**Функционал ПО «GAK-Box 2.0»**

1) Агент (ПО для ОС Windows)

1) Обнаружение уязвимостей ПО

2) Обнаружение не безопасных настроек ОС

3) Контроль параметров антивируса

2) Анализ безопасности локальных сетей

1) ARP-spoofing

2) Подмена шлюза

3) Уязвимости управляющих служб (DHCP, DNS)

4) Анализ настроек маршрутизатора

5) Контроль несанкционированного подключения к сети

3) Подбор паролей

1) Более чем по 40 протоколам

2) Ускорение за счёт использования радужных таблиц

3) Генерация уникальных таблиц под каждого сотрудника

4) Система управления/генерации словарей

4) Анализ безопасности WI-FI

1) Обнаружение атак

2) Тестирование на слабые пароли

3) Тестирование на несанкционированную смену алгоритма шифрования

4) Фишинг тестирование персонала  
 5) Анализ WPS

5) Анализ WEB-интерфейсов

1) Анализ контента компонентов браузера

2) Сканирование из-под авторизованного пользователя

3) Проверка уязвимостей во вложенных форматах, таких как JSON, XML, BASE64 и других

3) Анализ уязвимостей клиентских библиотек, таких как JQuery, Polymer, AngularJS и других

4) Анализ уязвимостей html5, таких как RTC, Web Sockets, CORS и других

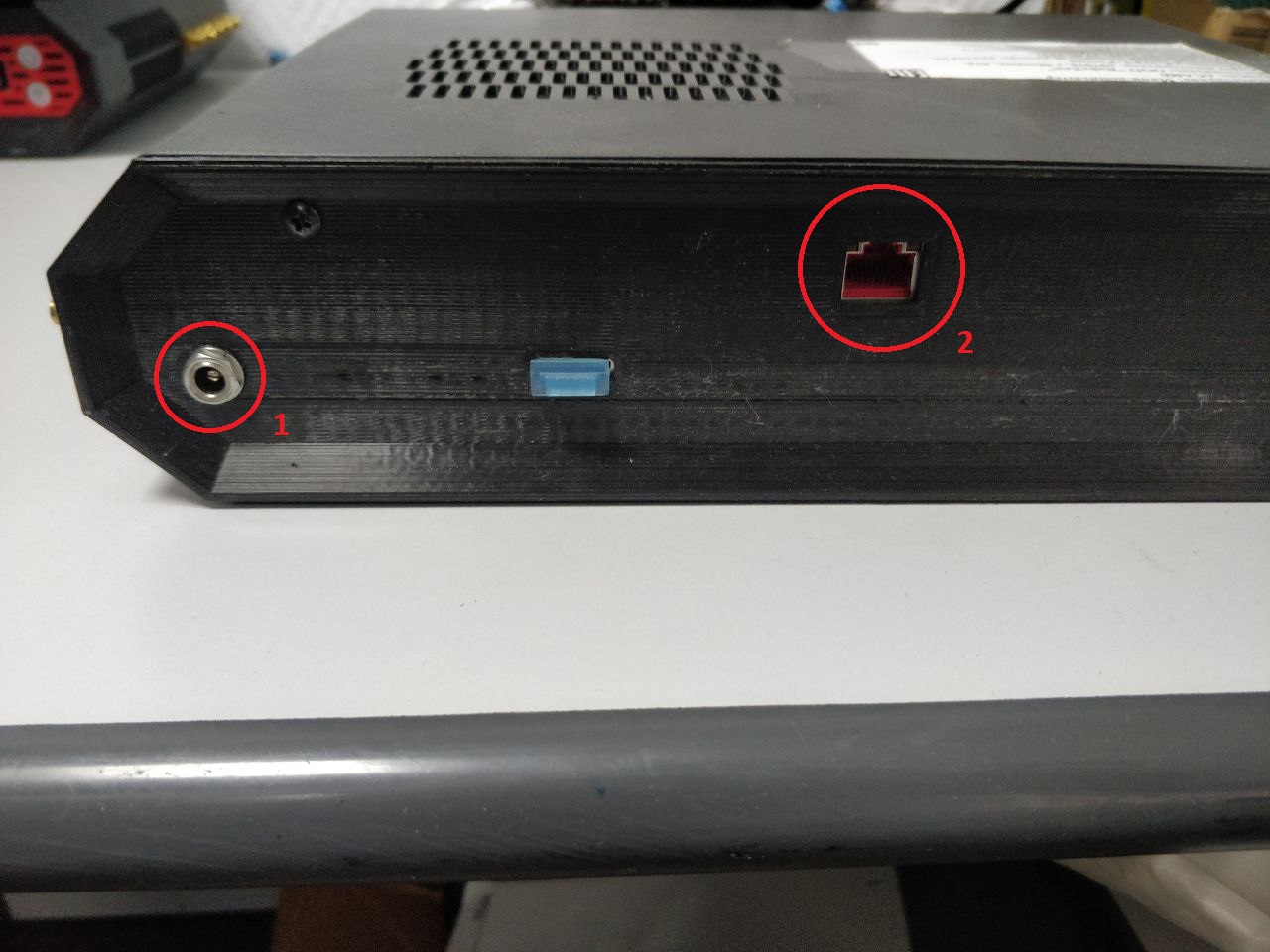
5) Уникальные проверки по типам данных, таких как URL, E-mail, телефоный номер и других

6) Система контроля уязвимостей

1) Генератор периодичных отчетов

2) Контроль качества и сроков исполнения задач по ИБ

**Руководство по использованию устройства GAK-Box**



Изображение задней части устройства

На изображении выше показаны элементы задней части устройства:

1. Разъем питания устройства
2. Разъем для подключения в локальную сеть



Изображение передней части устройства

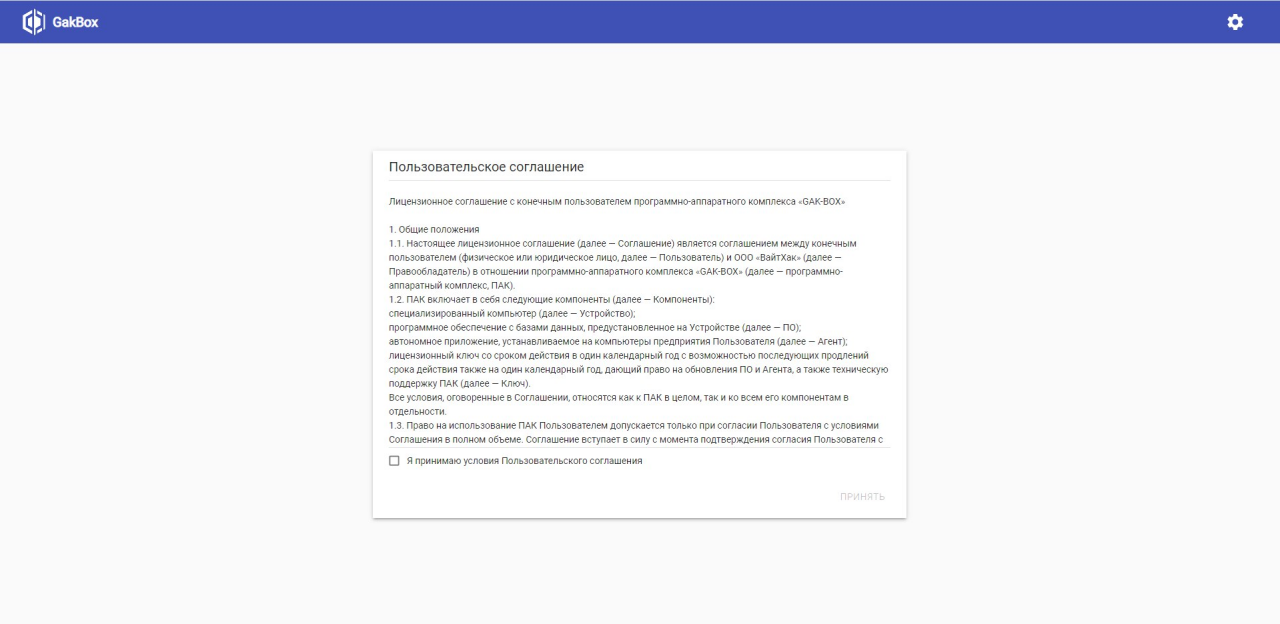
На изображении выше показаны элементы передней части устройства:

1. USB-порт
2. Кнопка включения устройства
3. Кнопка включения точки доступа WI-FI

Первоначально необходимо подключить устройство к питанию, проводом, идущим в комплекте, в разъем под номером (1), затем подключите интернет кабель в устройство, во вход под номером (2), после этого нужно включить устройство, нажав по кнопке под номером (4). Если будут сложности с определением адреса устройства, нажмите кнопку wi-fi доступа (5). Поднимется точка доступа, пароль от которой указан в лицензии. Нужно зайти и настроить соединение как требуется. Устройство готово к использованию.

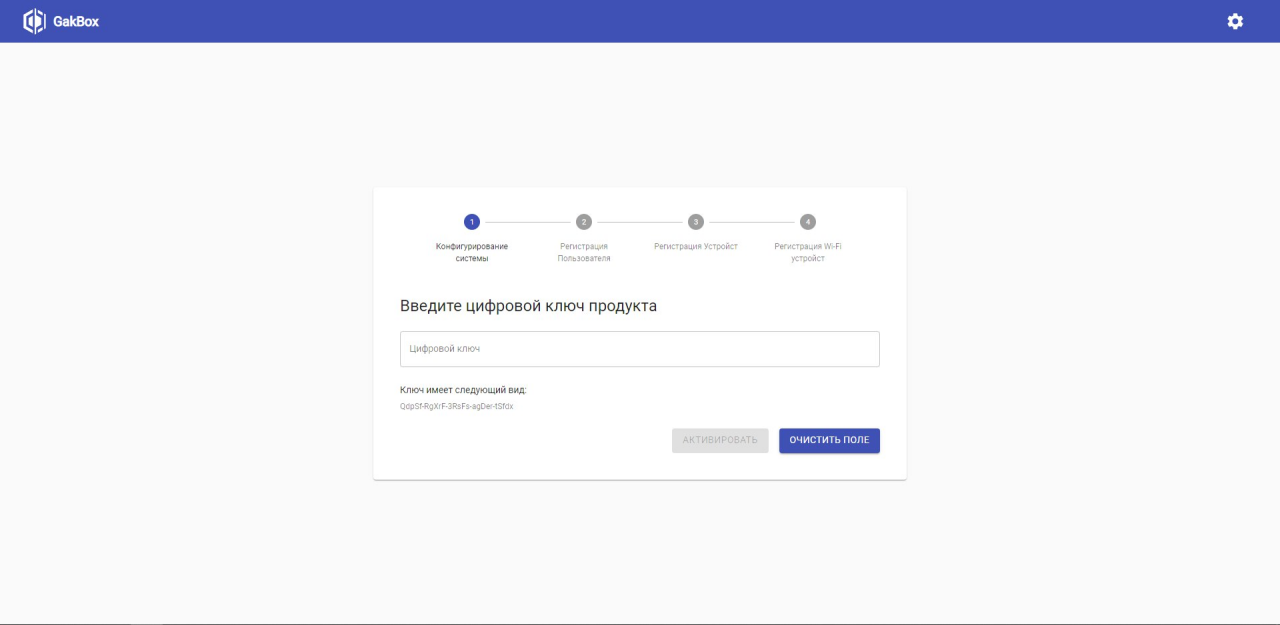
**Инструкция по эксплуатации ПО «GAK-Box 2.0»**

Прежде, чем перейти к использованию функциональных возможностей ПО «GAK-Box 2.0», необходимо определить, какой адрес в сети получило устройство.



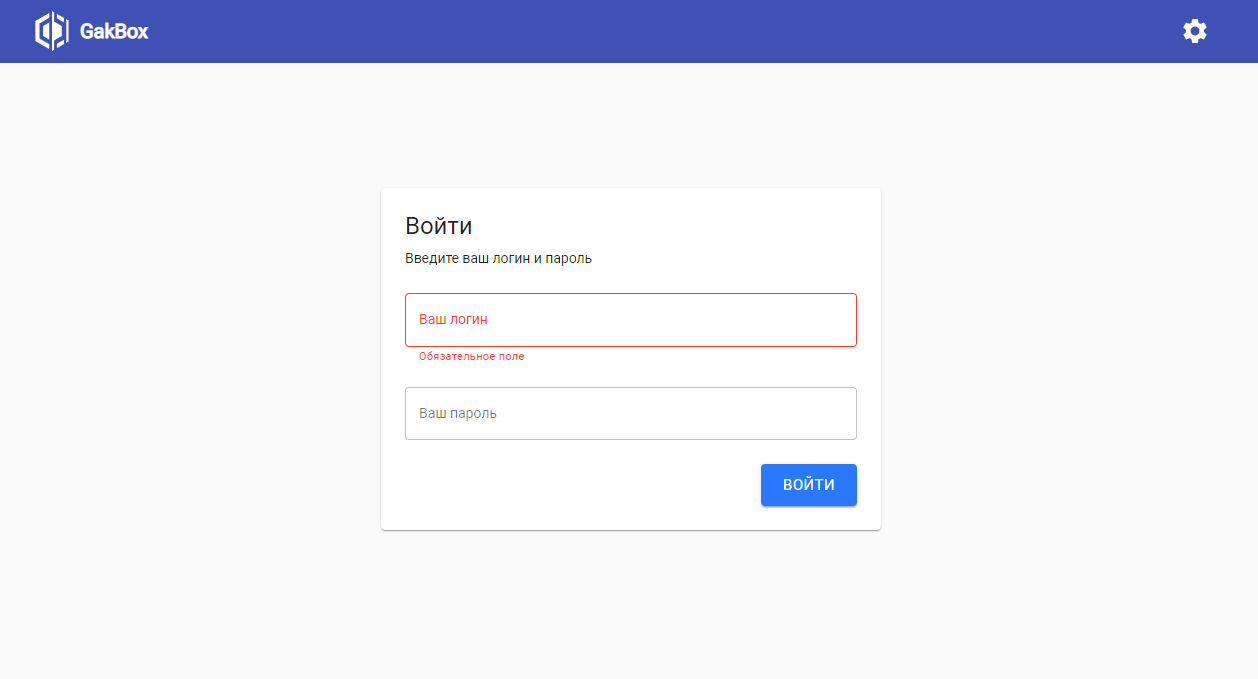
Окно программы ПО «GAK-Box 2.0» с изображением первой страницы инициализации устройства

На данной странице отображено пользовательское соглашение, прочитав которое и приняв, происходит переход на страницу создания пользователя системы.



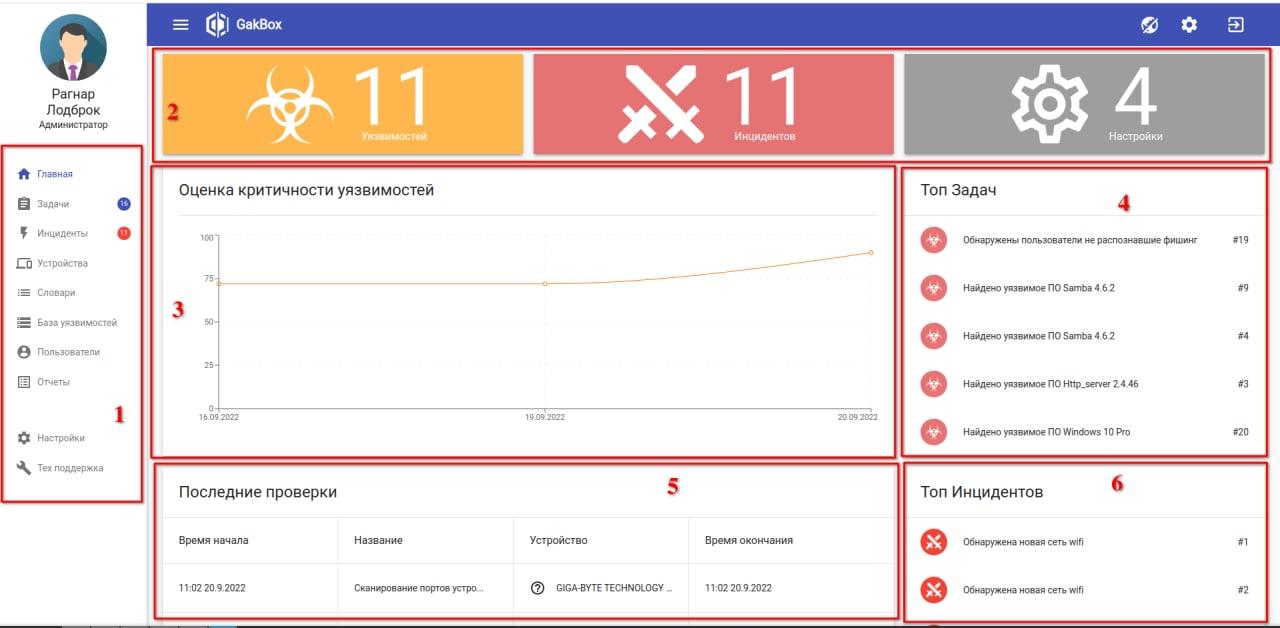
Окно программы ПО «GAK-Box 2.0» с изображением страницы ввода ключа.

У каждого устройства свой уникальный ключ лицензии, он идёт в комплекте с самим устройством.



Окно программы ПО «GAK-Box 2.0» с изображением страницы входа пользователя системы

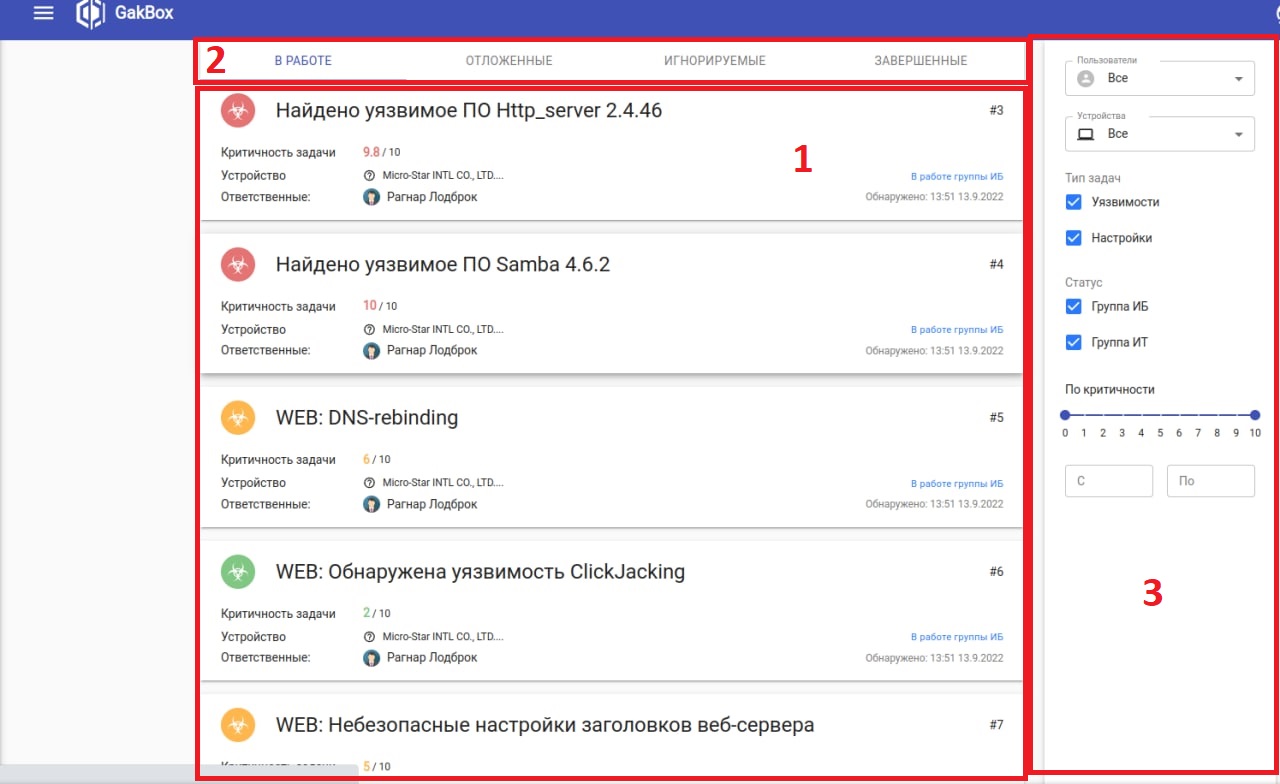
На данной странице происходит вход пользователя системы для работы в Web консоли.



Окно программы ПО «GAK-Box 2.0» с изображением главной страницы

На главной странице отображена основная информация:

1. Главное меню устройства
2. Общее количество событий
3. График общей уязвимости локальной сети
4. Последние задачи
5. Последние проверки
6. Последние инциденты

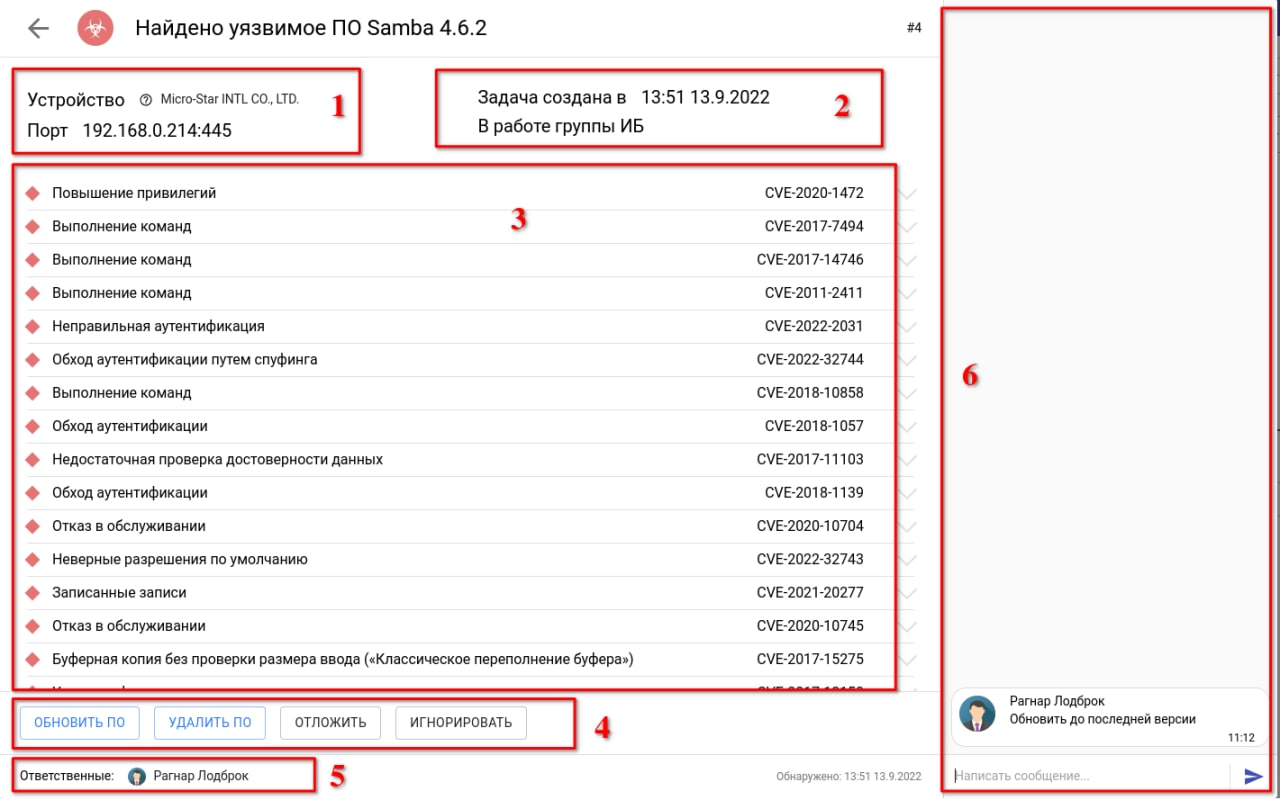


Окно программы ПО «GAK-Box 2.0» с изображением страницы задач с уязвимостями локальной сети

На данной странице отображаются все найденные уязвимости на устройствах, собранных сканерами локальной сети, web-сканнером, агентом и устройством перехвата воздушного трафика.

Элементы интерфейса:

1. Список обнаруженных уязвимостей
2. Статусы уязвимостей
3. Фильтр по уязвимостям, включающий в себя выбор конкретного устройства, критичности уязвимости и пользователя, который который ответсвенный за



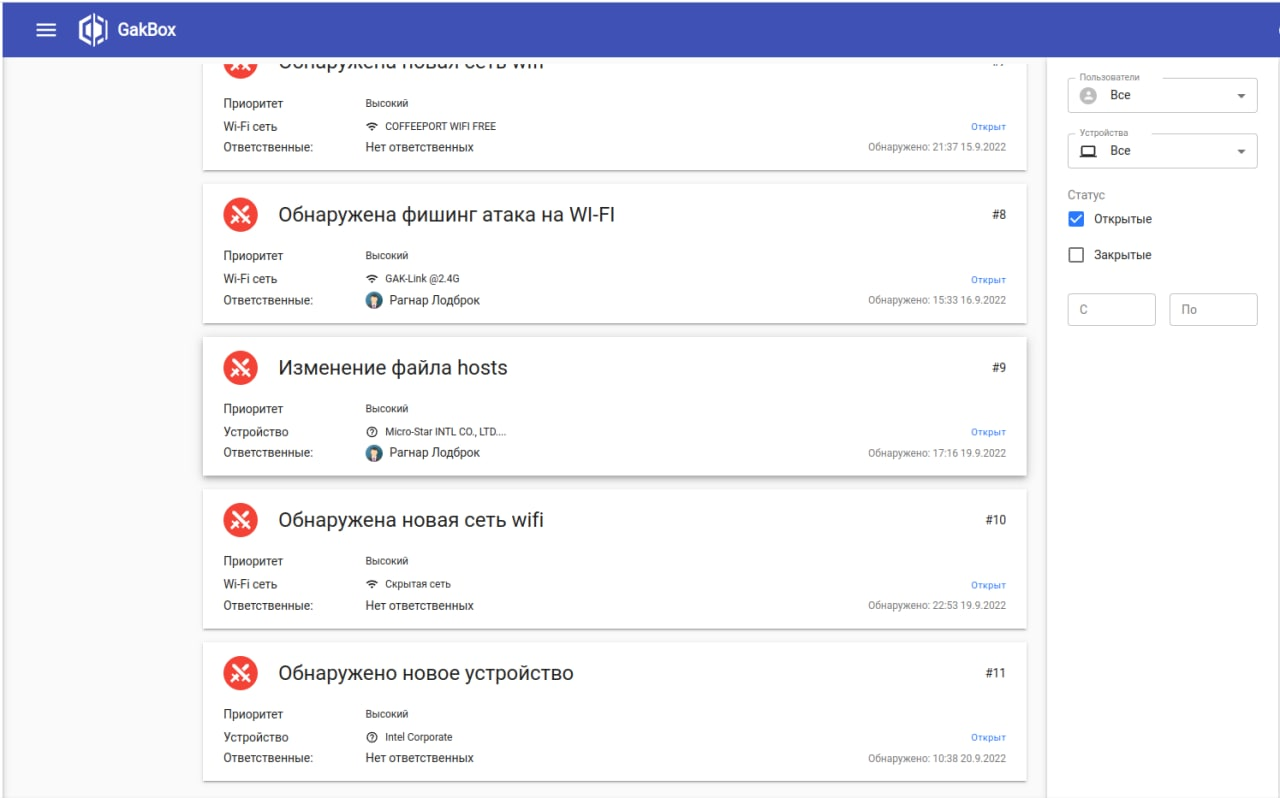
Окно программы ПО «GAK-Box 2.0» с изображением открытой уязвимости

На данном изображении показана открытая форма уязвимости, где указана информация по уязвимости: на каком устройстве было обнаружено, дата обнаружение, название уязвимости и описание.

Конкретно на данном скриншоте показан пример уязвимости софта обнаруженного с помощью сканирования порта локальной сети. В ней показан список CVE, нажав по которой, откроется ее описание.

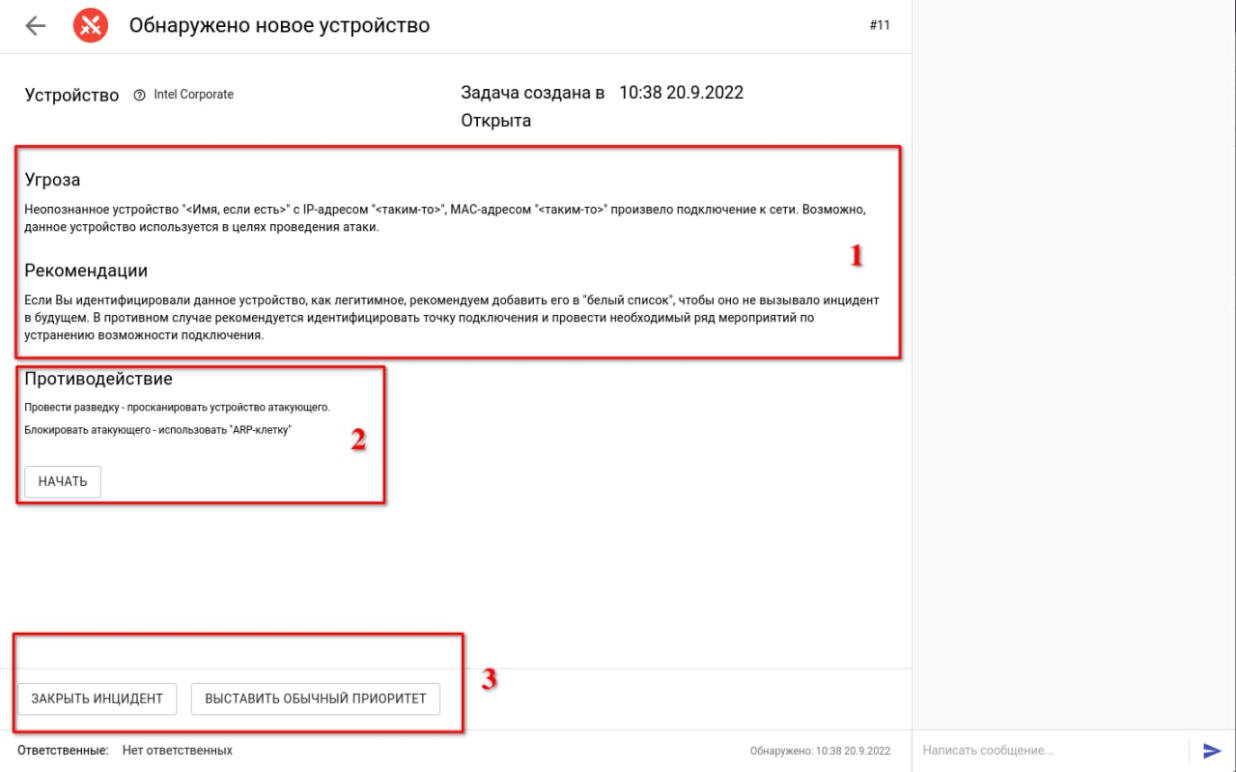
Элементы интерфейса:

1. Устройство, на котором обнаружена уязвимость
2. Время создания задачи и группа ответственных
3. Список CVE
4. Действия с задачей
5. Ответственные
6. Чат



Окно программы ПО «GAK-Box 2.0» с изображением страницы инцидентов локальной сети

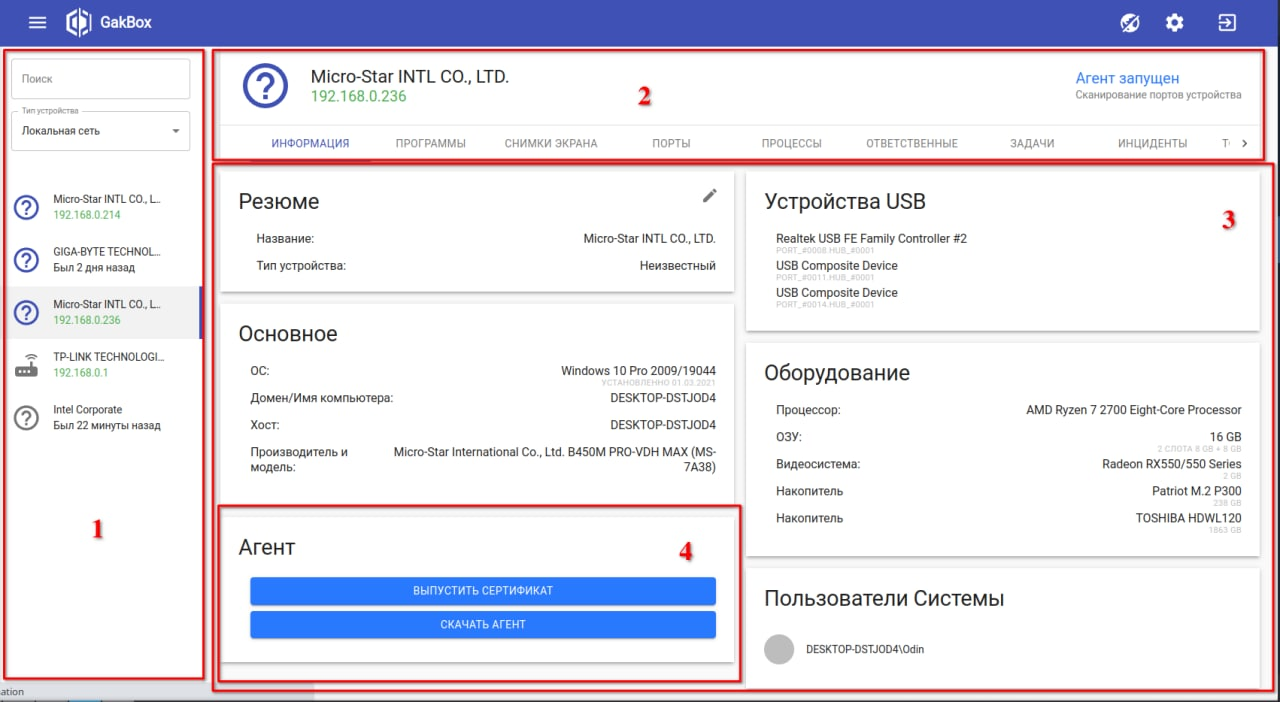
На данной странице список инцидентов, обнаруженных в локальной сети. Элементы интерфейса похожи, как и на странице задач с уязвимостями



Окно программы ПО «GAK-Box 2.0» с изображением открытого инцидента

Так же, как и у уязвимостей, здесь есть название, описание и устройство, на котором обнаружено событие. Основное отличие в центральном блоке. Там появились 3 элемента

1. Описание угрозы с рекомендациями по противодействию
2. Возможность начать противодействие
3. Действия над инцидентом

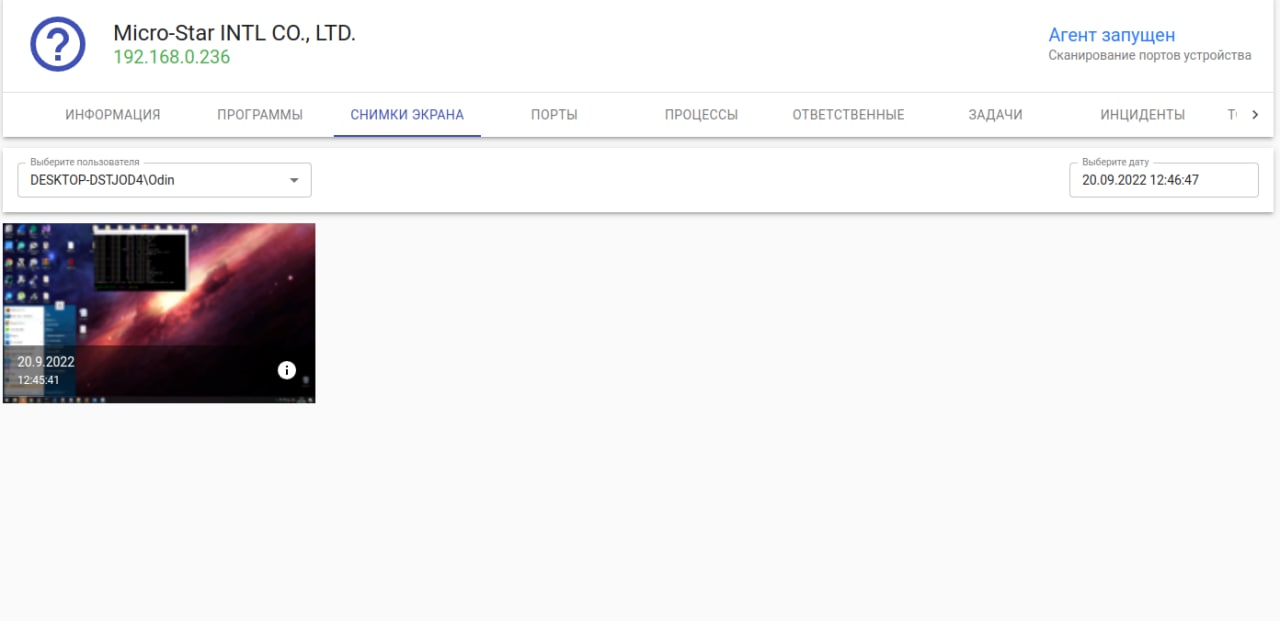


Окно программы ПО «GAK-Box 2.0» с изображением страницы устройств

1. Список устройств в локальной сети
2. Название, адрес и состояние агента на устройстве. Внизу вкладки, предоставляющие информацию об устройстве
3. Основной блок информации. В данном случае, отображена информация, собранная программой «Агент»
4. Окно для загрузки агента и выпуска сертификата

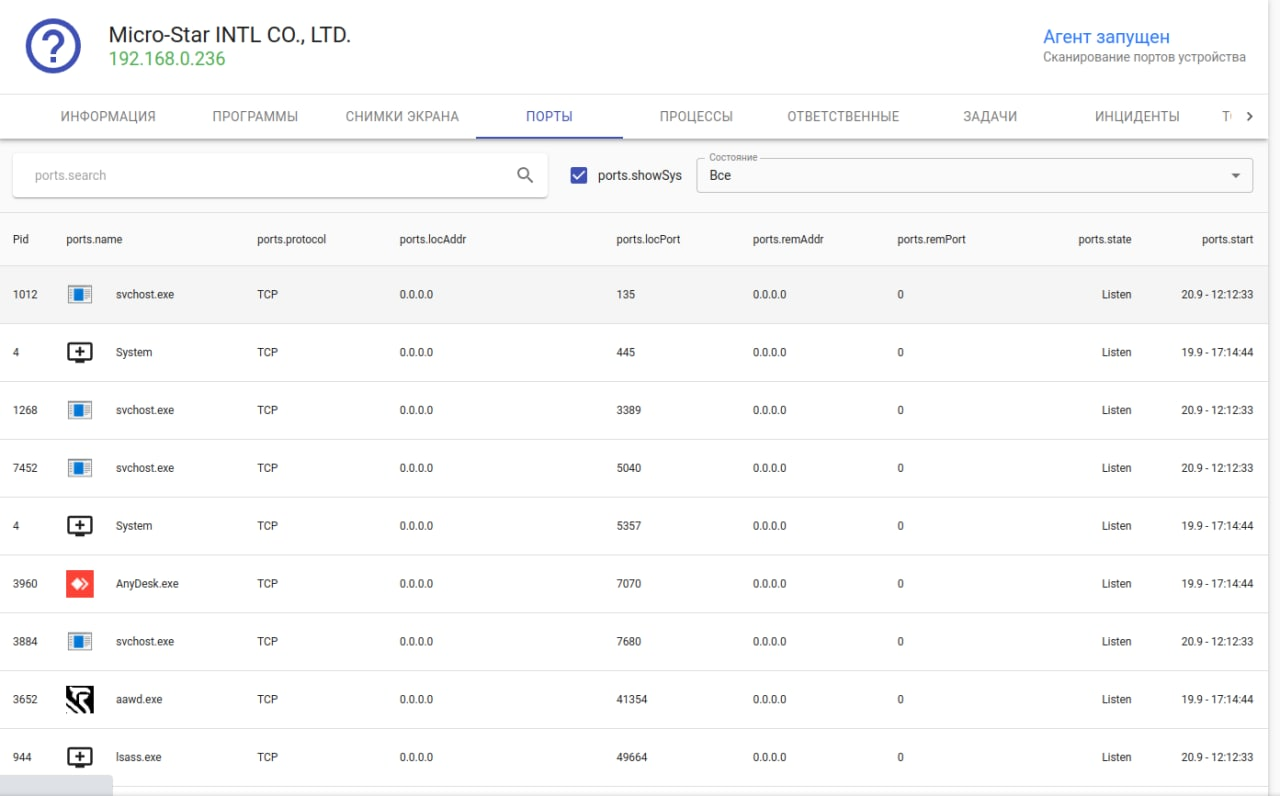
На данной странице показан список устройств в локальной сети, открыв которое будет отображена основная информация по устройству, так же найденные на нем уязвимости и события

Так же, если на устройстве установлено программное обеспечение «агент», информация, собранная им, отображается в общей информации устройства: полная информация об устройстве, включая имя компьютера и производителя, пользователей устройства, оборудование (процессор, оперативная память, видеокарта), подключенные usb устройства. Так же собирается список установленных программ на устройстве (изображение ниже).



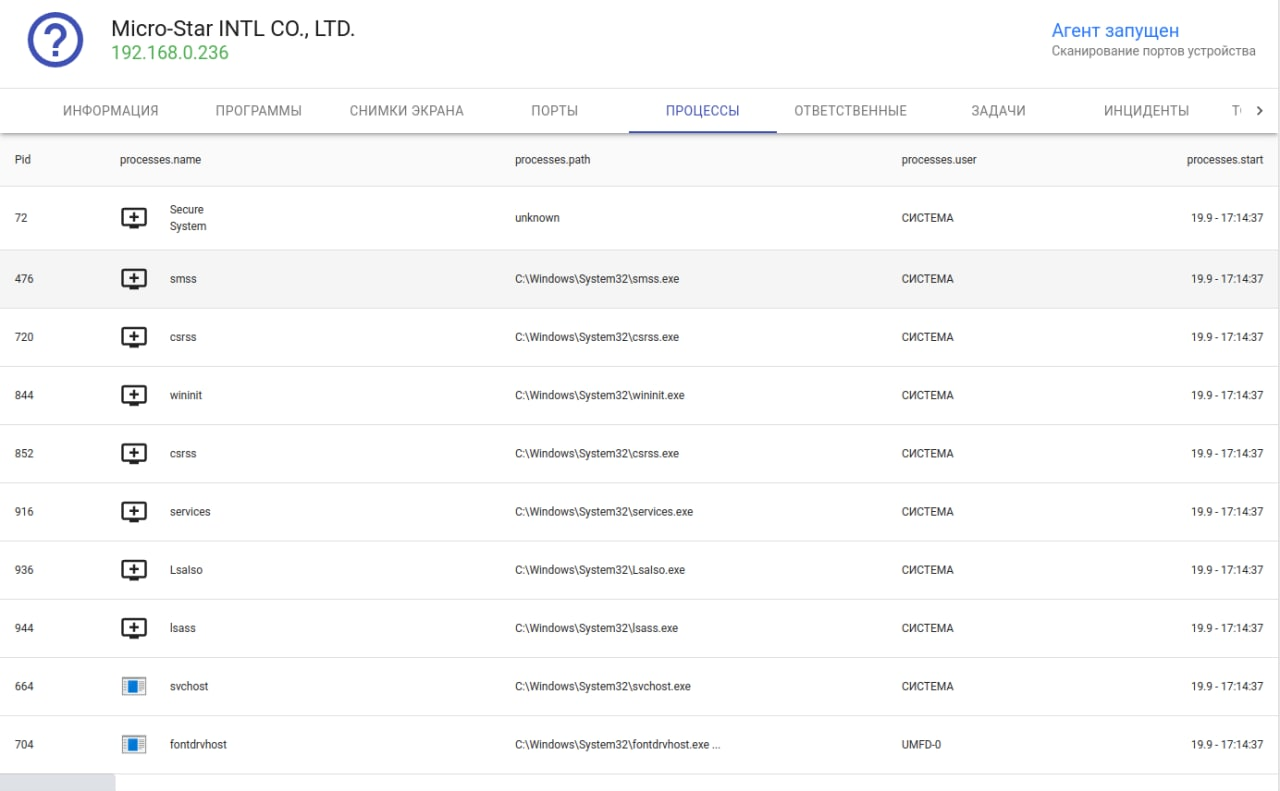
Окно программы ПО «GAK-Box 2.0» с изображением страницы скриншотов рабочей области

На данной странице можно просматривать скриншоты пользователей, сделанные через равные промежутки времени, которые выставляются во вкладке «настройки» далее в этой же области.



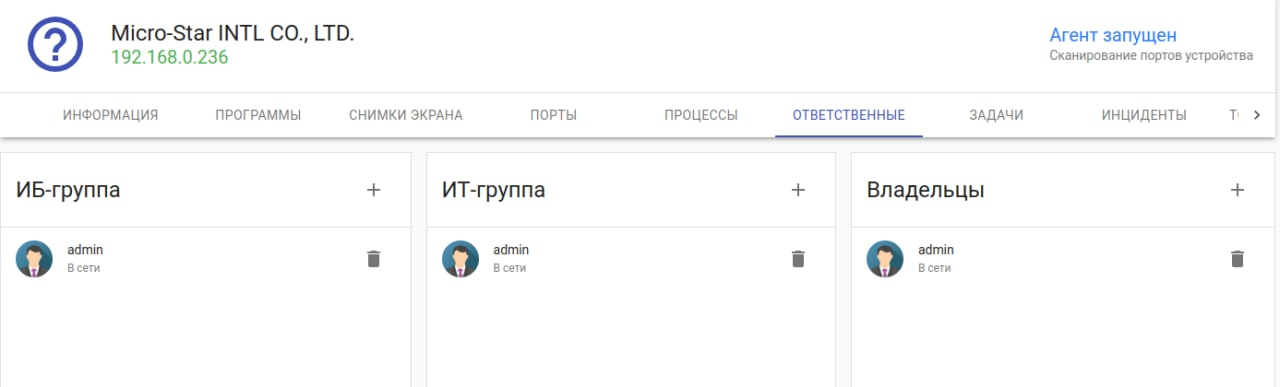
Окно программы ПО «GAK-Box 2.0» с изображением страницы портов устройства

На данной странице отображаются порты и устройства, которые их слушают, состояния и адреса, на которых висят сокеты. Эта информация собирается программой «агент»



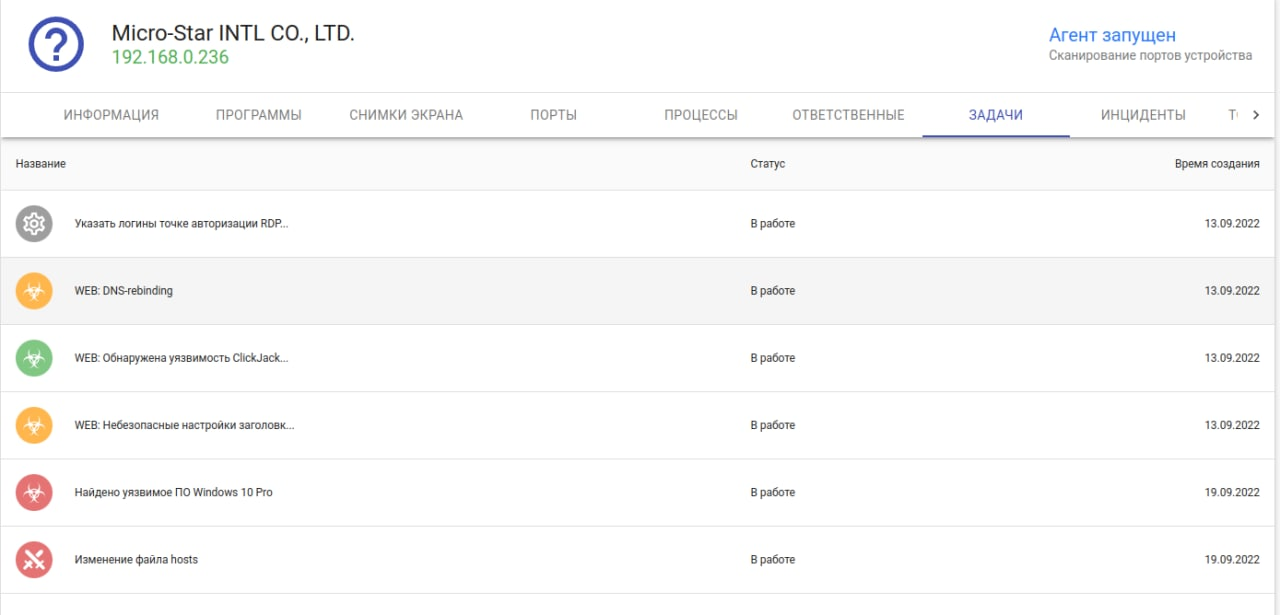
Окно программы ПО «GAK-Box 2.0» с изображением страницы процессов устройства

Тут отображаются процессы, запущенные на устройстве, их пути в системе и pid.



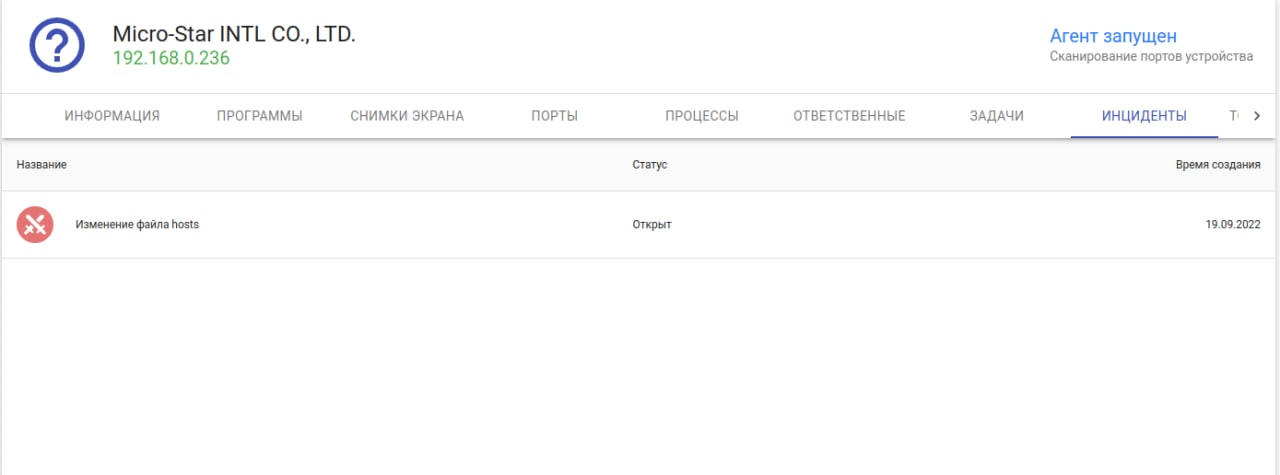
Окно программы ПО «GAK-Box 2.0» с изображением страницы отвественных

В этом окне отображены ответственные за устройство и владельцы устройства. В этом же окне их можно добавлять/удалять



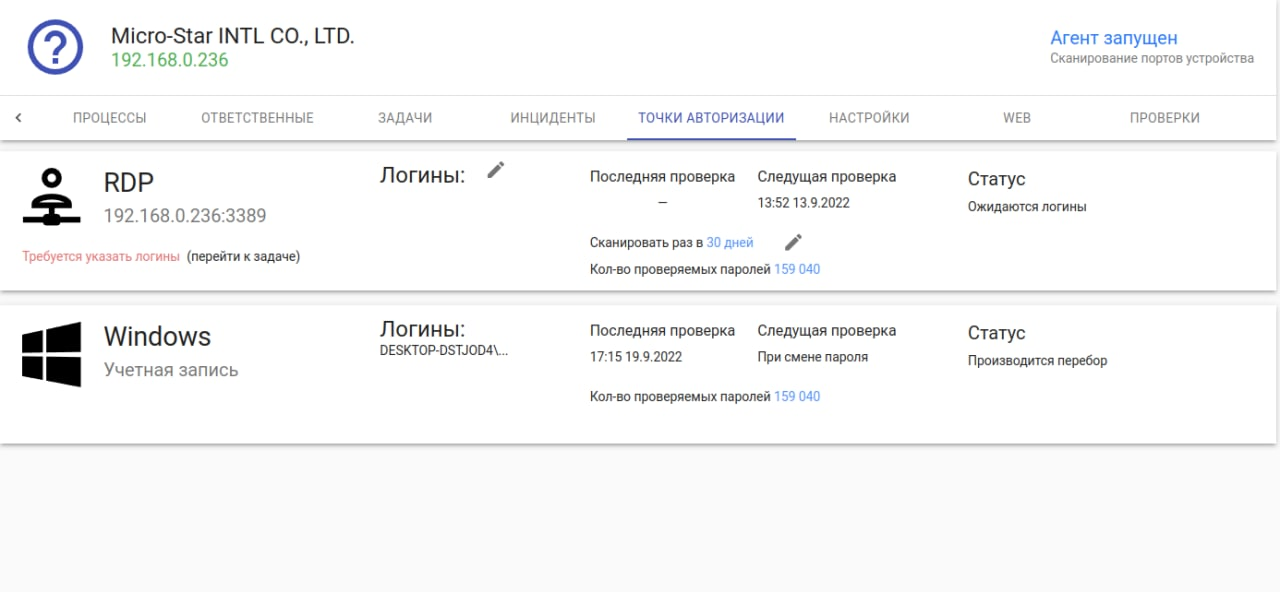
Окно программы ПО «GAK-Box 2.0» с изображением страницы задач конкретного устройства.

В этом окне отображаются задачи, их статусы и время создания



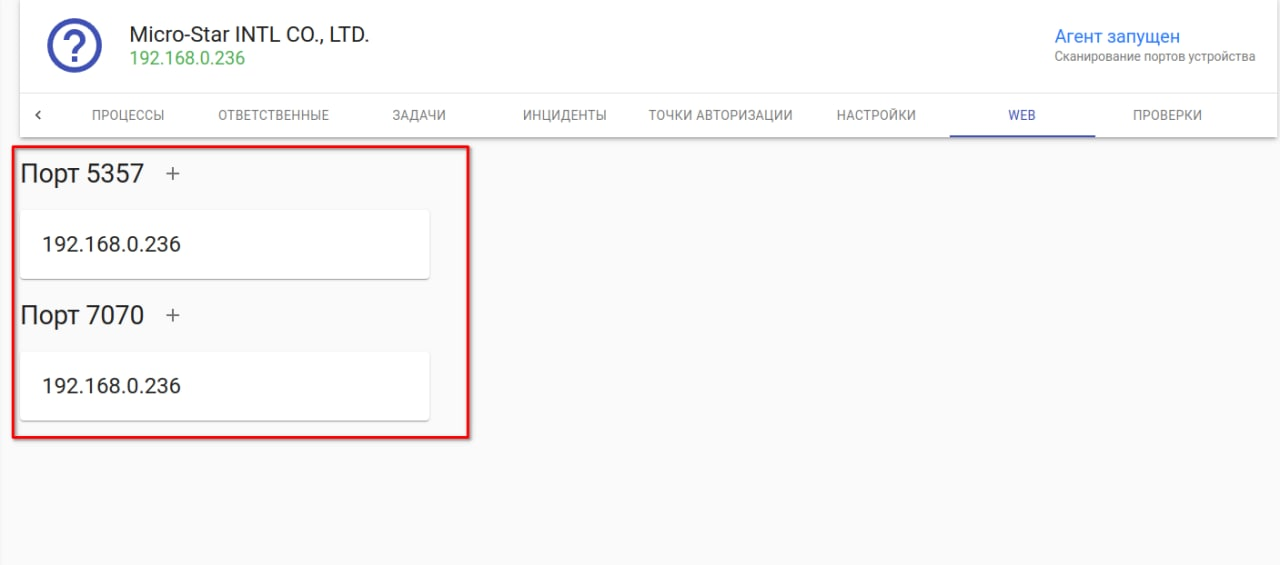
Окно программы ПО «GAK-Box 2.0» с изображением страницы инцидентов конкретного устройства.

В этом окне отображаются инциденты, их статусы и время создания.



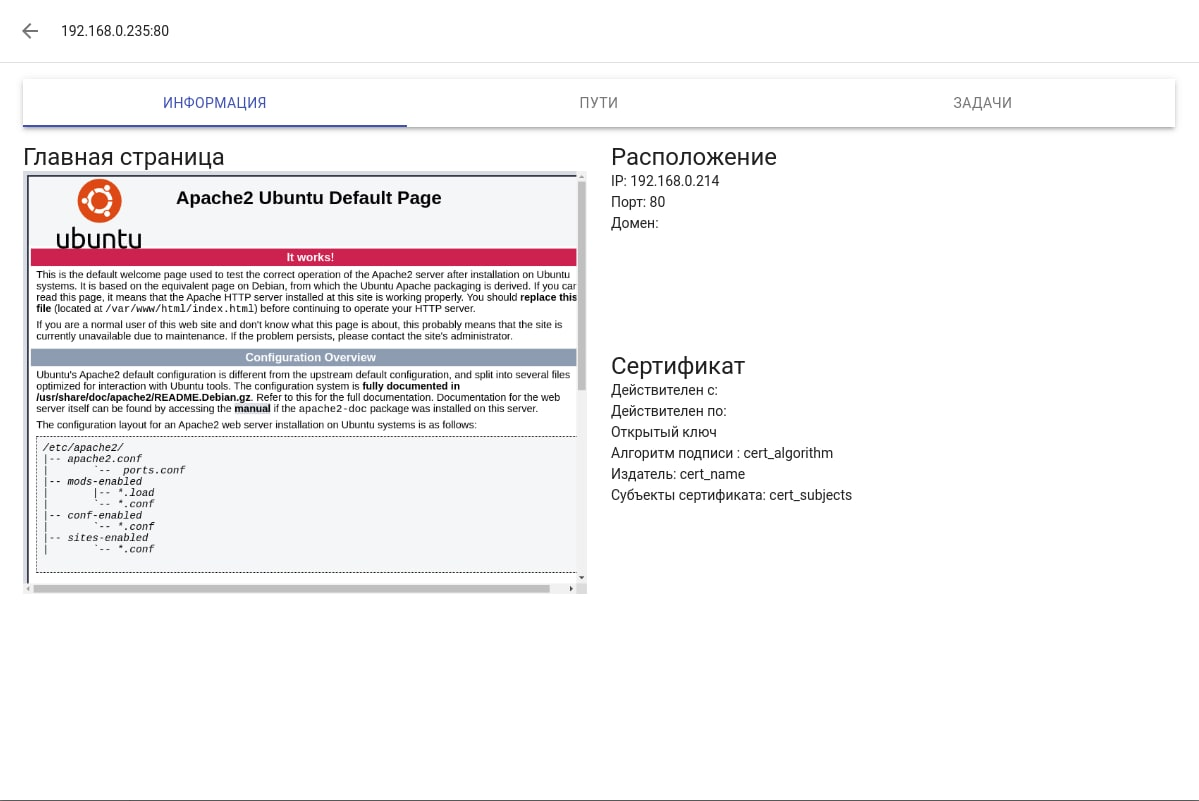
Окно программы ПО «GAK-Box 2.0» с изображением точек авторизации устройства.

В этом окне отражены обнаруженные точки авторизации, такие как SSH, RDP и так далее. Указываются процессы и результаты перебора логинов и паролей и их статусы. Нажав на карандаш, можно редактировать данные, такие как «Логины»



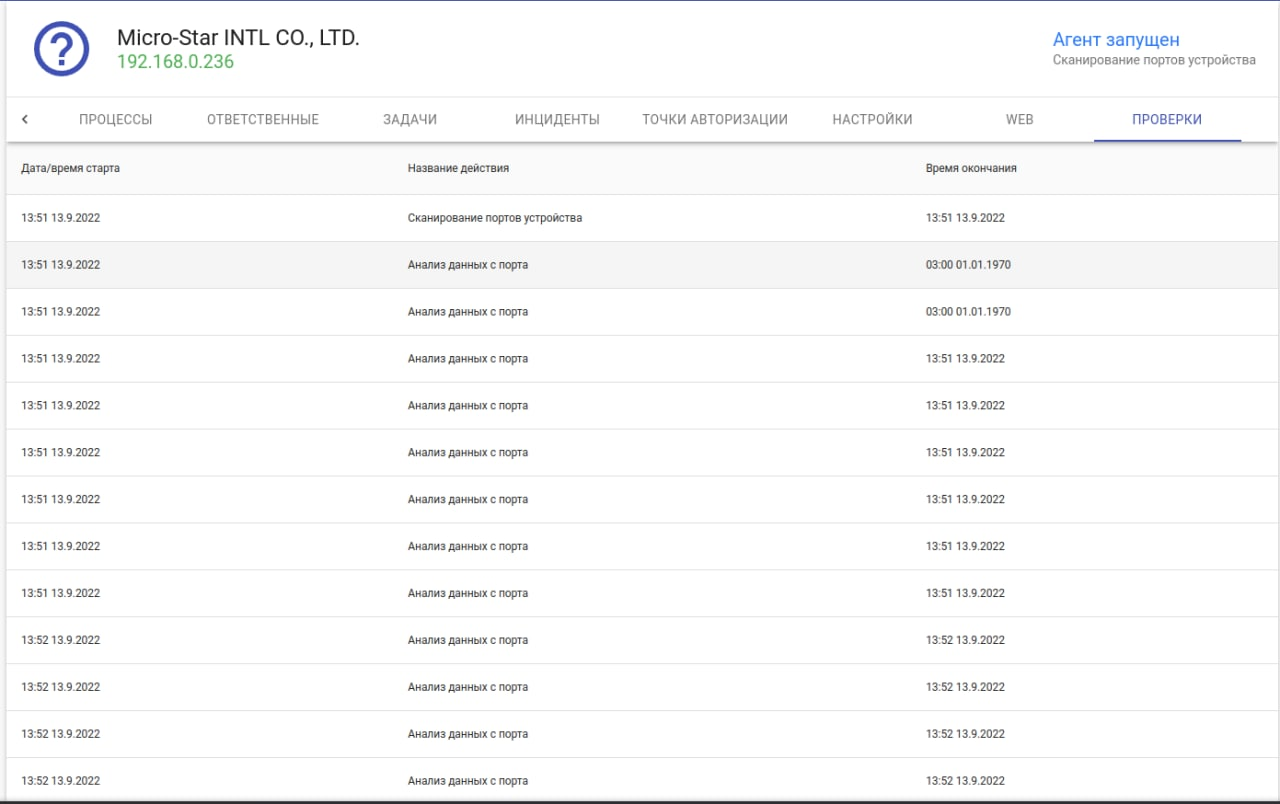
Окно программы ПО «GAK-Box 2.0» с изображением вкладки web устройства.

Во вкладке web указываются порты, на которых висит какой-либо web интерфейс. Нажав на кропку «+» рядом с номером порта, можно добавить доменное имя для web интерфейса на этом порте. При нажатии на кнопку с ip адресом, откроется следующее окно (скриншот ниже)



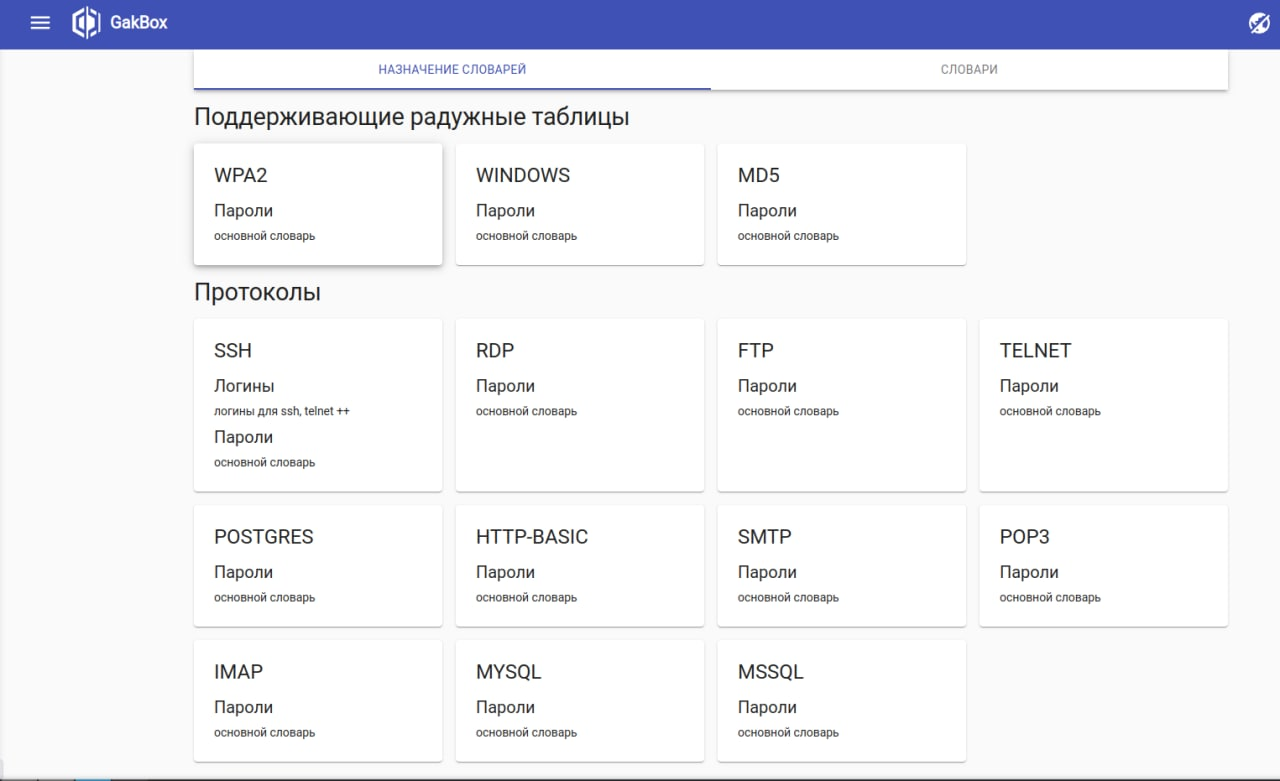
Окно программы ПО «GAK-Box 2.0» с изображением открытого окна вкладки web устройства.

В этом окне отображается скриншот интерфейса (если есть), расположение и сертификат (если есть). Так же в соседних вкладках отображены пути и задачи, связанные с этим веб интерфейсом.



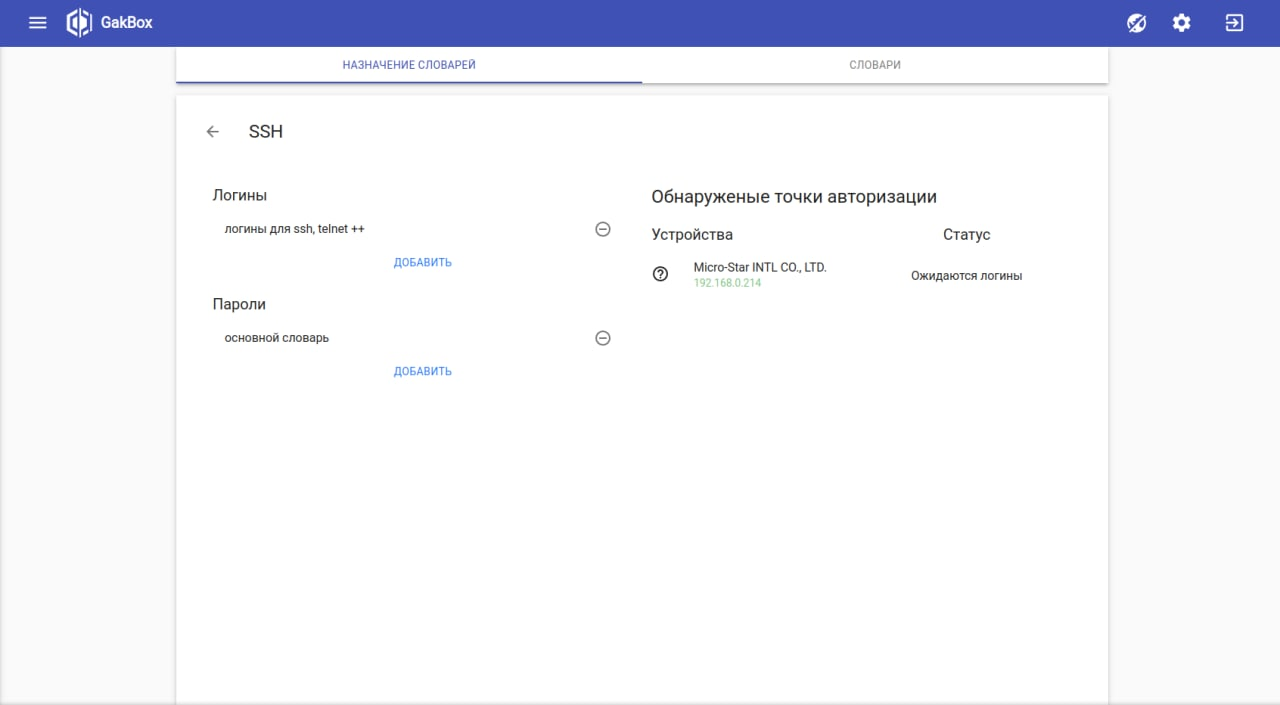
Окно программы ПО «GAK-Box 2.0» с изображением вкладки проверки устройства.

В этой вкладке отображена история проверок устройства



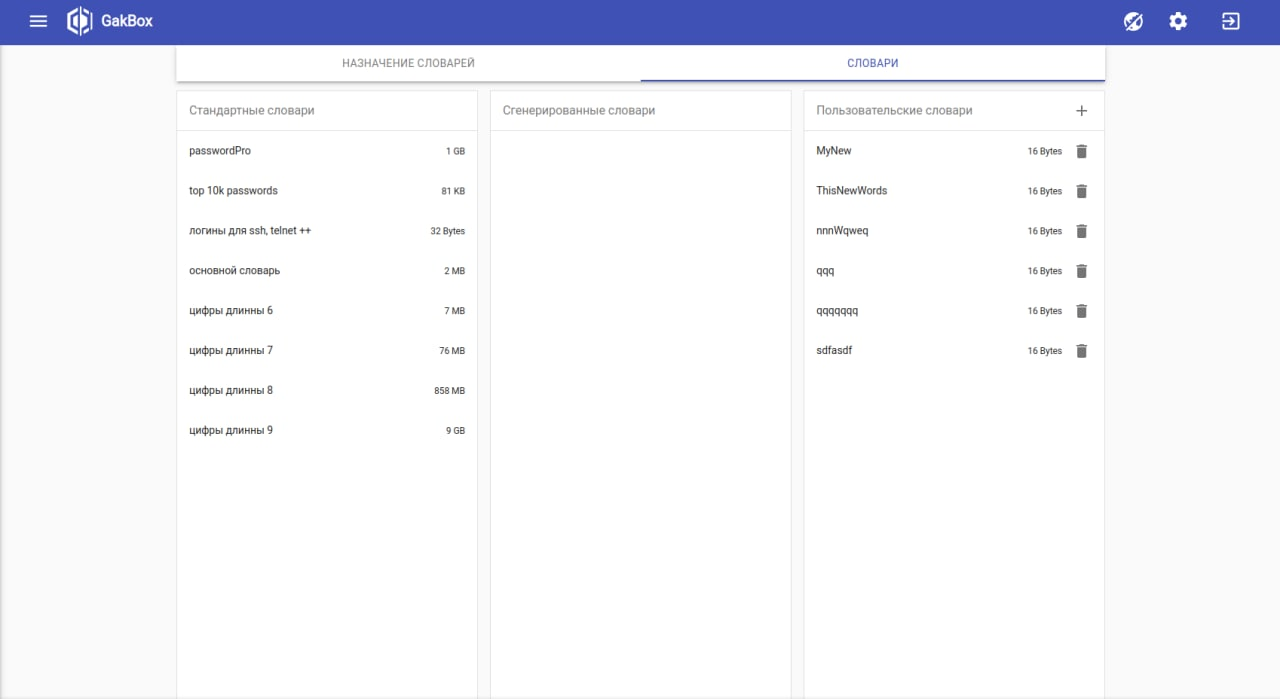
Окно программы ПО «GAK-Box 2.0» с изображением вкладки словарей.

В этой вкладке назначаются словари для перебора логина или пароля, или пары логин/пароль. Словари назначаются на протоколы



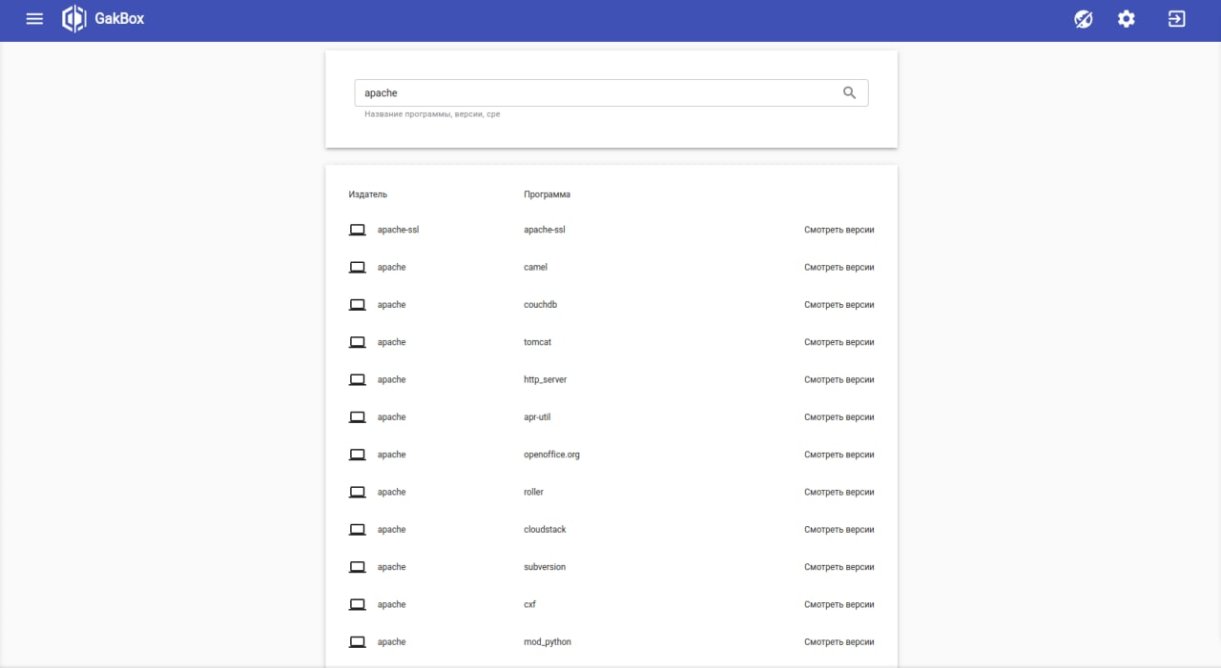
Окно программы ПО «GAK-Box 2.0» с изображением вкладки словарей для протокола SSH.

В этой вкладке назначение словарей для протокола SSH. Сюда добавляются либо удаляются словари логинов и паролей. Логины для SSH указываются в настроечной задаче, которая требует указать логины авторизации для протоколов. Справа указан статус переборов для устройств.



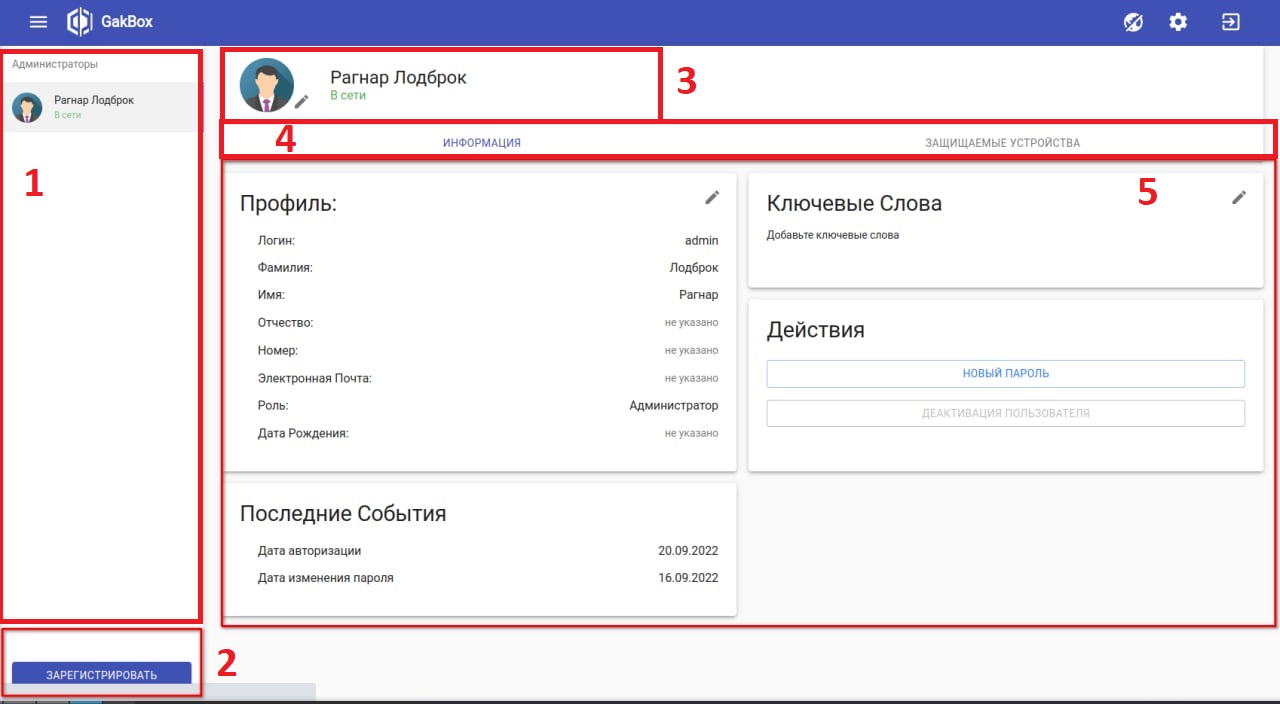
Окно программы ПО «GAK-Box 2.0» с изображением вкладки загрузки словарей.

В этой вкладке можно посмотреть имеющиеся словари, и загрузить собственные словари. 1 файл не должен превышать размер в 1 Гб. Посмотреть содержимое словарей через веб интерфейс нельзя.



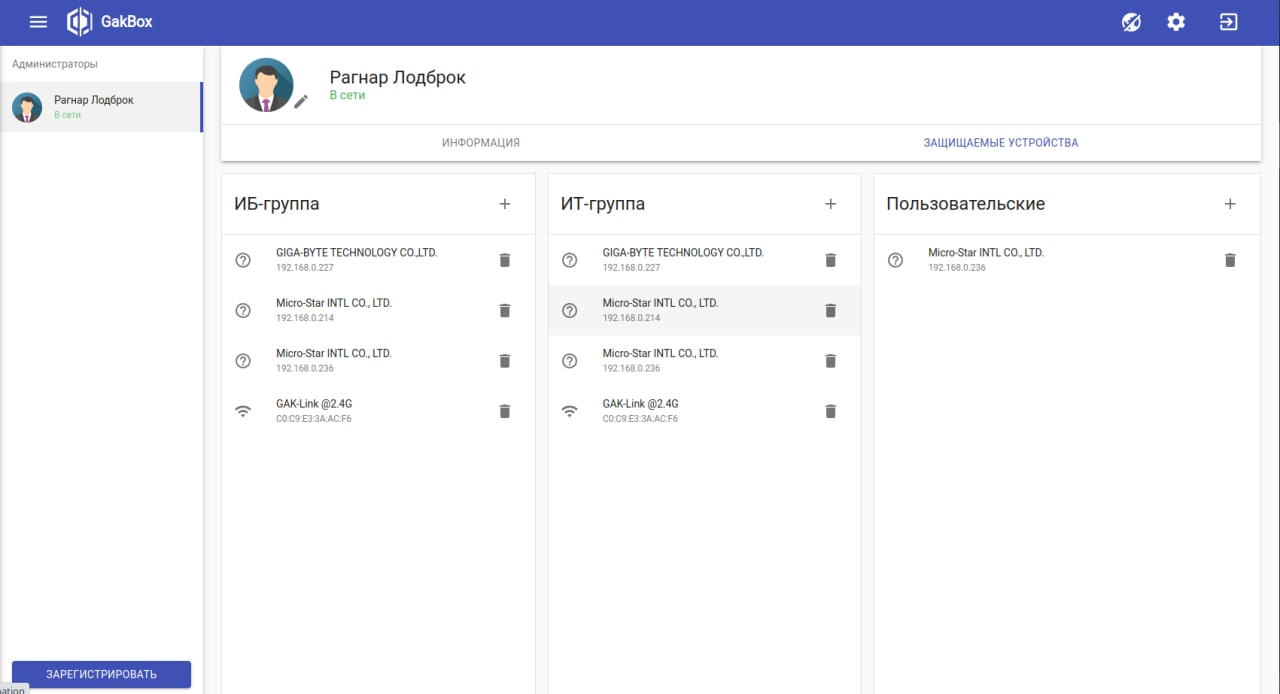
Окно программы ПО «GAK-Box 2.0» с изображением вкладки базы данных уязвимостей

В этой вкладке можно найти ПО, по названию или по CVE, и посмотреть содержимое базы данных. На скриншоте продемонстрирован поиск ПО – apache. Поиск вернул разных вендоров для apache. Кликнув по кнопке «Смотреть версии» будет выведен список версий от этого вендора. Кликнув по версии, будет выведен список CVE связанных с этой версией.



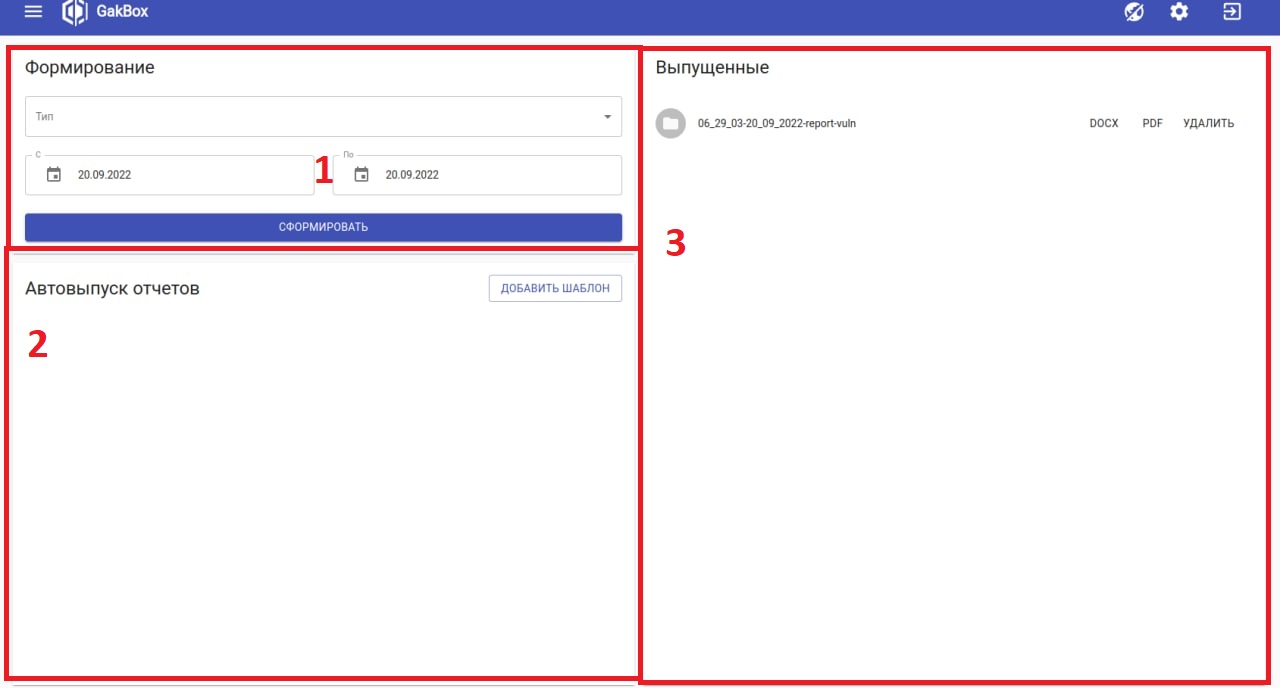
Окно программы ПО «GAK-Box 2.0» с изображением вкладки пользователей

Слева отображается список пользователей (1). Внизу кнопка регистрации пользователей (2). Сверху отображается имя и фамилия пользователя (3). Центральная панель (5) содержит информацию о пользователей. Чтоб посмотреть круг ответственности пользователя, выберите вкладку защищаемые устройства (4).



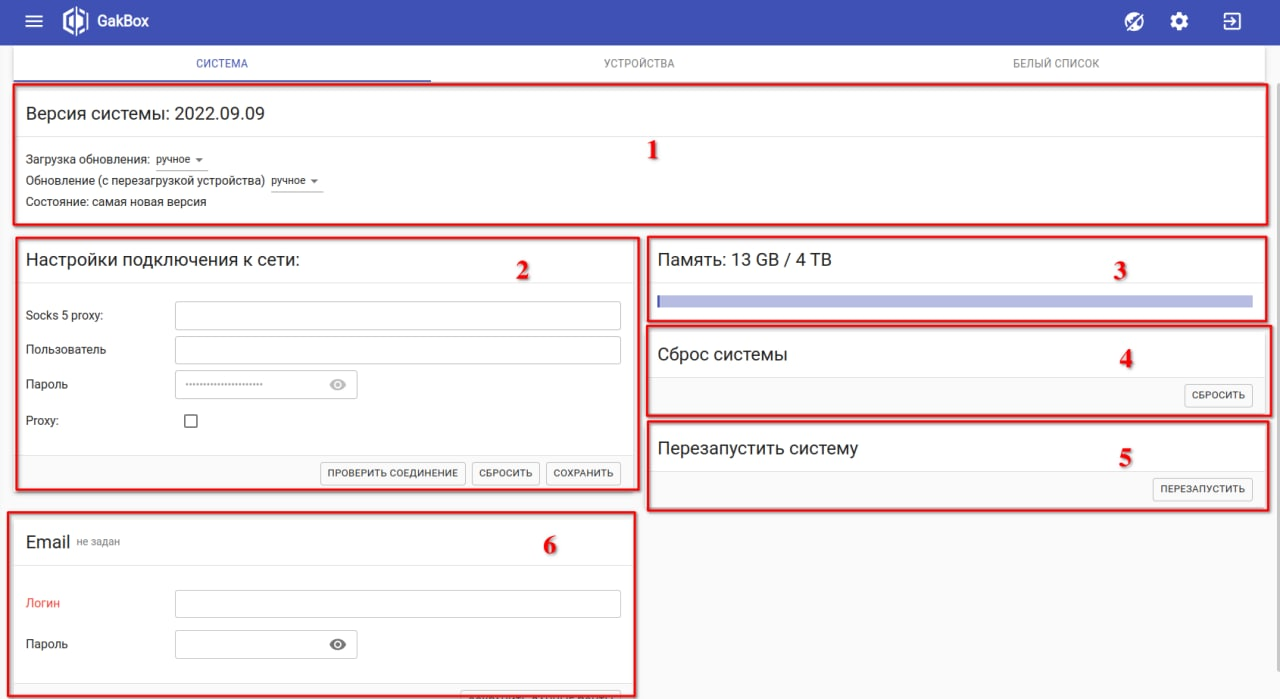
Окно программы ПО «GAK-Box 2.0» с изображением вкладки защищаемых устройств пользователя.

На изображении защищаемые устройства и круг ответственности пользователя.



Окно программы ПО «GAK-Box 2.0» с изображением вкладки отчётов.

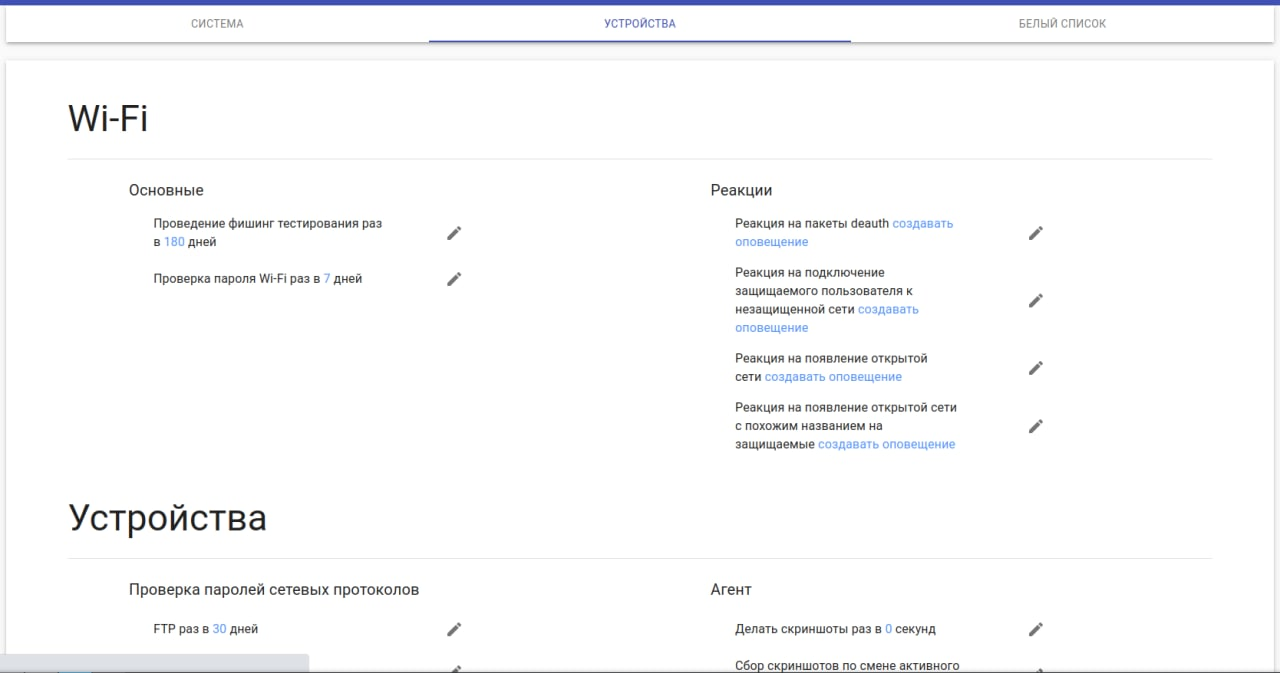
Отчёты формируются вручную (1), выбрав тип и дату периода отчёта. Готовый отчёт появится в правом окне (3). Либо можно автоматизировать генерацию отчётов через окно автовыпуска отчётов (3).



Окно программы ПО «GAK-Box 2.0» с изображением вкладки настроек.

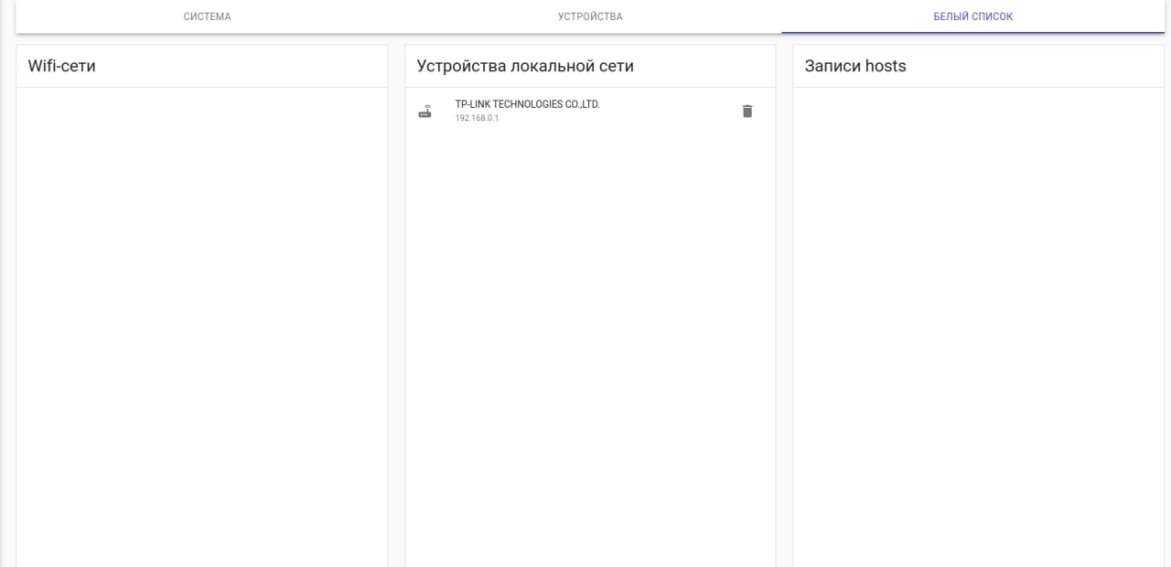
Окно настроек содержит окно версии и обновлений (1). Для обновления нужен интернет. Как становится доступно обновление, справа окна (1) появится кнопка «загрузить» обновление. После загрузки появится кнопка «установить». Так же можно поменять режим обновления на «автоматический». Возможно настроить proxy (2), указать почту для уведомлений (6).

Справа располагается индикатор свободной памяти (3) и кнопки сброса системы (4) и перезапуска (5).



Окно программы ПО «GAK-Box 2.0» с изображением вкладки настроек устройств.

В этой вкладке можно настроить различные параметры, связанные с устройствами

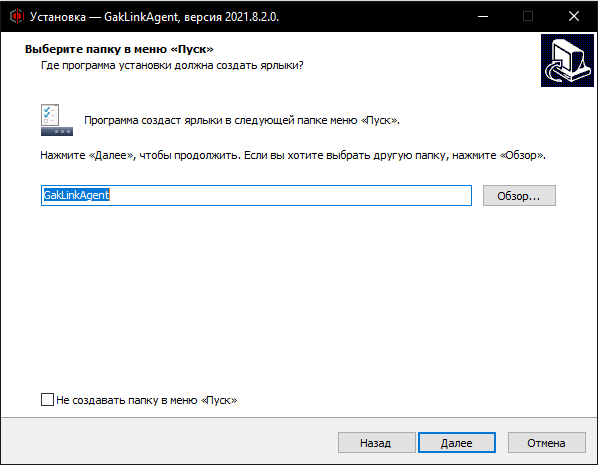
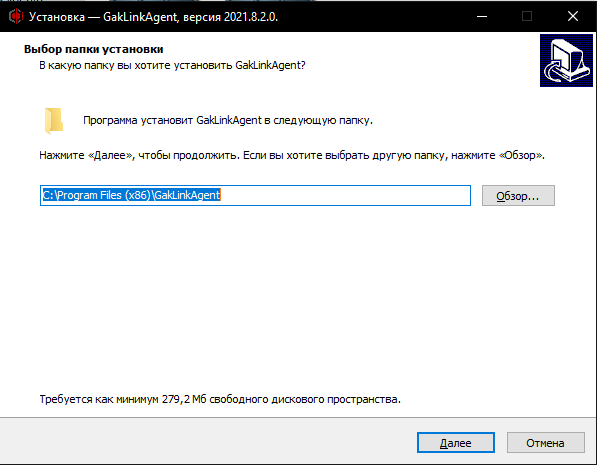


Окно программы ПО «GAK-Box 2.0» с изображением вкладки настроек устройств.

Белый список устройств, это список устройств на которых игнорируются некоторые уязвимости и неверные настройки.

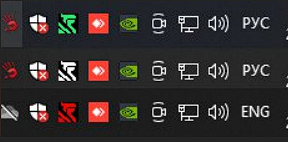
**Руководство по установке и эксплуатации ПО «агент»**

Скачав программу со страницы «система» и запустив установщик, запустится обычная установка программного обеспечения, где потребуется указать куда устанавливать устройство и основные настройки для установки ПО.

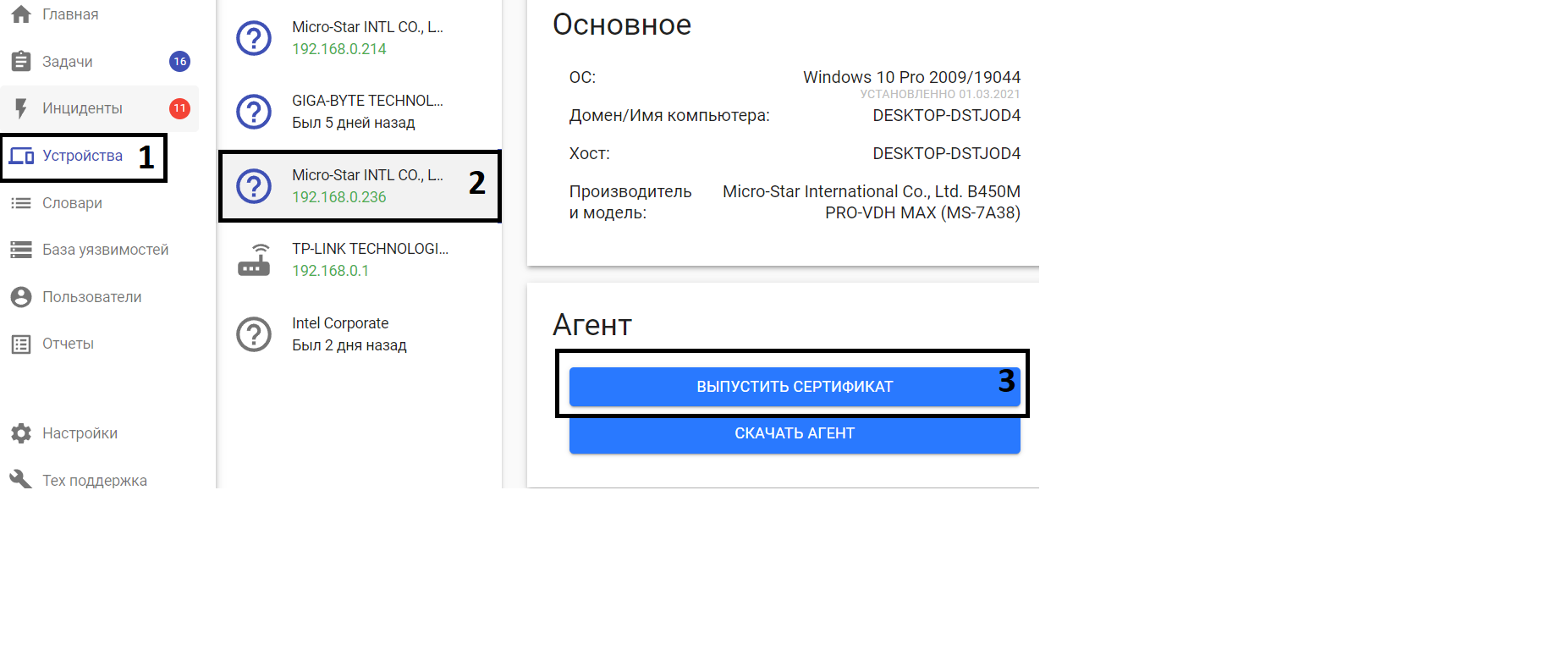


Изображения установки ПО «агент»

После установки программного обеспечения «агент», на рабочем столе появится ярлык GrifonAgent. После двойного нажатия запустится служба и интерфейс программы, которая будет отображаться на панели задач:



Нажав правой кнопкой мыши по значку агента, откроются его настройки. Далее, в окне web интерфейса, во вкладке «устройства» выберите устройство, на который было поставлено ПО «агент», и нажмите кнопку «Выпустить сертификат»



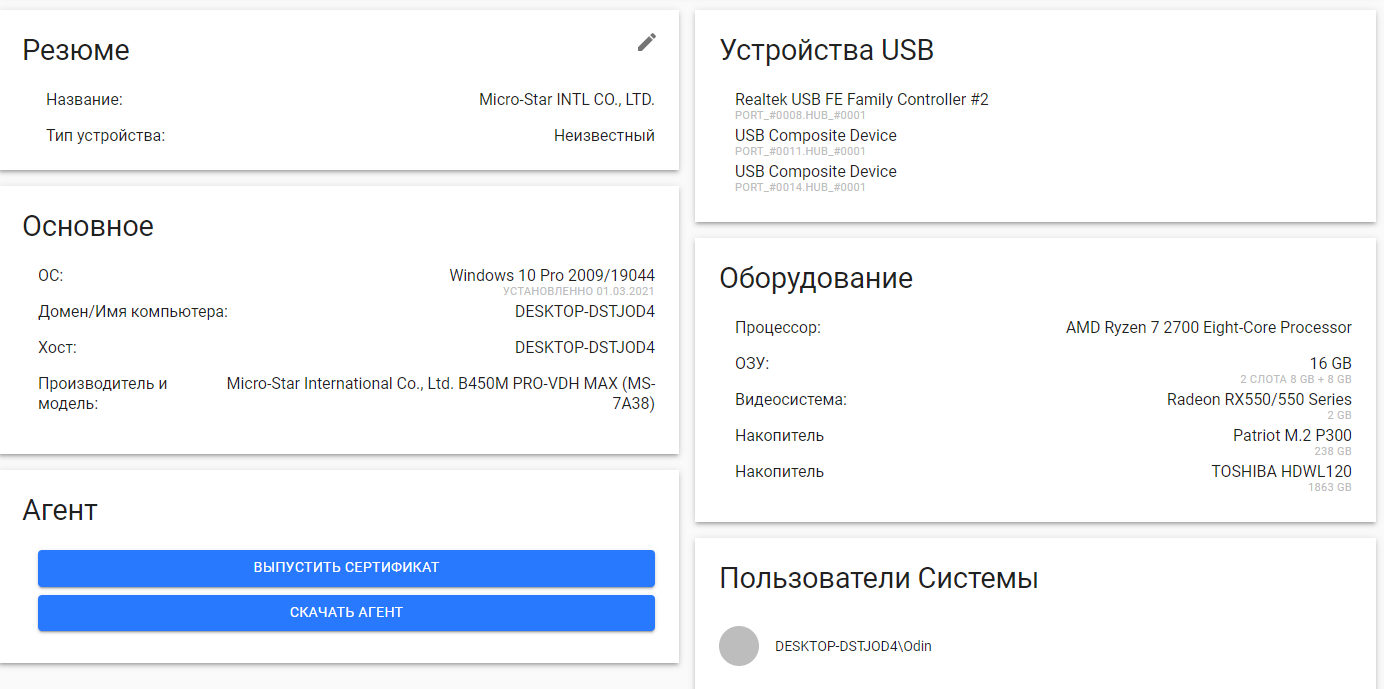
Окно программы ПО «GAK-Box 2.0» с пошаговым изображением выпуска сертификата.

Сертификат нужен для подключения ПО «агент» к ПО «GAK-Box 2.0», и получения дополнительной информации с устройства. Для выпуска сертификата для устройства, на котором стоит ПО «агент», следуйте шагами на скриншоте выше (названия и адреса устройств будут другими).  
 После загрузки сертификата, либо кликните на него двойным щелчком и он установится сам, либо нажмите правой кнопкой мыши по значку на панели задач, и нажмите «Установить сертификат». Откроется диалоговое окно, в котором необходимо указать пусть до загруженного ранее сертификата.

Удаляется программное обеспечение «агент» как все программы через приложения и возможности, просто выбрав программу в списке всех программ и нажав кнопку удалить.

Агент через службу собирает основную информацию об устройстве, об аппаратных составляющих, о пользователях системы, список софта, подключенные usb устройства.

ПО работает автономно, и не требует действий со стороны пользователя. Больше половины информации, которая была продемонстрирована в инструкции была собрана агентом. Ниже на скриншоте указана информация об устройстве и комплектующих.



Окно программы ПО «GAK-Box 2.0» с изображением основной информации полученной из программы «агент»