



# **AVSOFT KAIROS v2**

**Система защиты от спама и фишинга**

**Руководство по развертыванию**

**Москва  
2024 г**

## **Контактная информация**

127106, г. Москва, ул. Гостиничная, д.5

Тел.: +7 (495) 988-92-25 E-mail:

office@avsw.ru

www.avsw.ru/about/contacts

## **Авторское право**

ООО «АВ Софт» www.avsw.ru

© 2010-2024 ООО «АВ Софт»

## **Версия документа**

Апрель 10, 2024.

Настоящий документ является собственностью ООО «АВ Софт» (далее — «АВ Софт») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «АВ Софт».

Документ может быть изменен без предварительного уведомления.

## Содержание

1	Термины и определения .....	4
2	Описание поставки ПО KAIROS v2.....	4
3	Описание развертывания комплекса.....	5
4	Настройка сервиса менеджмента .....	9
5	Настройки в веб-интерфейсе .....	10

## 1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице 1.

Таблица 1. Термины и определения

№	Термин	Определение
1.	Primary interface	Основной интерфейс для общения между сенсором и сервисом менеджмента.
2.	Load interface	Интерфейс для загрузки данных

В настоящем документе используется перечень сокращений, представленный в таблице 2.

Таблица 2. Перечень сокращений

№	Сокращение	Значение
1.	АРМ	Автоматизированное рабочее место
2.	ПО	Программное обеспечение
3.	ВМ	Виртуальная машина
4.	VLAN	Virtual Local Area Network

## 2 Описание поставки ПО KAIROS v2

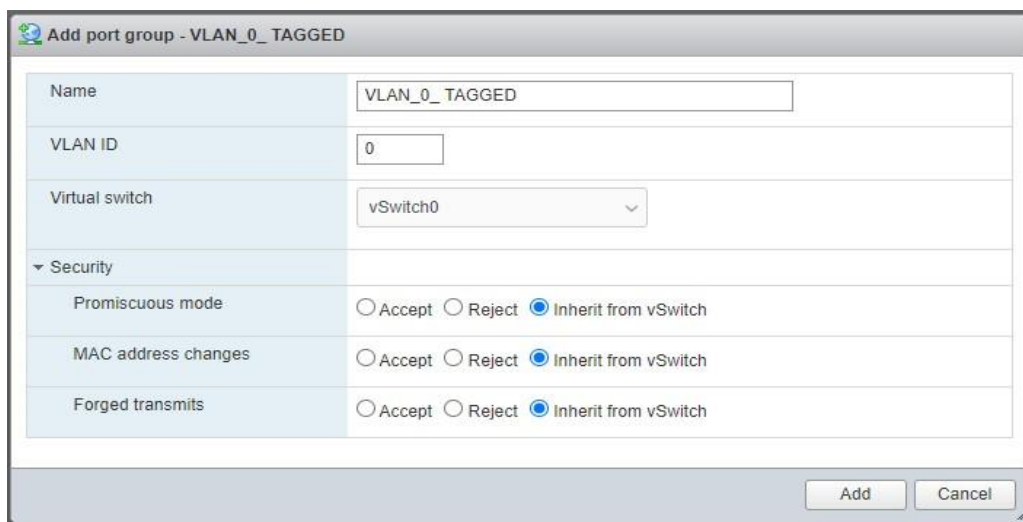
Программное обеспечение (далее – ПО) Системы защиты от спама и фишинга KAIROS v2 (далее – Система) состоит из программных модулей, описанных в таблице 3.

Таблица 3. Описание модулей ПО

№	Описание модуля	Описание	Формат файлов
1.	Модуль управления	Управление комплексом	kairos.ova

### 3 Описание развертывания комплекса

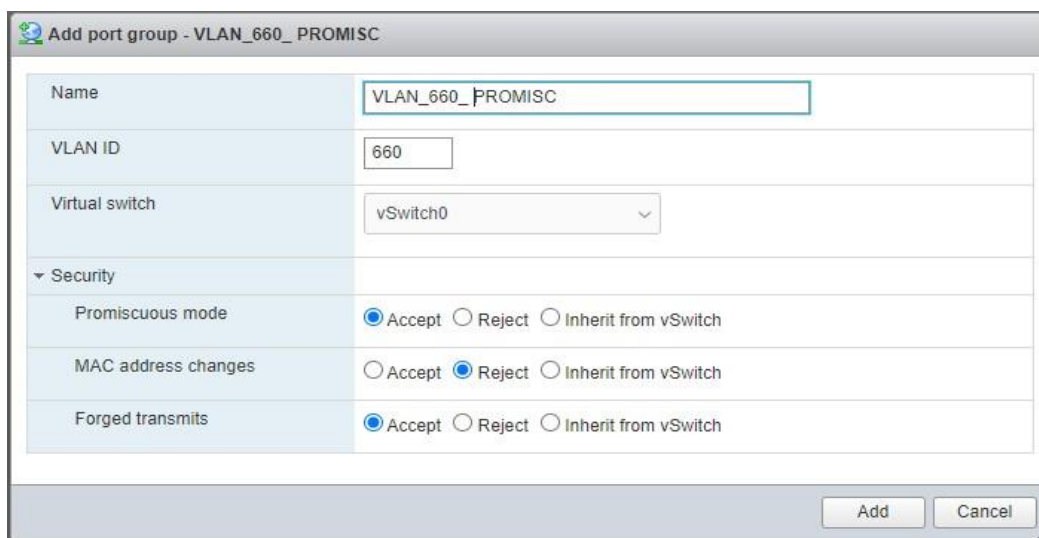
Для установки Системы в среде виртуализации ESXi, необходимо выделить сетевой интерфейс со свободным ID (выбранный ID необходимо будет вписать в настройки разворачиваемой виртуальной машины Системы). Для этого в интерфейсе ESXi в разделе «Networking > Port groups» необходимо создать VLAN\_(выбранный ID)\_TAGGED, «Add port group», со следующими настройками безопасности, как показано на рисунке 1. По завершении ввода данных необходимо нажать «Add».



Add port group - VLAN_0_TAGGED	
Name	VLAN_0_TAGGED
VLAN ID	0
Virtual switch	vSwitch0
▼ Security	
Promiscuous mode	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch
MAC address changes	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch
Forged transmits	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch
Add Cancel	

Рисунок 1. Настройка сетевого интерфейса модуля управления

В данном VLAN будет располагаться модуль управления Системой. Вторую Port Group по аналогии нужно сделать так, как показано на рисунке 2

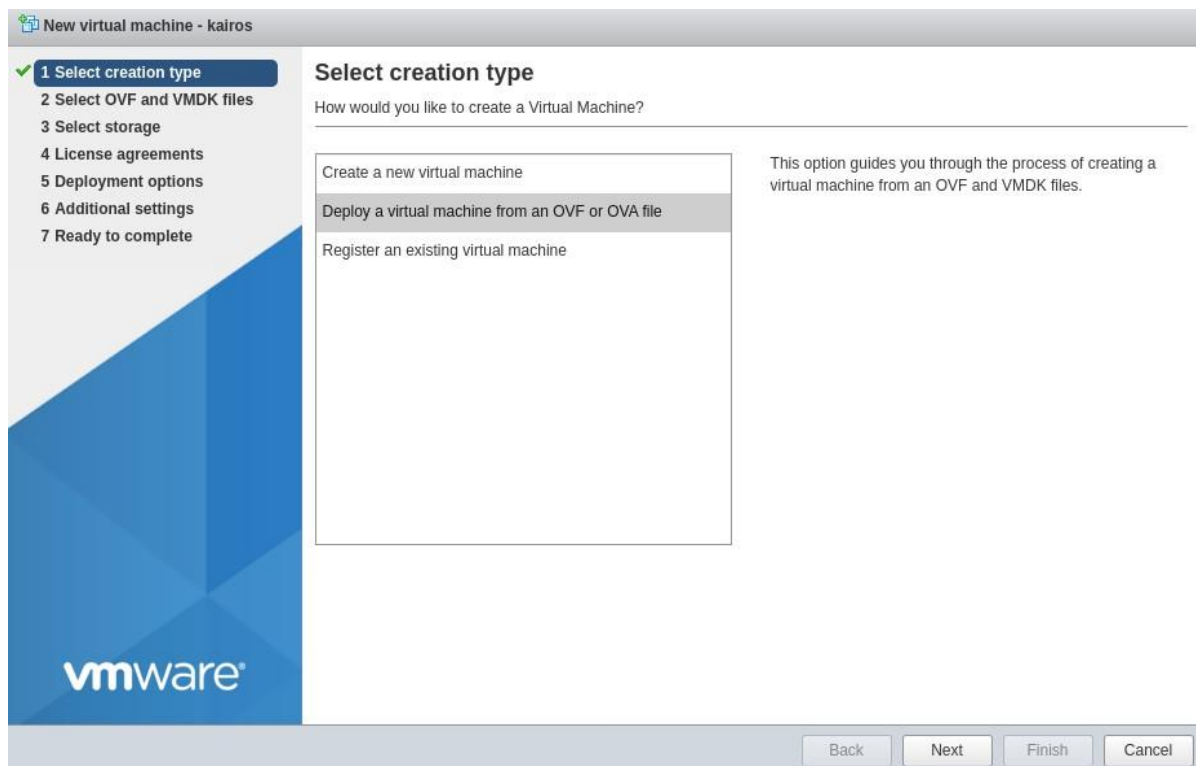


Add port group - VLAN_660_PROMISC	
Name	VLAN_660_PROMISC
VLAN ID	660
Virtual switch	vSwitch0
▼ Security	
Promiscuous mode	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch
MAC address changes	<input type="radio"/> Accept <input checked="" type="radio"/> Reject <input type="radio"/> Inherit from vSwitch
Forged transmits	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch
Add Cancel	

Рисунок 2. Настройка сетевого интерфейса

Далее необходимо создать ещё одну выделенную PortGroup «VLAN\_(выбранный ID) \_PROMISC» чтобы было как минимум две PortGroup: например, «VLAN\_660\_PROMISC» и «VLAN\_661\_PROMISC».

Далее необходимо создать виртуальную машину для развертывания образа дистрибутива сервиса менеджмента Системы. Для этого нужно перейти в раздел «Virtual Machines», нажать «Create / Register VM», в пункте 1 «Select creation type» выбрать «Deploy a virtual machine from an OVF or OVA file». Далее нажать кнопку «Next» (Рисунок 3).



**Рисунок 3. Выбор типа файла для развертывания**

Далее необходимо в пункте 2 «Select OVF and VMDK files» присвоить имя виртуальной машине и выбрать файл для загрузки (Рисунок 4).



**Рисунок 4. Импорт файла в виртуальную машину**

Далее в пункте 3 «Select storage» необходимо выбрать хранилище, в котором будет размещен образ и нажать кнопку «Next» (Рисунок 5).

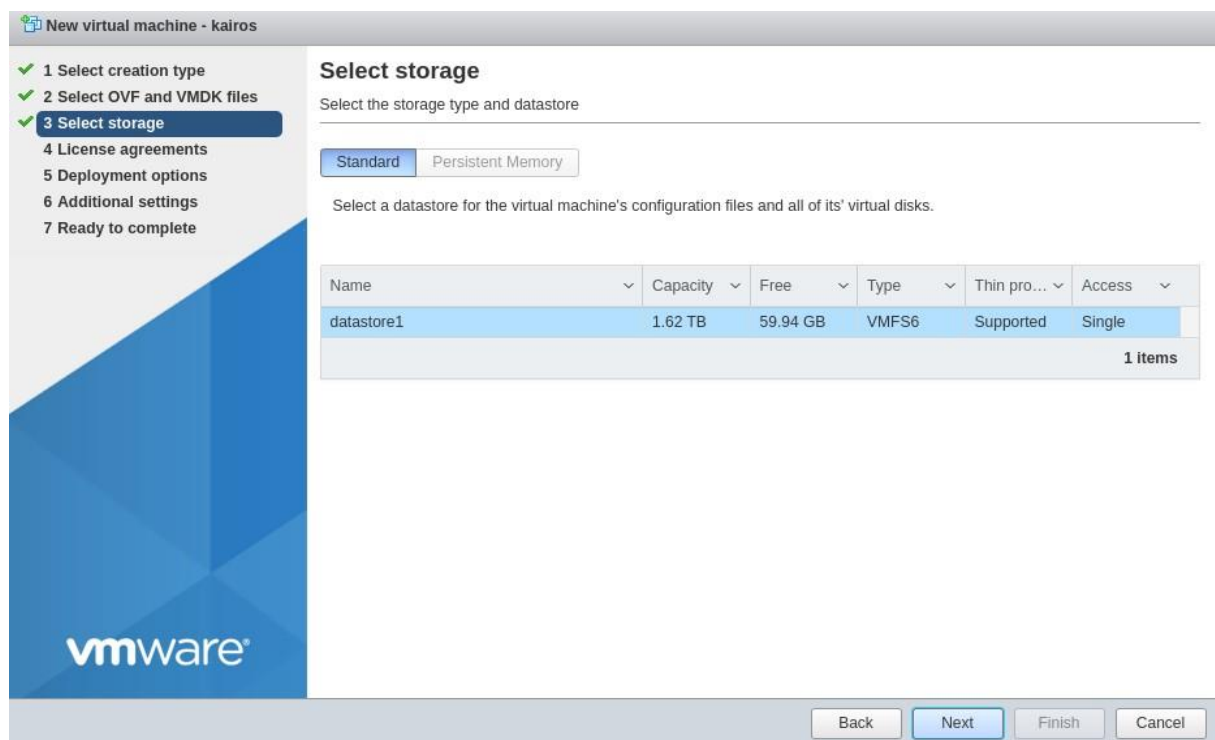


Рисунок 5. Выбор хранилища для размещения образа

Далее в пункте 4 «Deployment options» необходимо выбрать VLAN, способ размещения на диске (по умолчанию рекомендуется «тонкий», в случае необходимости — перезагрузите страницу) и автоматический способ запуска. Нажать кнопку «Next» (Рисунок 6).

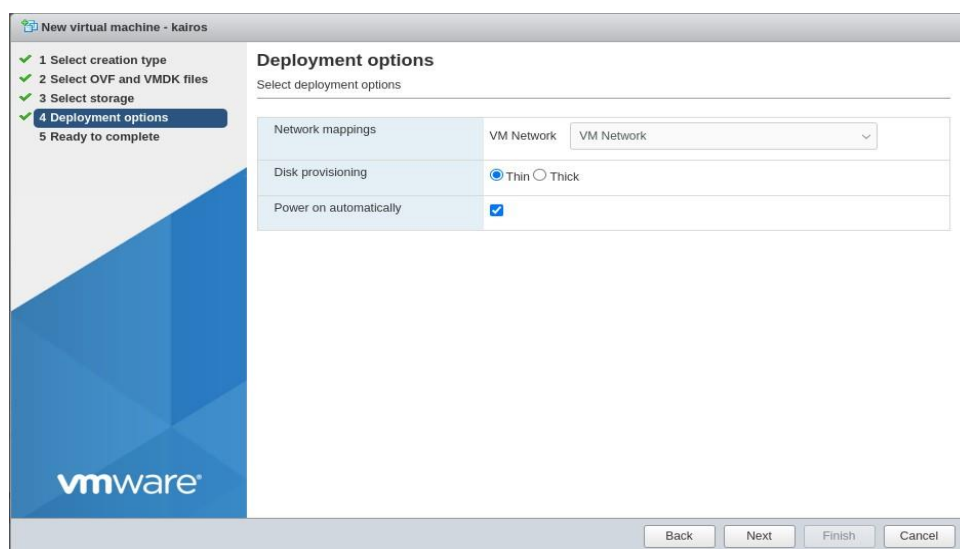
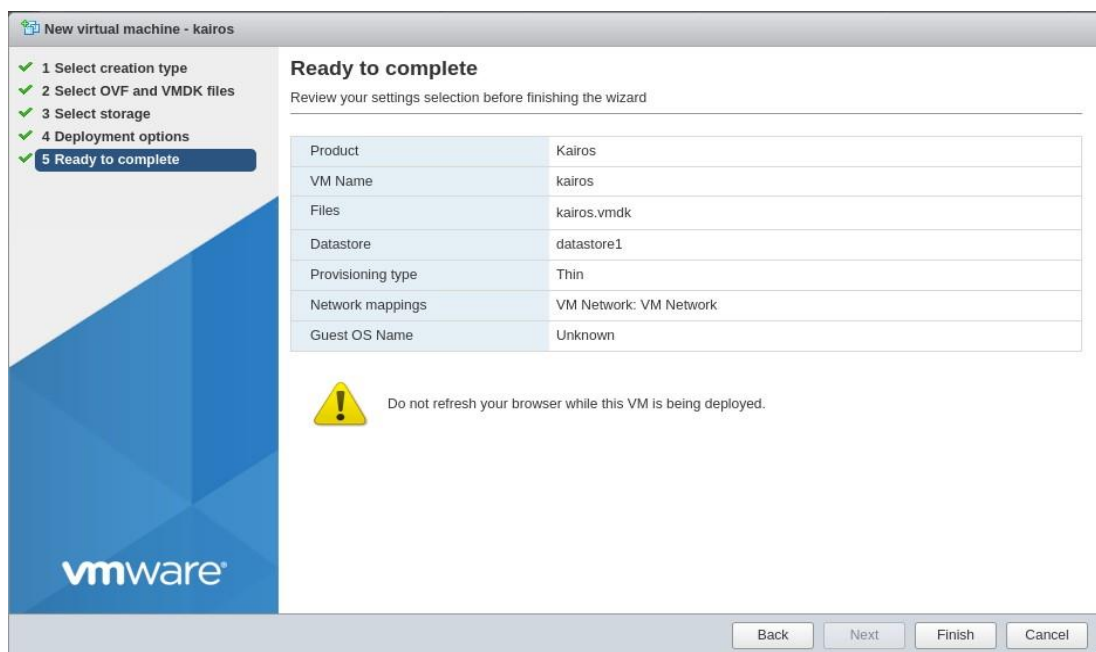


Рисунок 6. Выбор настроек установки

Далее в пункте 5 «Ready to complete» необходимо выполнить перепроверку настроек импорта и развертывания. Если все корректно, то нажать кнопку «Finish» (Рисунок 7).



**Рисунок 7. Перепроверка настроек установки и ее запуск**

После завершения импорта в таблице заданий «Recent tasks» в столбце «Result» статус следующих заданий должен быть «Completed successfully»:

- Upload disk (Загрузка диска)
- Create VM (Создание виртуальной машины)
- Import VApp (Импорт образов)
- Power On VM (Запуск на виртуальной машине)



## 4 Настройка сервиса менеджмента

После успешного импортирования необходимо осуществить настройку сервера. Для этого необходимо перейти в консоль терминала (Рисунок 8):

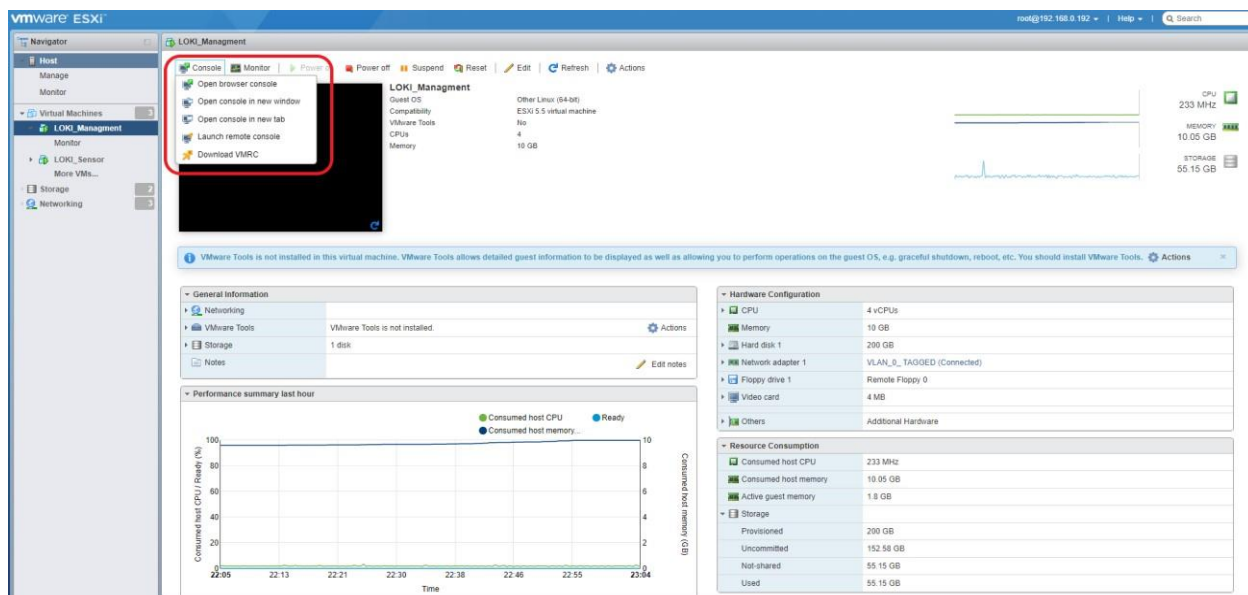


Рисунок 8. Переход в консоль терминала для настройки сервиса менеджмента

Далее необходимо авторизоваться под пользователем `avsoft_shell`, пароль от которого будет выдан вендором, чтобы попасть в консоль управления.

Для просмотра доступных сетевых интерфейсов нужно воспользоваться следующей командой:

```
interface info
```

Далее необходимо настроить сетевые интерфейсы. В случае, если в сети имеется DHCP-сервер, следует ввести команду:

```
interface edit INTERFACE dynamic
```

INTERFACE — имя настраиваемого интерфейса

В ином случае интерфейсы нужно настроить вручную, воспользовавшись следующей командой:

```
interface edit INTERFACE static --ip IP_ADDR --nm NETMASK --gw GATEWAY
```

INTERFACE — имя настраиваемого интерфейса;

NETMASK — маска подсети;

GATEWAY — шлюз (необязательный параметр).

Для проверки настроек сетевого интерфейса можно использовать команду:

```
interface info INTERFACE
```

INTERFACE — имя интерфейса

Сервису менеджмента также необходимо задать управляющий интерфейс. Сделать это можно следующей командой:

```
interface primary INTERFACE
```

INTERFACE — имя интерфейса

## 5 Настройки в веб-интерфейсе

Далее необходимо перейти в веб-интерфейс и выполнить авторизацию в нем (логин и пароль выдается вендором) (Рисунок 9).

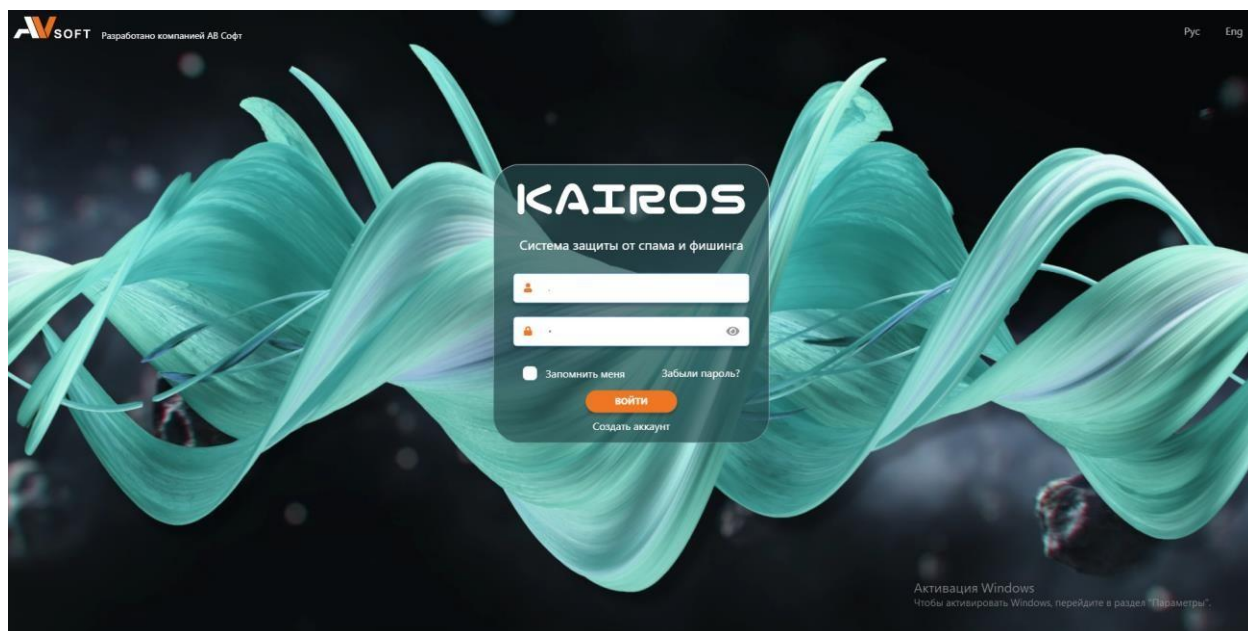


Рисунок 9. Авторизация в веб-интерфейс