

OOO «СОЛАР СЕКЬЮРИТИ»   
Компания группы ПАО «Ростелеком»   
Никитский пер.7, cтр.1, г. Москва, Россия,   
125009

T +7 (499) 755-07-70  
E info@rt-solar.ru  
W [rt-solar.ru](http://rt-solar.ru)

Solar Lighthouse.

Руководство пользователя.

Москва, 2024

Оглавление

[1. Обозначения и сокращения 4](#_Toc182830911)

[2. Термины и определения 6](#_Toc182830912)

[3. Введение 8](#_Toc182830913)

[4. Общие сведения 9](#_Toc182830914)

[4.1 Наименование программы 9](#_Toc182830915)

[4.2 Назначение и область применения программы 9](#_Toc182830916)

[4.3 Основные функции программы 9](#_Toc182830917)

[4.3.1 Настройка модулей и их конфигурации 9](#_Toc182830918)

[4.3.2 Агрегация информации об активах из различных источников 10](#_Toc182830919)

[4.3.3 Поиск активов путем активного сканирования 10](#_Toc182830920)

[5. Условия выполнения программы 10](#_Toc182830921)

[5.1 Требования к составу и параметрам технических средств 10](#_Toc182830922)

[5.1.1 Аппаратное обеспечение для установки (развертывания ПО) 10](#_Toc182830923)

[5.1.2 Аппаратное обеспечение для пользователей 12](#_Toc182830924)

[5.2 Требования к установленному общесистемному и прикладному программному обеспечению 12](#_Toc182830925)

[5.2.1 Программное обеспечение для среды функционирования 12](#_Toc182830926)

[5.2.2 ПО для работы пользователей 12](#_Toc182830927)

[6. Роли пользователей 13](#_Toc182830928)

[7. Выполнение программы 14](#_Toc182830929)

[7.1 Вход в программу 14](#_Toc182830930)

[7.1.1 Вход в программу при помощи логина и пароля 14](#_Toc182830931)

[7.2 Описание основных элементов интерфейса 15](#_Toc182830932)

[7.3 Ассеты 16](#_Toc182830933)

[7.4 Модули 17](#_Toc182830934)

[7.4.1 Добавление модуля 17](#_Toc182830935)

[7.4.2 Удаление модуля 19](#_Toc182830936)

[7.5 Конфигурации модулей 19](#_Toc182830937)

[7.5.1 Добавление конфигурации модулей 20](#_Toc182830938)

[7.5.2 Удаление конфигурации модулей 21](#_Toc182830939)

[7.6 Киперы 21](#_Toc182830940)

[7.6.1 Добавление кипера 22](#_Toc182830941)

[7.6.2 Удаление кипера 23](#_Toc182830942)

[7.7 Автоправила 23](#_Toc182830943)

[7.7.1 Добавление Автоправила 24](#_Toc182830944)

[7.7.2 Запуск Автоправила 25](#_Toc182830945)

[7.7.3 Удаление Автоправила 26](#_Toc182830946)

[9. Выход из программы, завершение работы 26](#_Toc182830947)

# 1. Обозначения и сокращения

|  |  |
| --- | --- |
| **Сокращение** | **Расшифровка** |
| АРМ | Автоматизированное рабочее место |
| БД | База данных |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| ПК | Персональный компьютер |
| CD | Continious delivery |
| CI | Continious integration |
| CLI | Command Line Interface |
| JSON | JavaScript Object Notation |
| RAM | Random Access Memory |
| SSD | Solid-State Drive |
| HDD | Hard Disk Drive |
| ОЗУ | Оперативное запоминающее устройство |
| YML | Это формат хранения данных, похожий на язык разметки |
| YAML | YAML Ain't Markup Language (alternative: Yet Another Markup Language) |

# 2. Термины и определения

|  |  |
| --- | --- |
| Термин | Определение |
| Программное обеспечение | Совокупность компьютерных программ (программ для ЭВМ) и программных документов, необходимых для эксплуатации этих программ. |
| Секреты | Идентификационная и аутентификационная информация, которая используется системами и приложениями для аутентификации или в качестве входных данных для сервисов и алгоритмов. |
| Зона  (Zone) | Логически или физически выделенный сетевой сегмент |
| Кипер  (Keeper) | Оркестратор модулей, собирающих информацию в определённой Зоне |
| Модуль  (Module) | Контейнер, выполняющий определенную функциональность по идентификации или сбору активов. |
| Vault | Защищенное хранилище секретов |
| Тенант | Это логическая сущность, имеющая возможность использовать ресурсы и сервисы. |
| Vlan | Виртуальная локальная компьютерная сеть. |
| Хосты | Любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. В более широком смысле под хостом могут понимать любой компьютер, подключённый к локальной или глобальной сети. |

# 3. Введение

Руководство пользователя содержит информацию об использовании программного обеспечения Solar Lighthouse (далее в тексте также могут быть использованы термины и сокращения: ПО, программа, программное обеспечение, ПО Solar Lighthouse). В руководстве описаны основные функции Solar Lighthouse, основные разделы графического интерфейса и приведены примеры действий пользователя при выполнении конкретных задач. Описание действий по установке (развертыванию), настройке ПО, а также других действий, доступных пользователю с административными правами, не рассматриваются в настоящем документе. Описание действий, доступных для администратора, приведено в документе "Руководство администратора".

# 4. Общие сведения

## 4.1 Наименование программы

Наименование ПО – Solar Lighthouse

## 4.2 Назначение и область применения программы

Solar Lighthouse это продукт для управления информационной безопасностью, основная задача которого — помочь пользователям привести свои активы в безопасное состояние, лучше понимать их и выстраивать эффективные процессы для их защиты.

Solar Lighthouse позволит пользователям эффективно интегрироваться с различными источниками информации, проводить активные сканирования инфраструктуры, реализовывать аудит соответствия требованиям и строить процессы по обеспечению безопасности инфраструктуры.

## 4.3 Основные функции программы

### 4.3.1 Настройка модулей и их конфигурации

В интерфейсе реализованы экраны для возможности просмотра/добавления/управления запускаемыми модулями.

Для добавленных модулей есть возможность создать, редактировать и удалить конфигурацию модуля, которая является частным способом настройки модуля.

### 4.3.2 Агрегация информации об активах из различных источников

В продукте предоставлен механизм для запуска модулей, которые могут интегрироваться с различными источниками активов (например хосты) и сохранять их в БД продукта.

### 4.3.3 Поиск активов путем активного сканирования

В продукте предоставлен механизм для запуска модулей, которые могут проводить активное сканирование инфраструктуры и сохранять найденные активы в БД продукта.

В продукте из коробки доступен один модуль для сканирования с помощью nmap.

# 5. Условия выполнения программы

## 5.1 Требования к составу и параметрам технических средств

### 5.1.1 Аппаратное обеспечение для установки (развертывания ПО)

ПО Solar Lighthouse предназначено для функционирования на аппаратной платформе с архитектурой процессора x86 64-бит.

Требования к аппаратному обеспечению применительно к компонентам программы приведены в Таблице №1.

Таблица 1. Требования по компонентам

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Компонент** | **Количество** | **Требования** | **Процессор** | **ОЗУ** | **Диск** |
| Core Service | 1 на инфраструктуру | Желательные | 2 ядра | 4Gb | 100Gb |
| Минимальные | 2 ядра | 4Gb | 100Gb |
| База данных Core Service | 1 на инфраструктуру | Желательные | 2 ядра | 4Gb | 100Gb |
| Минимальные | 2 ядра | 4Gb | 100Gb |
| Asset Manager | 1 на инфраструктуру | Желательные | 4 ядра | 8Gb | 100Gb |
| Минимальные | 2 ядра | 4Gb | 50Gb |
| База данных Asset manager | 1 на инфраструктуру | Желательные | 8 ядра | 16Gb | 100Gb |
| Минимальные | 4 ядра | 8Gb | 50Gb |
| Reflector | 1 на инфраструктуру | Желательные | 2 ядра | 2Gb | 5Gb |
| Минимальные | 2 ядра | 2Gb | 5Gb |
| Keeper  Module  База данных Keeper  Vault | По 1 на инфраструктуру | Желательные | 4 ядра | 8Gb | 150Gb |
| Минимальные | 2 ядра | 4Gb | 75Gb |

### 5.1.2 Аппаратное обеспечение для пользователей

Персональный компьютер (или ноутбук) с параметрами не хуже: центральный процессор (CPU) 1,5 ГГц, оперативная память 4 ГБ (RAM), дисковая подсистема 20 ГБ (HDD или SSD), разрешение монитора 1920х1080px, сетевой адаптер 100 Мбит/с (Network).

## 5.2 Требования к установленному общесистемному и прикладному программному обеспечению

### 5.2.1 Программное обеспечение для среды функционирования

* ПО предназначено для работы в среде (в том числе, обеспечивает безопасность среды) со следующими характеристиками и параметрами: операционная система: ОС на базе Linux, такая как: Ubuntu версии 24.04, версия ядра Linux должна быть не ниже версии 4.18 и не выше версии 6.8.

### 5.2.2 ПО для работы пользователей

Для ПК (или ноутбука) пользователя:

* браузер: Google Chrome версии 130 и выше, Firefox версии 131 и выше.

# 6. Роли пользователей

Для работы в программе предусмотрено несколько типов ролей пользователей с предварительно настроенными правами доступа к функциональности. Перечень ролей и их описание приведены в Таблице №2. Некоторые роли имеют технический характер, созданы для работы системы и не предназначены для работы пользователя в графическом интерфейсе. Информация о системных ролях приведена для справочных целей.

Пользователем с административными правами могут быть созданы дополнительные роли пользователей или изменены права доступа для имеющихся ролей. Порядок действий для создания ролей или изменения прав доступа приведены в документе "Руководство администратора".

Таблица 2. Роли пользователей ПО Solar Lighthouse

|  |  |
| --- | --- |
| **Роль в программе** | **Описание роли** |
| Администратор | Эта роль предназначена для администраторов. Данная роль применяется для того, чтобы предоставить пользователю доступ на чтение и запись ко всем ресурсам. |

# 7. Выполнение программы

## 7.1 Вход в программу

Для запуска и выполнения программы от пользователя не требуется специальных действий т.к. ПО Solar Lighthouse является веб-приложением, которое не требует от пользователя действий по запуску или остановке выполнения, и для работы в нем пользователю достаточно произвести аутентификацию – осуществив вход в программу.

На данный момент, возможность входа в программу одна: по логину и паролю.

### 7.1.1 Вход в программу при помощи логина и пароля

Для входа в программу необходимо открыть веб-браузер (поддерживаемые версии см. в п.5.2.2 и перейти по ссылке, которую задал администратор вашей организации. ссылка может отличаться от указанной в зависимости от конкретной реализации, развертывания в определенной инфраструктуре. Актуальные данные предоставляются администратором системы или представителями разработчика ПО.

Откроется окно (см. рисунок 1), где пользователю необходимо ввести данные для авторизации:

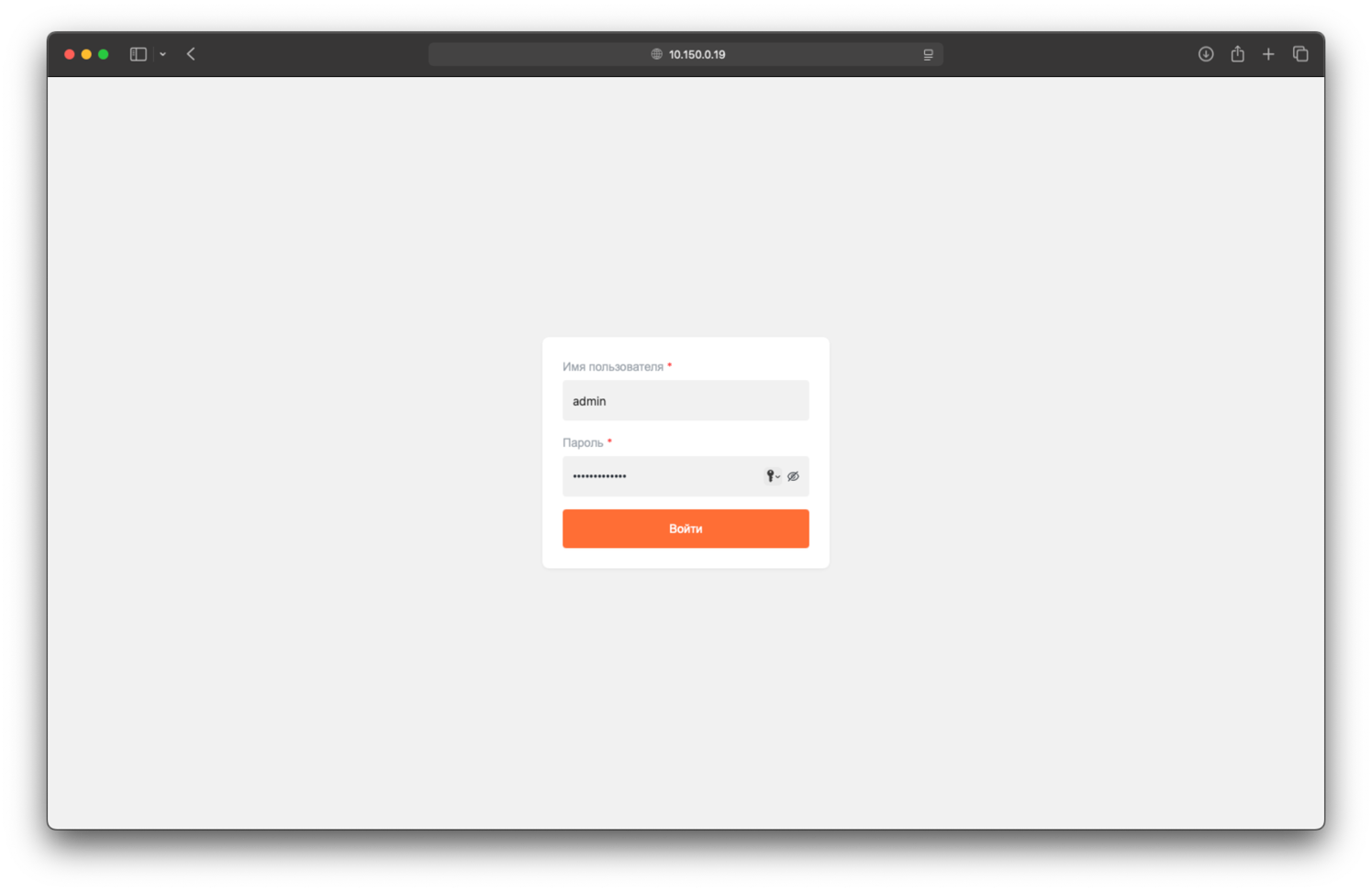
Примечание: логин и пароль для входа могут отличаться от указанных в документе. Актуальные данные предоставляются администратором системы или представителями разработчика ПО. 

Рисунок 1. Окно выхода в программу

При успешной авторизации откроется главная страница ПО Solar Lighthouse (по умолчанию в качестве главной страницы открывается страница "Главная страница"), см. рисунок 2. Если пользователь ввел некорректные данные (логин или пароль), появится сообщение "Пользователь не существует или введен не верный пароль".

## 7.2 Описание основных элементов интерфейса

Типовая страница ПО Solar Lighthouse (см. рисунок 2) содержит следующие элементы:

(1) Область навигации внутри раздела - содержит наименование раздела и также в зависимости от раздела может содержать основные количественные показатели, ссылки и др.

(2) Кнопка разлогина пользователя

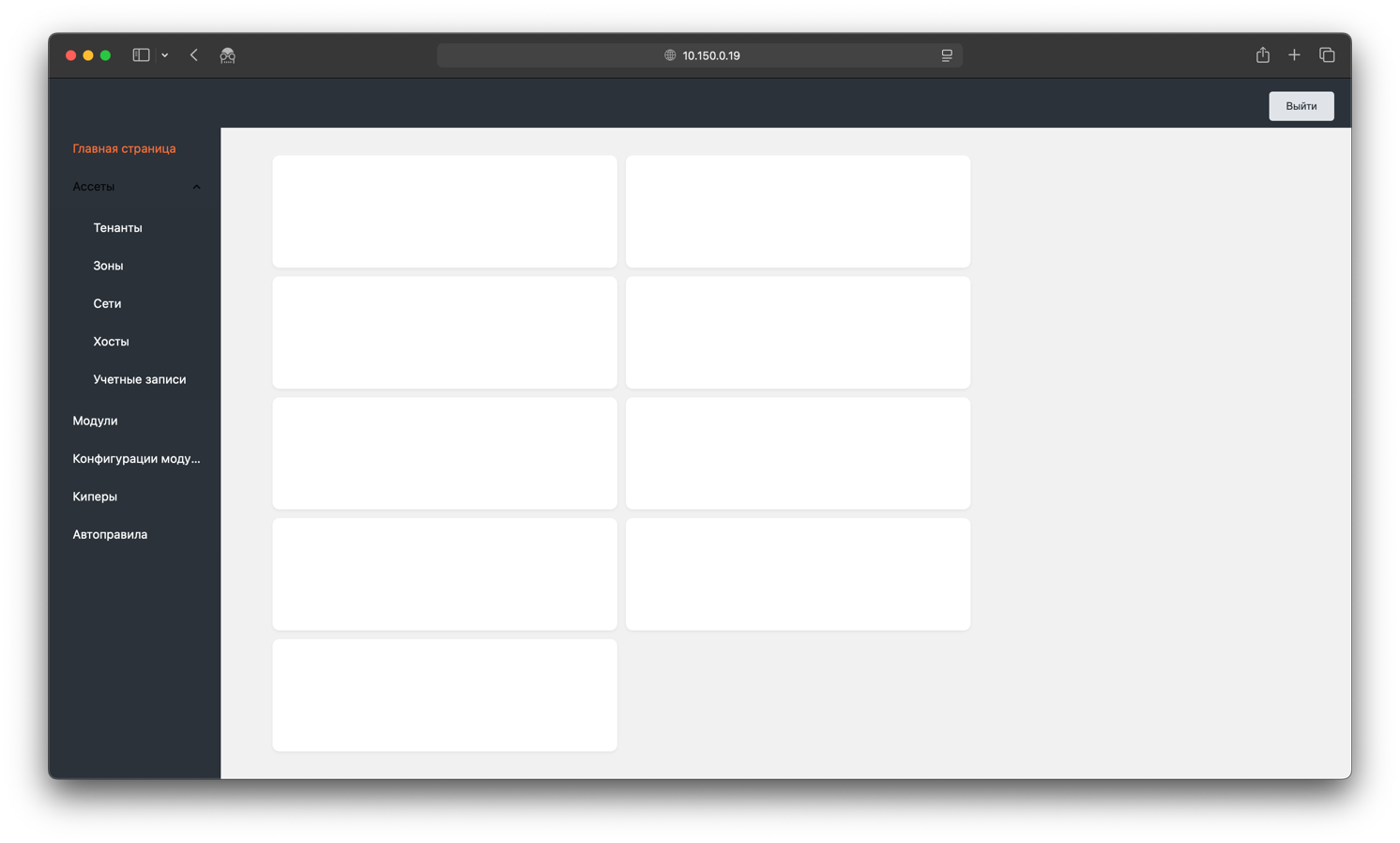


Рисунок 2. Основные элементы типовой страницы

## 7.3 Ассеты

В разделе «Ассеты» реализована возможность просмотра результатов сканирования модулей, таких как:

* Тенанты
* Зоны
* Сети
* Хосты
* Учетные записи

## 7.4 Модули

В разделе «Модули» реализована возможность добавления/удаления модулей. Модули это - контейнеры, выполняющий определенную функциональность по идентификации или сбору активов. Экран модулей представлен на рисунке №3.

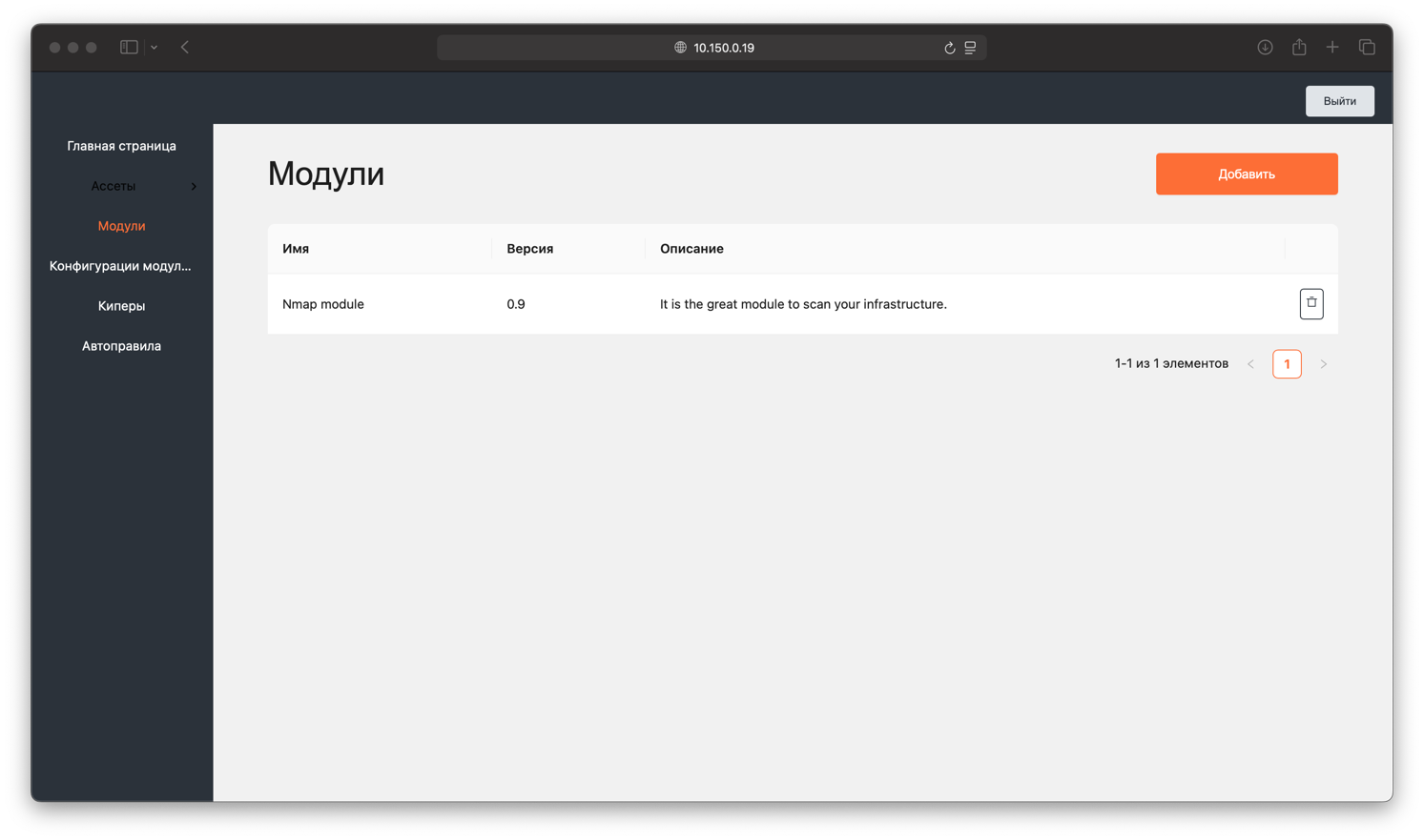


Рисунок 3. Экран "Модули"

### 7.4.1 Добавление модуля

При нажатии на кнопку «Добавить» пользователь перенаправляется на страницу «Добавить Модуль». Добавление модуля возможно загрузкой/перетаскиванием файла формата YML, YAML.

При правильно загруженном файле отобразится следующая информация (см. рисунок №4):

* Имя модуля
* URL – адрес по которому можно скачать модуль
* Описание
* Версия
* Версия модуль менеджера
* Шаблон конфигурации – описание того, с какими параметрами запускается модуль

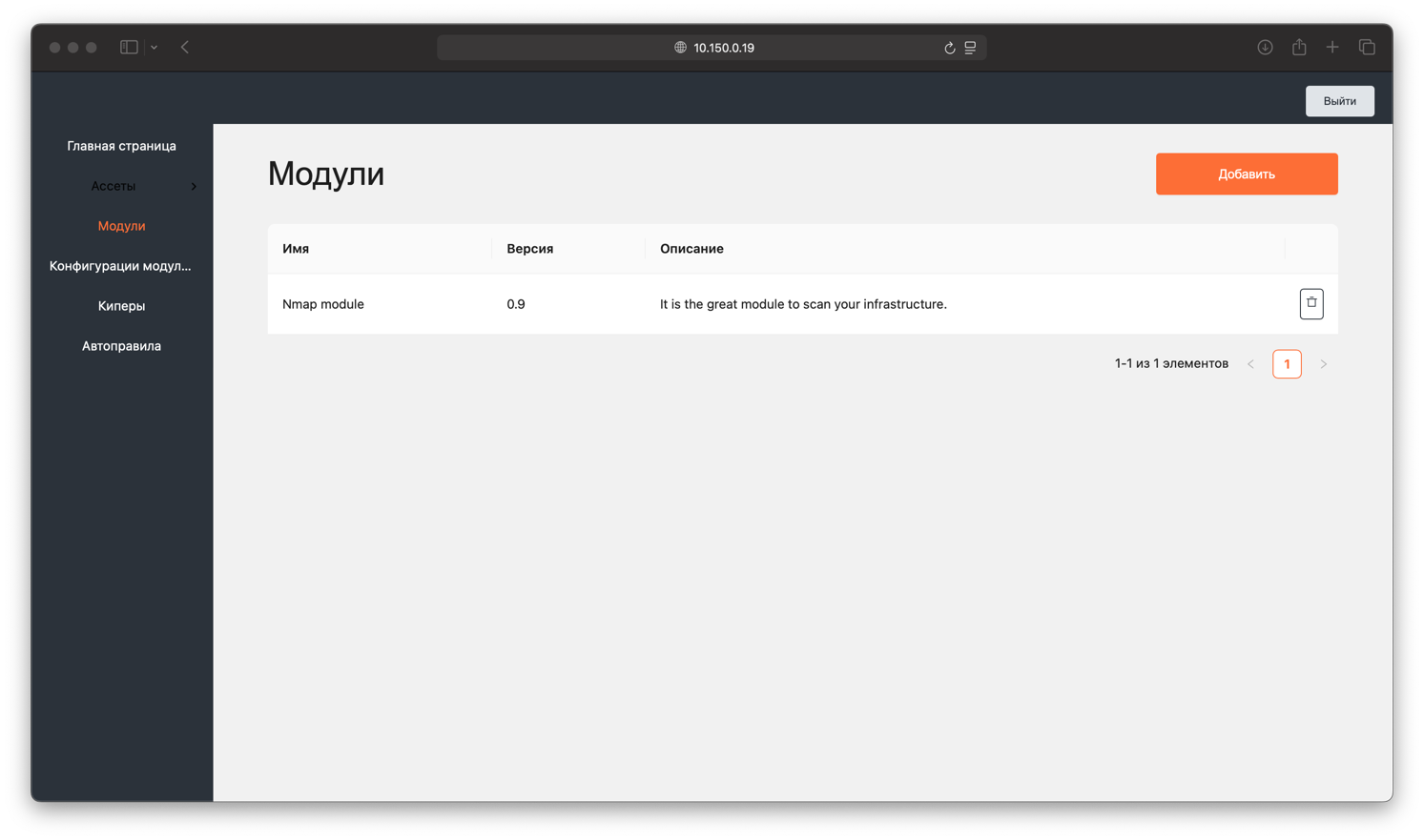


Рисунок 4. Успешный экран добавления модуля

При нажатии на кнопку «Сохранить» пользователя переведет на основной экран «Модули»

### 7.4.2 Удаление модуля

На основном экране «Модули» выберите интересующий Вас модуль. Откроется страница просмотра модуля, при нажатии на кнопку «Удалить» пользователя вернет на экран «Модули», соответствующий модуль удалится из системы.

## 7.5 Конфигурации модулей

На данной странице отображается список всех ранее созданных конфигурации модулей в табличном виде. Отображается название конфигурации, имя и версия модуля, для которого назначена конфигурация. Экран «Конфигурации модулей» представлен на рисунке №0.

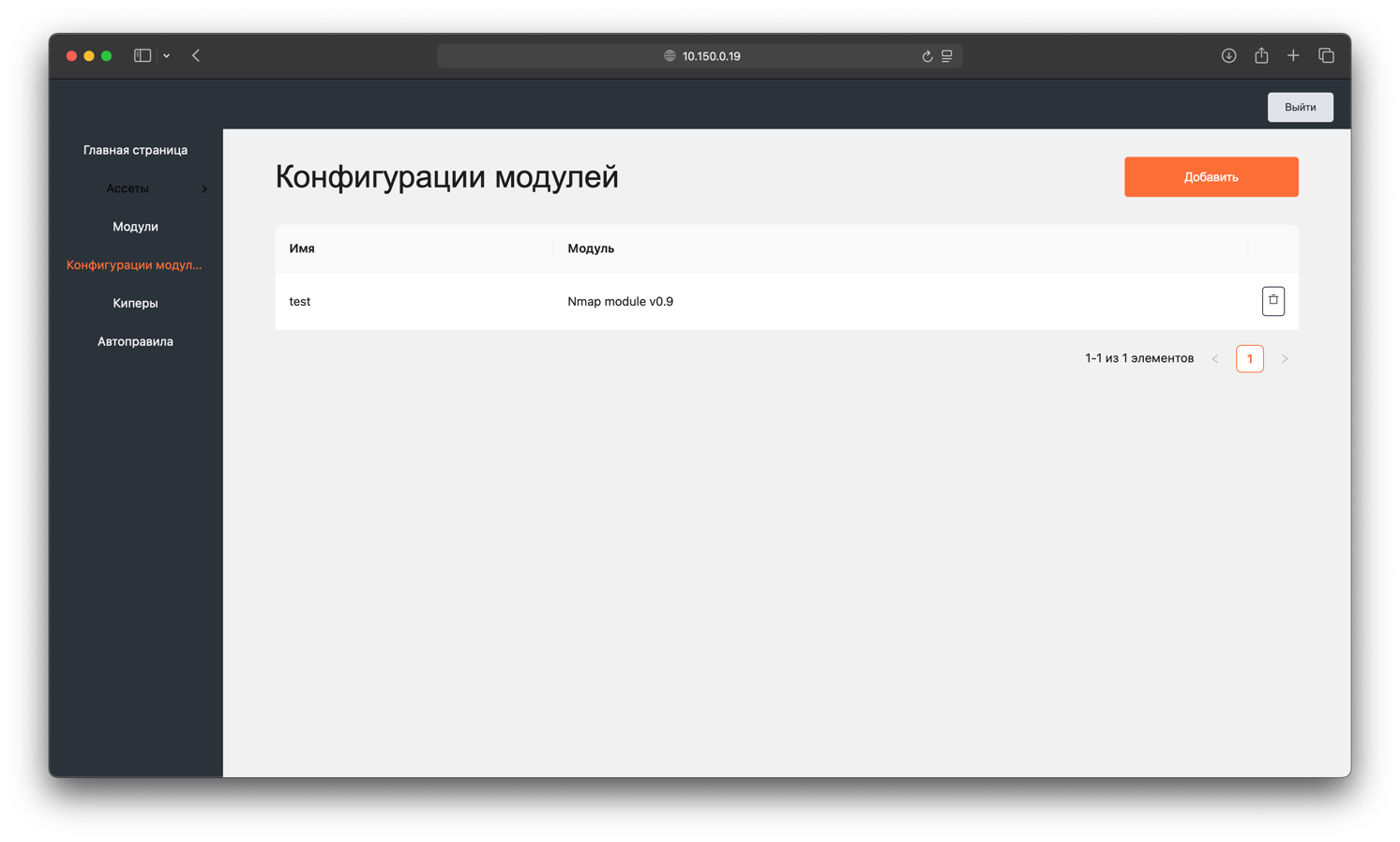


Рисунок 5. Экран "Конфигурации модулей"

### 7.5.1 Добавление конфигурации модулей

На основном экране «Конфигурации модулей» необходимо нажать на кнопку «Добавить», на первом шаге необходимо выбрать модуль, для которого создается конфигурация. На следующем шаге, необходимо заполнить требуемые параметры для настройки конфигурации модуля. Конкретные параметры определяются шаблоном конфигурации модуля (см. 7.4.1 Добавление модуля) и группируются в именованные блоки.

Например, для настройки конфигурации могут быть доступны следующие параметры:

* Main -
  + Host IP – (обязательное поле)
  + Flags – (необязательное поле)
* Additional –
  + Port – (обязательное поле)
  + Return error - (необязательное поле)

Где Main и Additional группы, а Host, Flags и т.д. – параметры конфигурации.

При завершении выбора параметров конфигурации необходимо нажать кнопку «Сохранить», после чего Вас вернет на основной экран «Конфигурации модулей», созданная конфигурация отобразится в общем списке.

### 7.5.2 Удаление конфигурации модулей

На основном экране «Конфигурации модулей» существует 2 варианта удаления конфигурации:

1. На основном экране «Конфигурации модулей» найти необходимую конфигурацию и нажать соответствующую иконку «Корзины» напротив конфигурации. Конфигурация удалится и Вас вернет на основной экран.
2. На основном экране «Конфигурации модулей», выбрать интересующую Вас конфигурацию, на открывшейся странице конфигурации нажать кнопку «Удалить». Конфигурация удалится и Вас вернет на основной экран.

## 7.6 Киперы

Кипер - оркестратор модулей, собирающих информацию в определённой Зоне. Экран «Киперы» представлен на рисунке №0, в табличной форме.

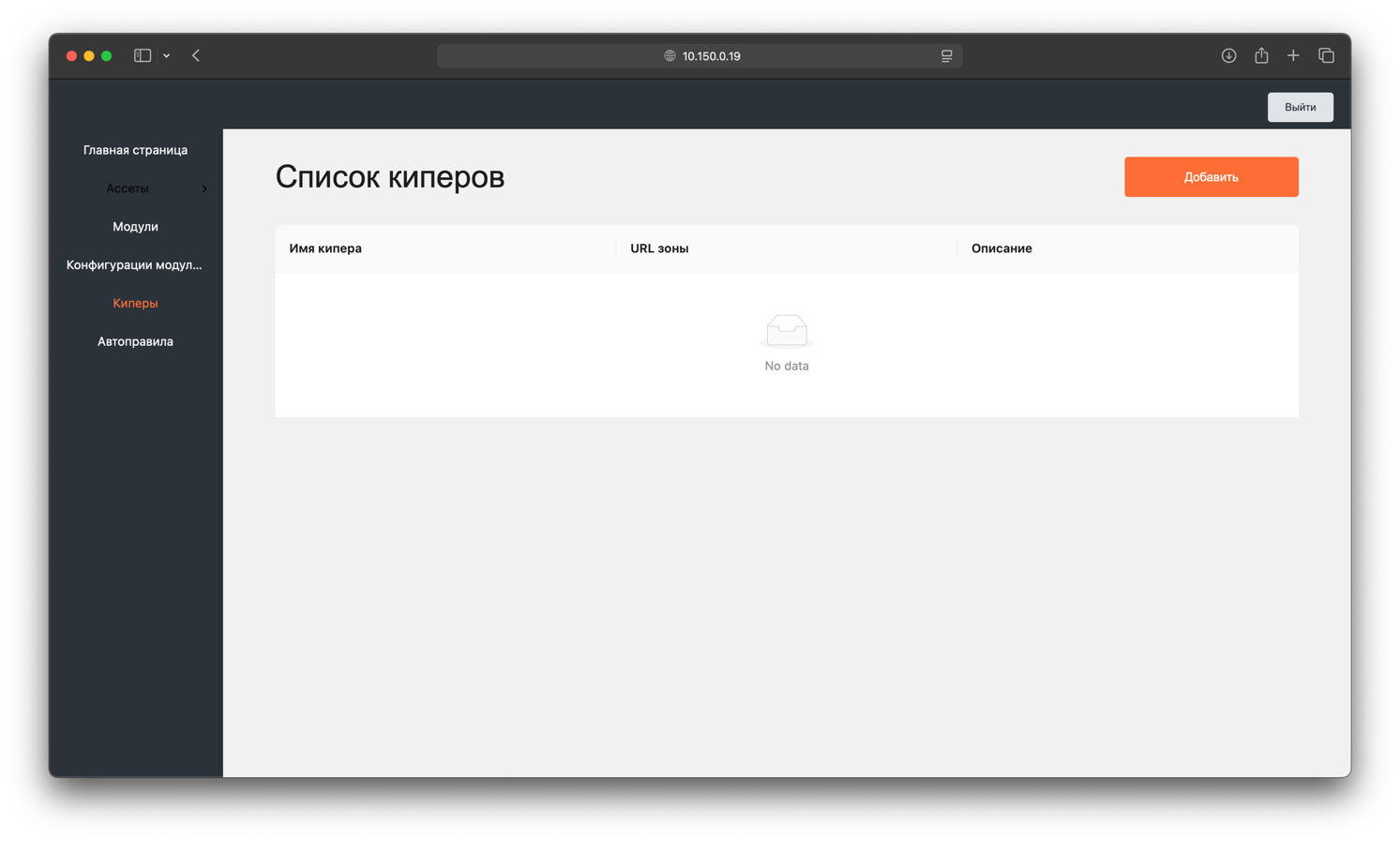


Рисунок 6. Экран "Киперы"

### 7.6.1 Добавление кипера

На основном экране «Список киперов» необходимо нажать на кнопку «Добавить», далее на первом шаге нужно выбрать зону, за которую отвечает кипер. На странице «Добавление кипера» необходимо прописать следующие параметры:

* Имя кипера (text)
* Адрес кипера (url) – ***на тестовом стенде адрес кипера 10.150.0.6:8080***
* Описание (text area)

После введения параметров необходимо нажать кнопку «Сохранить», после чего Вас вернет на основной экран «Список киперов», созданный кипер отобразится в общем списке.

***Примечание***: для каждой зоны может быть создан только один объект кипера. При попытке добавления кипера на уже «занятую» зону отобразится соответствующая ошибка.

### 7.6.2 Удаление кипера

На основном экране «Список киперов» выберите интересующий Вас кипер. Откроется страница просмотра кипера, при нажатии на кнопку «Удалить», Вас вернет на экран «Список киперов», соответствующий кипер удалится из системы.

## 7.7 Автоправила

Автоправила – триггер, по которому происходит запуск сканирования модулем. Экран «Автоправила» представлен на рисунке №7.

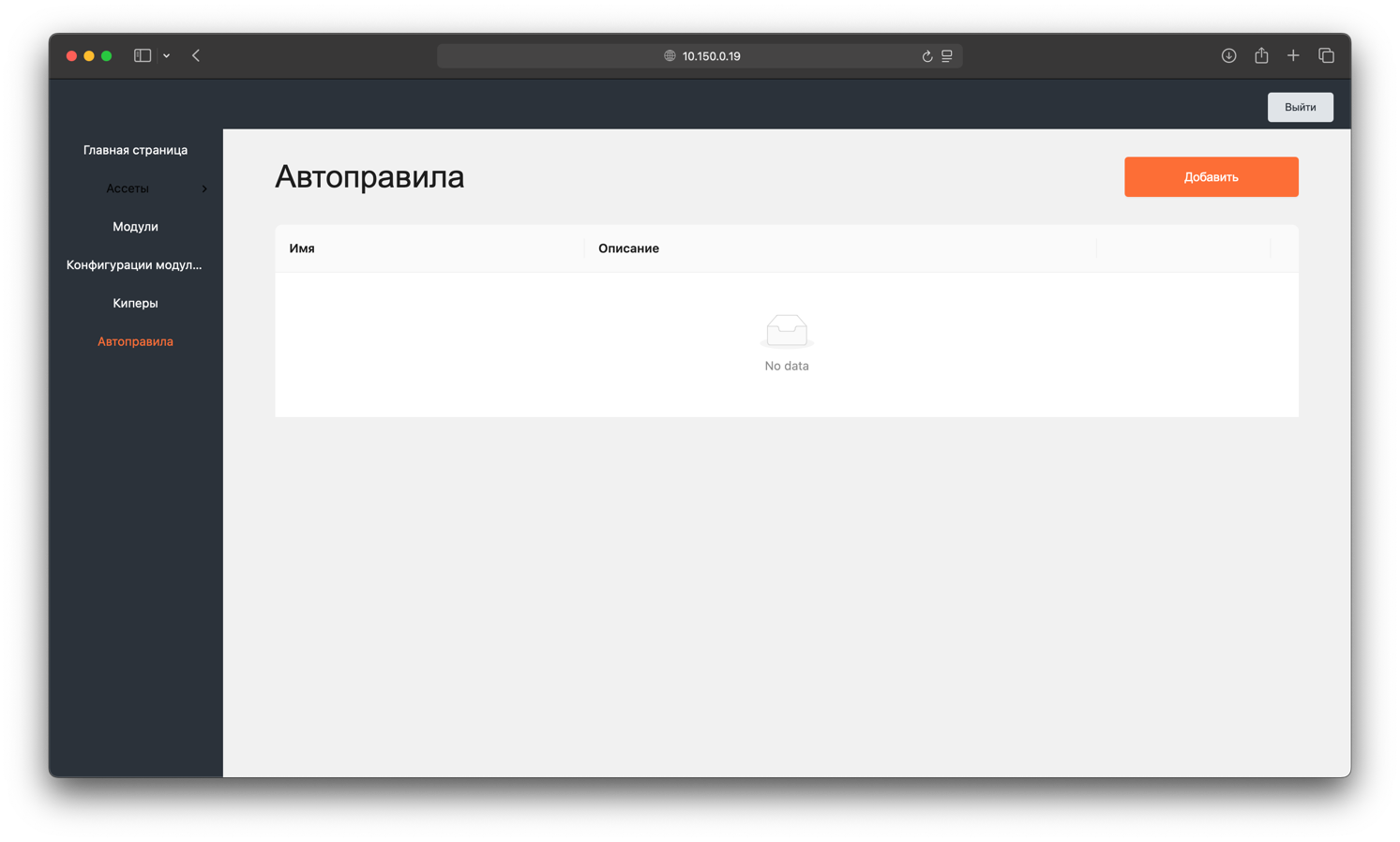


Рисунок 7. Экран "Автоправила"

### 7.7.1 Добавление Автоправила

На основном экране «Автоправила» необходимо нажать на кнопку «Добавить», далее на первом шаге нужно выбрать имя и краткое описание автоправила, а также условия, по которым оно запускается. На странице «Создание автоправила» необходимо прописать следующие параметры:

* Имя
* Описание
* Триггер

***Примечание***: в настоящий момент доступен один вид триггера – Расписание. Можно выбрать интервал, либо по дням.

После заполнения необходимых параметров, нужно выбрать тенант, на котором будет происходить сканирование. А также выбор соответствующего модуля.

Созданный модуль отразится на основной странице «Автоправила». Пример успешно созданного автоправила представлен на рисунке №8.

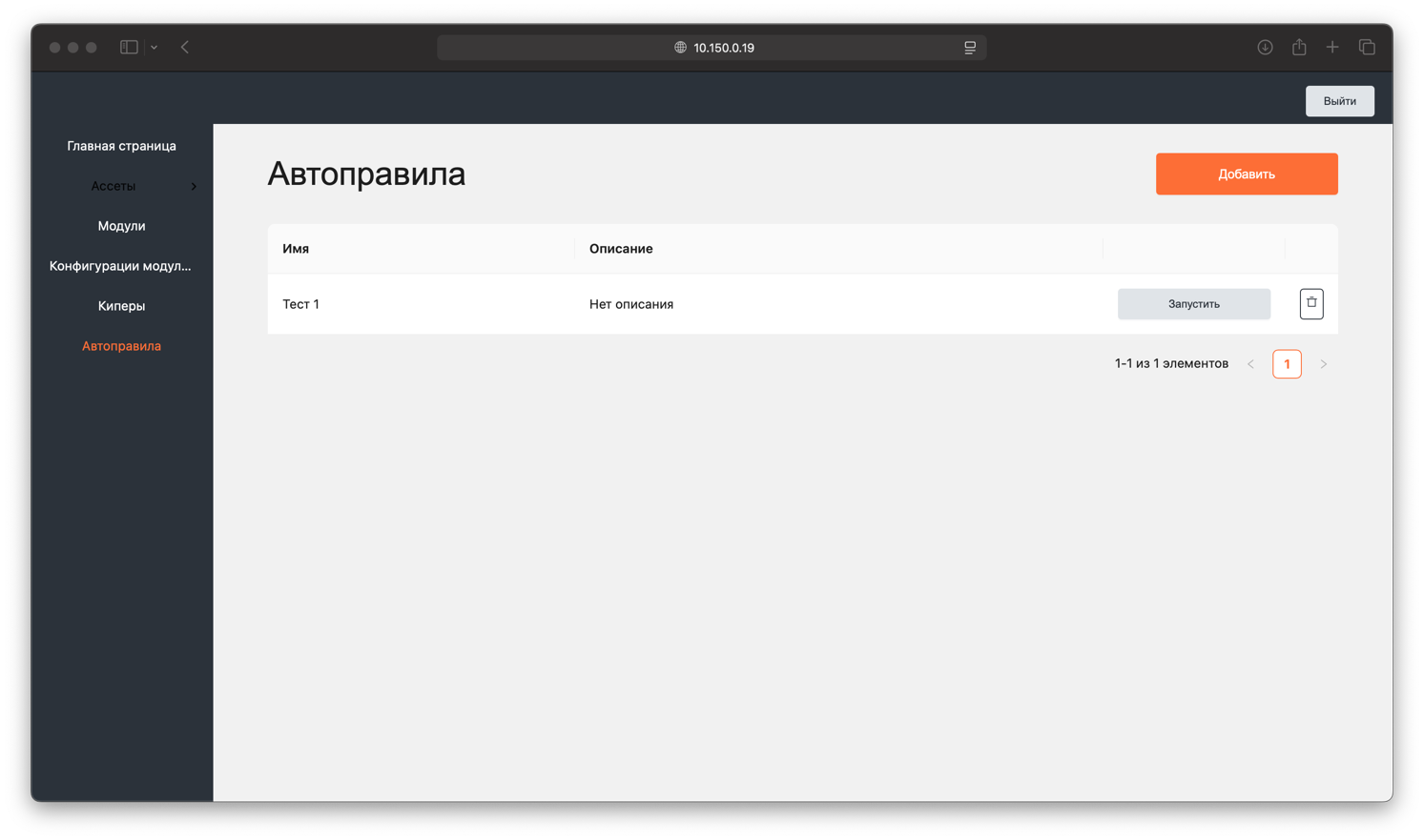


Рисунок 8. Экран успешно созданного автоправила

### 7.7.2 Запуск Автоправила

На основной странице «Автоправила», необходимо выбрать интересующее Вас автоправило, и нажать кнопку «Запустить». После чего происходит запуск сканирования, результаты сканирования можно просмотреть в разделах (на тестовом стенде запуск автоправила длится как правило от 1 до 3 минут):

* Ассеты
  + Сети
  + Хосты
  + Учетные записи

### 7.7.3 Удаление Автоправила

На основном экране «Автоправила» найти необходимое автоправило и нажать иконку «Корзины» напротив автоправила. Автоправило удалится и Вас вернет на основной экран «Автоправила».

# 9. Выход из программы, завершение работы

Для выхода из программы необходимо нажать на кнопку разлогина пользователя (См. 7.2 Описание основных элементов интерфейса).