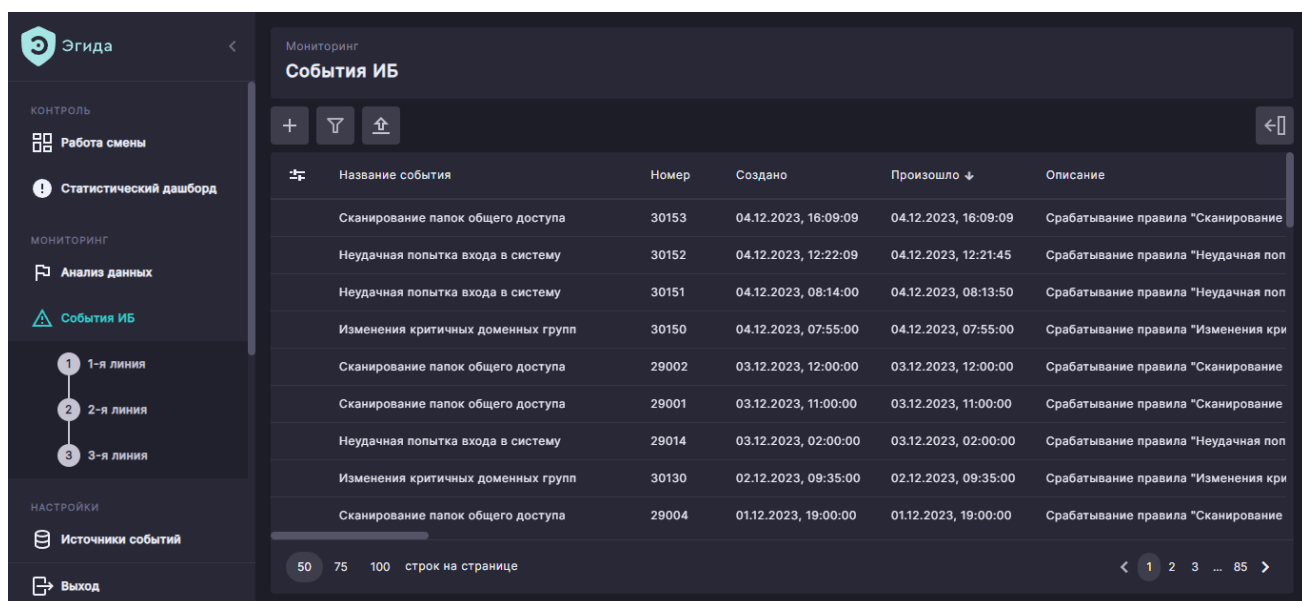


Рисунок 15 – Окно интерфейса управления программным комплексом

В установленном программном комплексе присутствуют демонстрационные данные за период 4 декабря 2022 г. – 4 декабря 2023 г.

## 5. СОСТАВ МОДУЛЕЙ И КОМПОНЕНТОВ

Программный комплекс представляет из себя веб-приложение, а также системы сбора, подготовки, хранения, мониторинга и корреляции событий. Программный комплекс использует модульную архитектуру и разворачивается в кластере Kubernetes версии 1.27. Модуль состоит из комплекта контейнеров с компонентами внутри. Внутри контейнеров файлы компонентов модулей с префиксом aegis находятся в директории /app.

Функциональное деление модулей:

- Обеспечение работы веб-приложения (модули aegis-domain-service, aegis-control-center-server, aegis-event-storage, aegis-signaler-hub и aegis-control-center-client). В кластере компоненты модулей находятся в пространстве имен aegis.
- Обработка событий и анализ на предмет потенциальных угроз информационной безопасности (модули aegis-alert-mover, aegis-persistent-storage-publisher-enriched, aegis-persistent-storage-publisher-raw, aegis-normalizer, aegis-correlation и aegis-midas). В кластере компоненты модулей находятся в пространстве имен aegis.
- Оповещение пользователей программного комплекса (модули aegis-notifier-service, aegis-notifier-service, aegis-telegram-processor и aegis-email-processor). В кластере компоненты модулей находятся в пространстве имен aegis.
- Хранение данных внутри кластера (модуль Longhorn). В кластере компоненты модуля находятся в пространстве имен longhorn-system.
- Организация сети внутри кластера (модуль Cilium). В кластере компоненты модуля находятся совместно с другими системными модулями Kubernetes в пространстве имен kube-system.
- Обеспечение доступа извне к веб-приложению внутри кластера (модуль ingress-nginx). В кластере компоненты модуля находятся внутри пространства имен ingress-nginx.

### 5.1. Собственные компоненты

Компонент	Базовый образ	Описание
aegis-alert-mover	dotnet/sdk:8.0	Передача событий ИБ от коррелятора бэкенду
aegis-audit	dotnet/sdk:8.0	Аудит действий пользователя программного комплекса
aegis-control-center-client	dotnet/sdk:8.0	Клиентское приложение (HTML, CSS, VueJS)
aegis-control-center-server	dotnet/sdk:8.0	API для клиентского приложения пользователей программного комплекса

<b>Компонент</b>	<b>Базовый образ</b>	<b>Описание</b>
aegis-domain-service	dotnet/sdk:8.0	API доступа компонентов программного комплекса к базе данных
aegis-event-storage	dotnet/sdk:8.0	API доступа к хранилищу событий
aegis-correlation	openjdk-17	Корреляция событий
aegis-midas	openjdk-17	Обогащение событий
aegis-curator	dotnet/sdk:8.0	Оповещение агента об изменении настроек
aegis-edr-service	dotnet/sdk:8.0	EDR-сервис
aegis-normalizer	dotnet/sdk:8.0	Нормализация событий
aegis-persistent-storage-publisher-raw	dotnet/sdk:8.0	Публикация исходных событий в хранилище
aegis-persistent-storage-publisher-enriched	dotnet/sdk:8.0	Публикация обогащенных событий в хранилище
aegis-notification-data-service	dotnet/sdk:8.0	API для сервиса оповещений
aegis-notifier-service	dotnet/sdk:8.0	Сервис оповещений
aegis-signalr-hub	dotnet/sdk:8.0	Сервис оповещения для графического интерфейса
aegis-telegram-processor	dotnet/sdk:8.0	Сервис отправки оповещений в Telegram
aegis-email-processor	dotnet/sdk:8.0	Сервис отправки оповещений по электронной почте

## 5.2. Сторонние решения

Компонент	Базовый образ	Описание
clickhouse	clickhouse-server:23.7	Колоночная база данных ClickHouse
kafka	quay.io/strimzi/kafka:0.34 .0-kafka-3.3.2	Менеджер сообщений Kafka
postgresql-db	postgres:14.4	СУБД PostgreSQL
consul	hashicorp/consul:1.16	Хранилище конфигураций Consul
collector	logstash:0.3.131	Сборщик событий Logstash
schema-registry	confluentinc/cp-schema- registry:7.2.1	Хранилище структуры сообщений Schema Registry

## 5.3. Рекомендации по мониторингу компонент

В виртуальной машине установлена и настроена графическая оболочка [k9s](#), позволяющая производить мониторинг запущенных компонентов программного комплекса. Для запуска оболочки k9s введите учетные данные пользователя ОС, имеющего полномочия на выполнения команд от имени суперпользователя:

Имя пользователя: `aegis`

Пароль: `aegis`

Затем выполните команду `k9s`. Отобразится графическая оболочка со списком запущенных компонентов программного комплекса (Рисунок 15).

```


Context: kubernetes-admin@cluster.local
Cluster: cluster.local
User: kubernetes-admin
K9s Rev: v0.28.2
K8s Rev: v1.27.7
CPU: 56%
MEM: 24%

```

```

<0> all
<1> kube-system
<2> longhorn-system
<3> default

```



---

Pods (all) [43]

NAMESPACE↑	NAME	PF	READY	RESTARTS	STA
aegis	aegis-audit-565c4995d-9vkw8	•	1/1	13	Run
aegis	aegis-control-center-client-9c46f7b5d-b6541	•	1/1	25	Run
aegis	aegis-control-center-server-766cc78c8-xh2vp	•	1/1	9	Run
aegis	aegis-domain-service-78cc4b89fc-fctgf	•	1/1	0	Run
aegis	aegis-event-storage-784bf4c7ff-fk7f9	•	1/1	3	Run
aegis	aegis-kafka-cluster-entity-operator-5cb87c56d-nz6bd	•	3/3	241	Run
aegis	aegis-kafka-cluster-kafka-0	•	1/1	9	Run
aegis	aegis-kafka-cluster-kafka-exporter-6f6c8c5b77-khps7	•	1/1	55	Run
aegis	aegis-kafka-cluster-zookeeper-0	•	1/1	12	Run
aegis	aegis-signalr-hub-7f5f454f58-cjvw1	•	1/1	4	Run
aegis	chi-clickhouse-cluster-aegis-0-0-0	•	1/1	2	Run
aegis	clickhouse-keeper-0	•	1/1	0	Run
aegis	confluent-schema-registry-6c89f4866c-vs5hp	•	1/1	518	Run
aegis	postgresql-db-0	•	1/1	1	Run
aegis	strimzi-cluster-operator-65c4474f6-7qf5q	•	1/1	111	Run
aegis	strimzi-registry-operator-bfd4c6d5c-5vjr2	•	1/1	5	Run
ingress-nginx	ingress-nginx-controller-mhtvq	•	1/1	8	Run
kube-system	calico-kube-controllers-f58b6455c-qlpm6	•	1/1	60	Run
kube-system	calico-node-c92zx	•	1/1	57	Run

Рисунок 15 – Окно графической оболочки мониторинга компонент

## 6. КОНТАКТЫ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Тел.: +79038404433

Email: [info@heftech.ru](mailto:info@heftech.ru)