

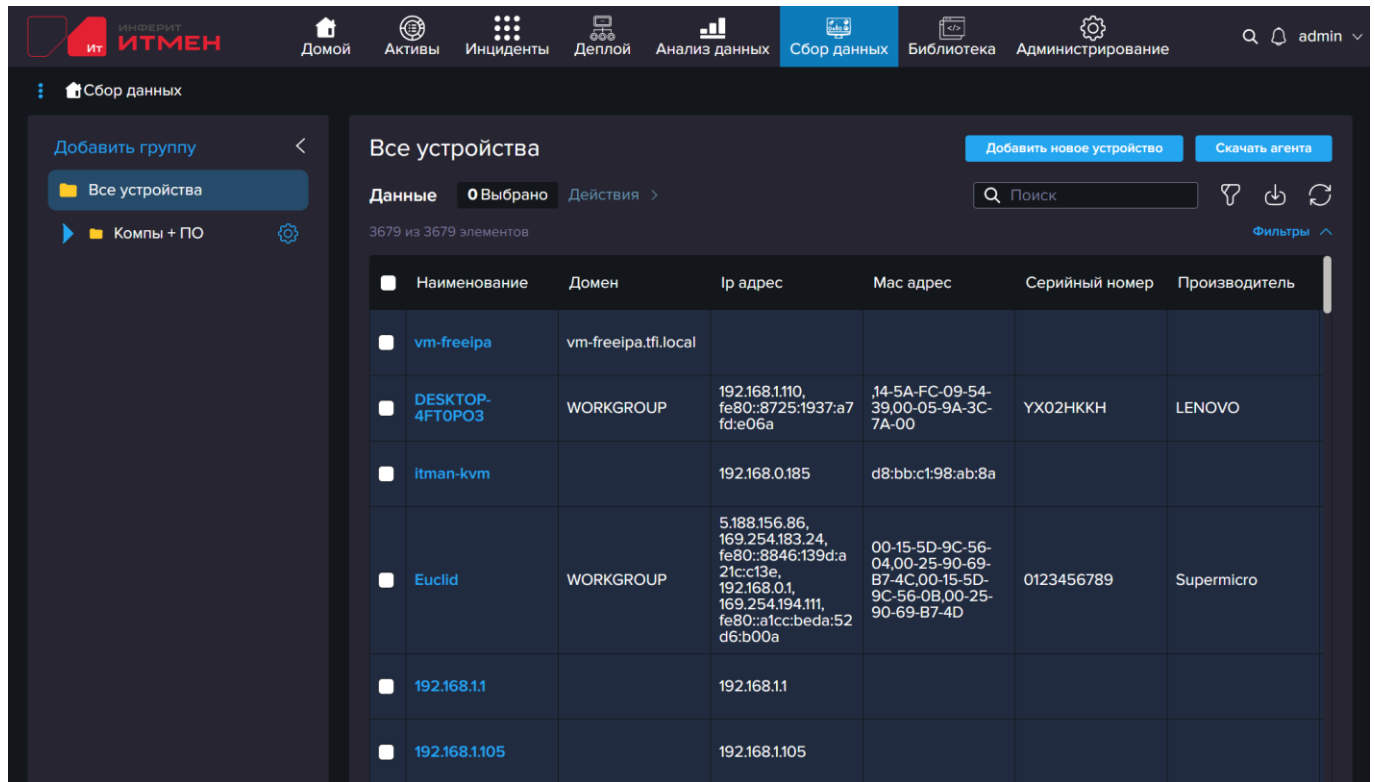
# **Инструкция по тестированию системы ИТМЕН**

## Оглавление

Инструкция по тестированию системы ИТМЕН.....	1
Краткое описание системы .....	3
1.1 Область применения .....	3
1.2 Краткое описание возможностей.....	3
2 Технические требования .....	5
Системные требования .....	5
Аппаратные требования .....	5
Учетные записи и привилегии .....	8
Что необходимо настроить чтобы попробовать демо версию? .....	9
3.1 Первое знакомство с продуктом .....	9
Шаг 1. Знакомство с системой .....	9
Шаг 2. Настройка агента.....	10
3.2.1 Раздел Администрирование.....	18
3.2.1 Настройки.....	19
3.2.2 Справочники .....	26
3.2.3 Отчетность .....	38
3.3 Сбор данных .....	41
3.3.1 Все Устройства .....	41
3.3.2 Управление инвентаризацией .....	46
3.3.3 Сенсоры.....	60
3.3.4 Модель данных .....	65
3.4 Анализ данных .....	70
3.5 Библиотека.....	72
3.6 Разделы в доработке .....	81
3.6.1 Активы.....	81
3.6.2. Все активы.....	81

## 1. Краткое описание системы

ИТМен – Платформа для управления ИТ-инфраструктурой (рабочие места, Сервера и т.д.) и контроля Информационной безопасности.



Архитектура работы системы состоит из компонентов, которые общаются между собой: Reader, Server, DataManager, Writer, Interact, Data Base, Agent.

### 1.1 Область применения

ИТМен помогает обслуживать устройства и проводит инвентаризацию программного обеспечения, железа, пользователей, устройств в одном окне.

### 1.2 Краткое описание возможностей

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПОД ВАШИ ЗАДАЧИ:

1. Сбор данных и обнаружение устройств в режиме реального времени:

- Автоматический поиск и обнаружение устройств,
- Сбор инвентаризационной информации WMI, SSH, SNMP,
- Сбор данных с внешних источников AD, YC, VMWare, SCCM, SW, Samba, FreeIPA,
- Нормализация данных,
- Предоставление данных в реальном времени,
- Аналитические отчеты и графические показатели,
- Настраиваемая модель данных,

Дата документа: 29.08.2024

Версия системы: 5.5

- Динамическая модель данных.

## 2. Управление ИТ-активами:

- Сохранение и идентификация ИТ-активов,
- Карточки учета ИТ-активов,
- Контроль изменений конфигураций,
- Обогащение данных с ИИ,
- Аналитика исторических данных,
- Графические показатели и аналитические отчеты.

## 3. Управление конфигурациями:

- Удаленное развертывание ПО/пакетов,
- Передача данных с технологией peer-to-peer,
- Управление обновлениями программного обеспечения,
- Удаленное управление конфигурациями,
- Управление политиками,
- Применение скриптов и кода,

## 4. Выявление инцидентов:

- Поиск уязвимостей по базе (CVE),
- Вывод данных о сроке эксплуатации ОС и ПО,
- Сканирование и отображение открытых портов,
- Проверка паролей и учетных записей,
- Создание собственных правил для поиска уязвимостей,
- Настройка правил соответствия конфигураций

## 2. Технические требования

Следующие сведения относятся к полному агенту инвентаризации при развертывании и инвентаризации на целевом устройстве.

### Системные требования

Windows	Linux
<ul style="list-style-type: none"> <li>§ Windows Server 2008 R2 x64, 2012, 2012 R2, 2012 R2, 2016, 2019, 2022</li> <li>§ Windows Server Core 2008, 2008 R2 x64, 2012, 2012 R2</li> <li>§ Windows Server Standard (ранее известный как Windows Server Core) 2016, 2019</li> <li>§ Windows 7, 8, 10, 11</li> </ul>	<ul style="list-style-type: none"> <li>§ Astra Linux – от версии 1,7</li> <li>§ Debian – от 9 версии и выше</li> <li>§ Ubuntu – от версии 4.10</li> <li>§ Astra Linux SE</li> <li>§ CentOS 7</li> <li>§ Oracle Linux Server 8.3</li> <li>§ Red Hat Enterprise 8</li> <li>§ Red Hat Enterprise Linux 7.4</li> <li>§ Suse Linux – в зависимости от версии</li> </ul>

### Аппаратные требования

В этом разделе приведены рекомендации по размеру оборудования для различных профилей установки. Чтобы узнать о конкретных требованиях к оборудованию, просмотрите профили установки, чтобы определить, какой профиль лучше всего соответствует количеству инвентаризируемых клиентских компьютеров в среде.

Это минимальные требования применимые ИТМЕН:

#### 1. Управляющий сервер:

- 2 CPU
- 8 GB RAM + 8 GB RAM при работе распознавания правил в Библиотеке ПО (от 50000 правил)
- 10Gb Disc space
- .Net Core 7.x
- Windows Server 2012 и др., 7 SP1, 8 или 8.1., и др.
- Linux Debian 9 или выше, Astra Linux, RedOS и др.

APM в необходимом количестве:

- 1 CPU
- 2 GB RAM

- 100Mb Disc space
- Windows любой выше XP
- Linux Debian 9 и выше, Astra Linux, RedOS и др.

2. Требования для Discovery.Server собирающего данные удаленно:

Процессор: AMD® A8 3870 3,6 Ghz or Intel® Core™ i3 2100 3.1Ghz

Чем мощнее процессор, чем больше ядер и потоков, тем быстрее идет обработка и импорт данных в базу, а также формирование отчетов.

Данные к потреблению полного приложения ИТМЕН

Рекомендуемые показатели к ОЗУ при инвентаризации клиентских компьютеров от 1- 10000:

Сервер	Модули приложения	Память (ГБ)	ЦП/Ядра	Хранилище (конфигурации диска)
1	Discovery.Server	4	1/2	20ГБ
2	Discovery.Interact	2	1/2	5ГБ
3	Discovery.Agent	0,5	1/2	2ГБ
4	Discovery.Agent+ SCCM (без файлов)	2,5	1/2	5ГБ
5	Discovery.Agent+ SCCM (со сбором файлов)	5	1/2	10ГБ
6	Библиотека ПО (от 50000 правил)	8	1/2	5ГБ
7	Библиотека ПО (от 500000 правил)	10	1/2	10ГБ

Рекомендуемые показатели к ОЗУ при инвентаризации клиентских компьютеров от 10000- 20000:

Сервер	Модули приложения	Память (ГБ)	ЦП Ядра	Хранилище (конфигурации диска)
1	Discovery.Server	16	1/4	30ГБ
2	Discovery.Interact	4	1/4	10ГБ
3	Discovery.Agent	0,5	1/2	2ГБ
4	Discovery.Agent+ SCCM (без файлов)	4,5	1/4	10ГБ
5	Discovery.Agent+ SCCM (со сбором файлов)	12	1/4	15ГБ
6	Библиотека ПО (от 50000 правил)	8	1/4	10ГБ
7	Библиотека ПО (от 500000 правил)	10	1/4	15ГБ

Рекомендуемые показатели к ОЗУ при инвентаризации клиентских компьютеров от 20000- 50000:

Сервер	Модули приложения	Память (ГБ)	ЦП Ядра	Хранилище (конфигурации диска)
1	Discovery.Server	32	1/4	40ГБ
2	Discovery.Interact	8	1/4	15ГБ
3	Discovery.Agent	0,5	1/2	2ГБ

4	Discovery.Agent+ SCCM (без файлов)	10,5	1/4	15ГБ
5	Discovery.Agent+ SCCM (со сбором файлов)	14	1/4	20ГБ
6	Библиотека ПО (от 50000 правил)	8	1/4	15ГБ
7	Библиотека ПО (от 500000 правил)	12	1/4	15ГБ

Рекомендуемые показатели к ОЗУ при инвентаризации клиентских компьютеров от 20000- 70000:

Сервер	Модули приложения	Память (ГБ)	ЦП Ядра	Хранилище (конфигурации диска)
1	Discovery.Server	32	1/8	50ГБ
2	Discovery.Interact	16	1/8	20ГБ
3	Discovery.Agent	1	1/4	4ГБ
4	Discovery.Agent+ SCCM (без файлов)	14,5	1/4	20ГБ
5	Discovery.Agent+ SCCM (со сбором файлов)	18	1/8	30ГБ
6	Библиотека ПО (от 50000 правил)	12	1/8	20ГБ
7	Библиотека ПО (от 500000 правил)	16	1/8	20ГБ

Рекомендуемые показатели к ОЗУ при инвентаризации клиентских компьютеров от 70000- 100000:

Сервер	Модули приложения	Память (ГБ)	ЦП Ядра	Хранилище (конфигурации диска)
1	Discovery.Server	64	1/16	128ГБ
2	Discovery.Interact	32	1/8	30ГБ
3	Discovery.Agent	2	1/4	10ГБ
4	Discovery.Agent+ SCCM (без файлов)	20,5	1/4	30ГБ
5	Discovery.Agent+ SCCM (со сбором файлов)	32	1/16	35ГБ
6	Библиотека ПО (от 50000 правил)	16	1/16	30ГБ
7	Библиотека ПО (от 500000 правил)	32	1/16	30ГБ

При развертывании задач инвентаризации SCCM и сетевой инвентаризации лучше предоставить 16+ GB ОЗУ. Это позволит обработать 30 000+ устройств из базы SCCM.

При развертывании задач инвентаризации SCCM и файлы лучше предоставить +12 GB ОЗУ

**Важно!** Если общее ОЗУ будет заполнена на 85% и более — Это очень сильно замедлит выполнение задачи.

На данный момент сбор данных и логирование сохраняют все результаты.

Поэтому в ходе долгой эксплуатации или же при развертывании задач инвентаризации SCCM и сетевой инвентаризации потребуется больше места (лучше 20+ GB) или же очистка каталогов:

..\Discovery.Reader\{companyGuid}\TasksData

Дата документа: 29.08.2024

Версия системы: 5.5

..\Discovery.Server\{companyGuid}\TasksData

..\Discovery.Agent\Data

## Учетные записи и привилегии

Агент ИТМЕН предъявляет различные требования к учетным записям на разных платформах.

Windows	Linux
Агент инвентаризации ИТМЕН должен работать под системной учетной записью local SYSTEM	Агент инвентаризации ИТМЕН должен работать от имени пользователя root

Так же при инвентаризации вам будет необходим PowerShell от версии 6.x и выше.

Для удалённого сбора данных Hyper-V / VMM должны быть доступны следующие порты:

- WMI - tcp/135,
- WinRM - tcp/5986,
- tcp - udp/49152-65535

Для сбора данных о виртуальных машинах на хостах VMware ESXi необходимо создать учетную запись пользователя с соответствующими правами доступа.

Чтобы получить доступ к данным о виртуальных машинах на хостах ESXi, учетной записи пользователя необходимо предоставить следующие права и роли:

- Права на чтение данных о виртуальных машинах, хостах, кластерах и датацентрах.
- Роль VirtualMachine.GuestOperations в соответствующих объектах. Это позволит выполнять операции на уровне гостевой операционной системы виртуальных машин.
- Роль Datastore.Browse для просмотра данных хранилища данных, используемых виртуальными машинами.

Кроме того, для удаленного доступа к данным на хостах ESXi необходимо настроить доступ по протоколу SSH.

Важно отметить, что доступ к данным на хостах ESXi по протоколу SSH может быть потенциально опасным, поэтому необходимо обеспечить соответствующую безопасность и защиту доступа к учетной записи пользователя.

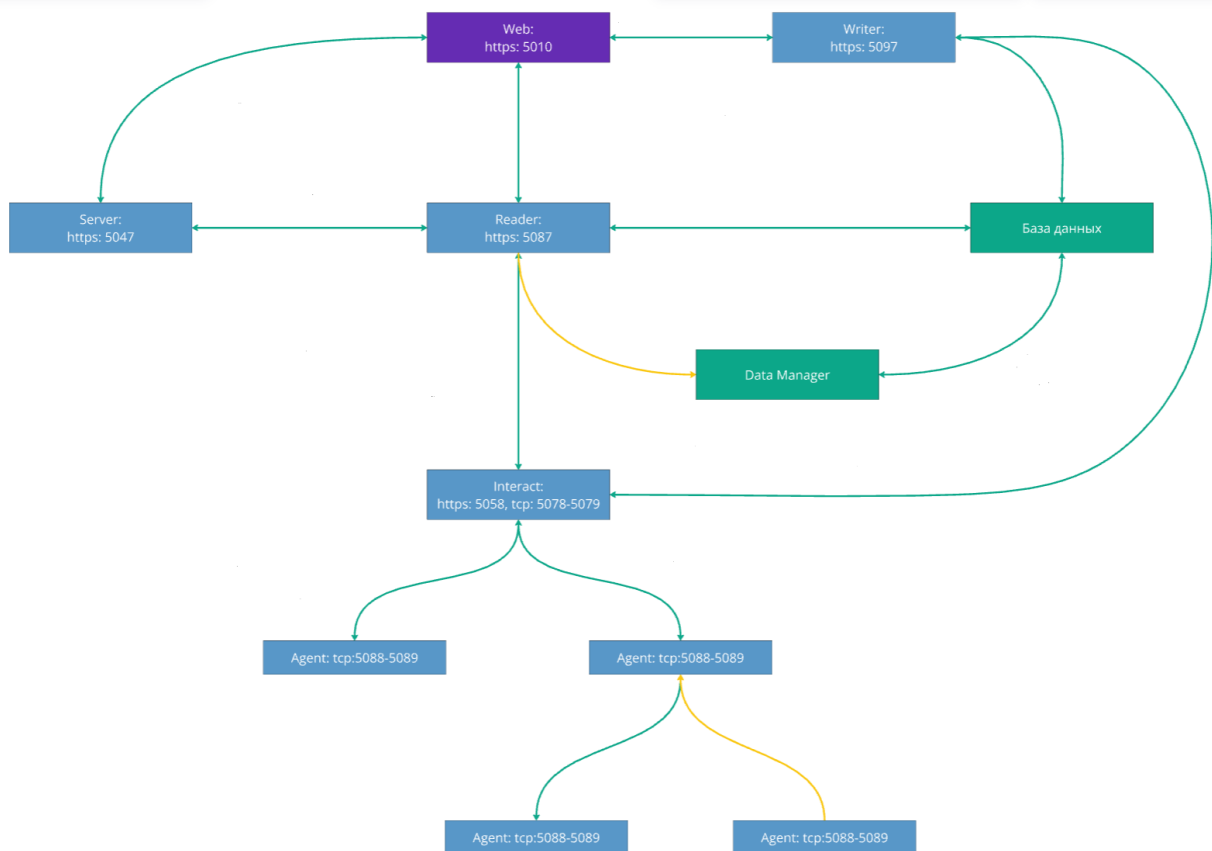
### Требования для SNMP

Возможно, Вы захотите использовать SNMP для сбора данных с таких устройств как принтеры, сетевые коммутаторы, маршрутизаторы или ИБП, которые, как правило, поддерживают SNMP. Система поддерживает сбор данных с SNMP версии 2. Для того чтобы реализовать сбор вам



необходимо настроенное SNMP и также ввод community name. Настраивается сбор данных через задачу Сетевой инвентаризации в Сборе данных.

### Схема работы системы:



### Что необходимо настроить чтобы попробовать демо версию?

Для того, чтобы попробовать демоверсию, вам необходимо выполнить следующие действия: убедитесь, что у вас нет ограничений на передачу данных через порт, который вам передали(например, отключите межсетевой экран или настройте его так, чтобы разрешить передачу данных через этот порт).

Если вы выполните эти действия, то сможете попробовать демоверсию без проблем с передачей данных. Далее рассмотрим пошагово с чего начать.

## 3.1 Первое знакомство с продуктом

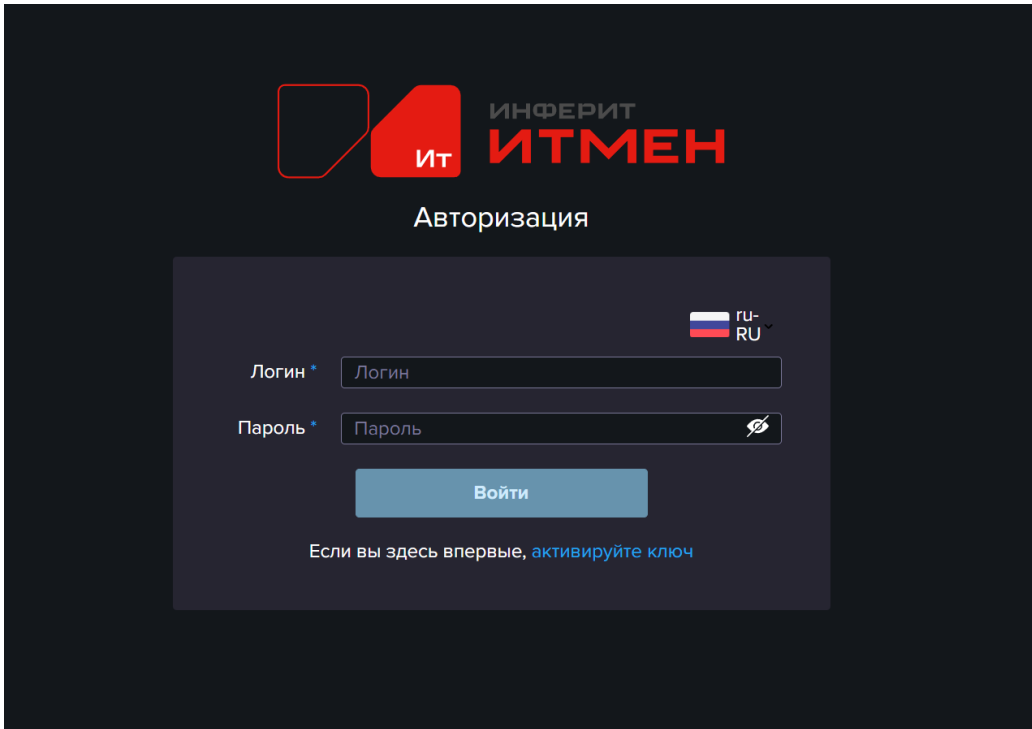
### Шаг 1. Знакомство с системой

Если вы хотите начать работать с системой, то вам необходимо выполнить следующие действия:

1. Откройте браузер и введите адрес, который вам предоставлен в адресную строку.

2. На открывшейся странице введите свой логин и пароль, которые были предоставлены вам для доступа к системе.
3. Нажмите на кнопку "Войти".

После этого вы попадете в систему и сможете начать работу с ней. Обратите внимание, что для входа в систему вам необходимо иметь учетные данные, которые были выданы вам для доступа. Если вы не получили учетные данные или забыли их, обратитесь к администратору системы.



После того, как вы войдете в систему, вы увидите интерфейс, который состоит из следующих разделов:

- Домой - раздел, где отображается краткая информация о системе и ее состоянии.
- Активы - раздел, где можно просмотреть информацию обо всех активах, которые собраны в системе.
- Анализ данных - раздел, где можно проводить анализ данных и получать отчеты.
- Сбор данных - раздел, где можно настроить сбор данных и выполнить инвентаризацию.
- Библиотека - раздел, где можно хранить и управлять документацией и другими ресурсами.
- Администрирование - раздел, где можно управлять настройками системы и пользователями.

## Шаг 2. Настройка агента

Если в системе нет данных, то для начала работы с ней необходимо настроить агента и выполнить сбор данных. Для этого необходимо знать на какую операционную систему будете устанавливать агента, затем определится, где у вас файлы установки. Файлы установки могут быть:

Дата документа: 29.08.2024

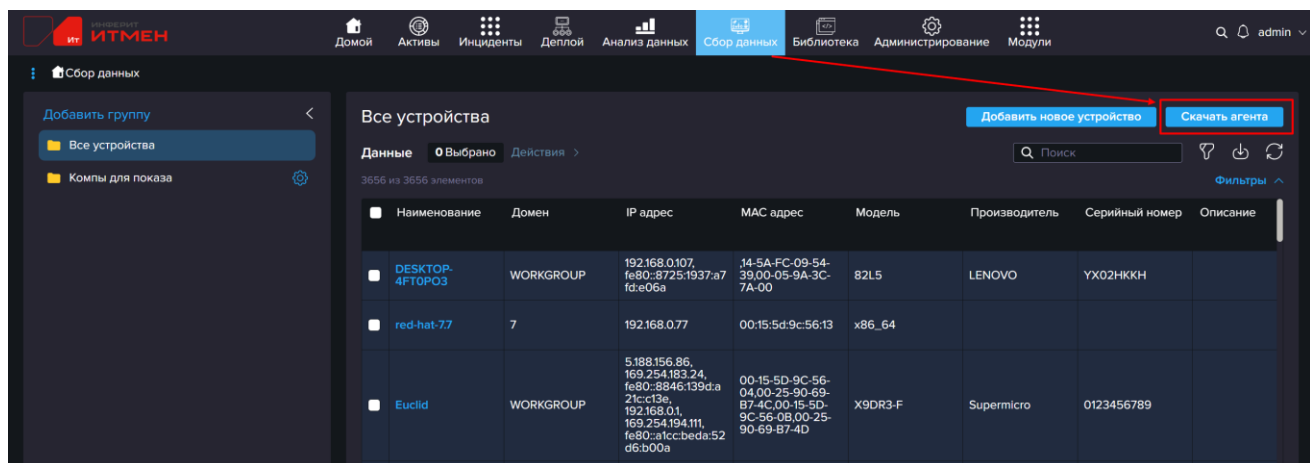
Версия системы: 5.5

1. Переданы вместе с данными при открытии Демо версии, то их можно использовать для установки агента на одну из машин в вашей сети (инструкция по установке ниже).

2. Если у вас нет файлов для установки агента, то вы можете скачать их напрямую из системы, перейдя в раздел "Сбор данных" и нажав на кнопку "Скачать агента" в правом верхнем углу. Затем в открывшемся выпадающем списке нужно выбрать нужный файл установки.

Чтобы скачать агента при втором варианте, вам необходимо выполнить следующие действия:

1. Перейти в раздел "Сбор данных".
2. Найти кнопку "Скачать агента" в правом верхнем углу.
3. Выбрать нужный файл установки из открывшегося выпадающего списка.



После того, как вы скачали агента выбираем один из вариантов установки относительно вашей Операционной системы:

### 1. Установка агента на Windows

Чтобы агент установился и работал корректно необходимо проверить наличие C++ Redistributable. При отсутствии, его необходимо установить.

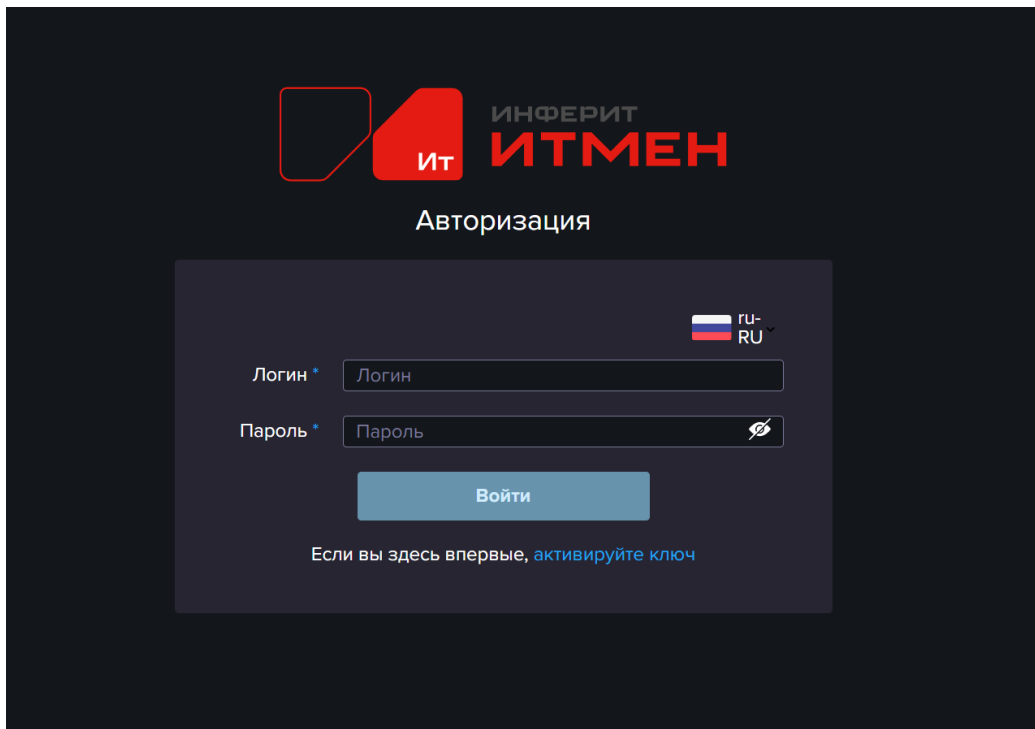


Далее необходимо понять какие функции он будет исполнять, а именно: будет он работать для инвентаризации сети или нет. Виды агентов:

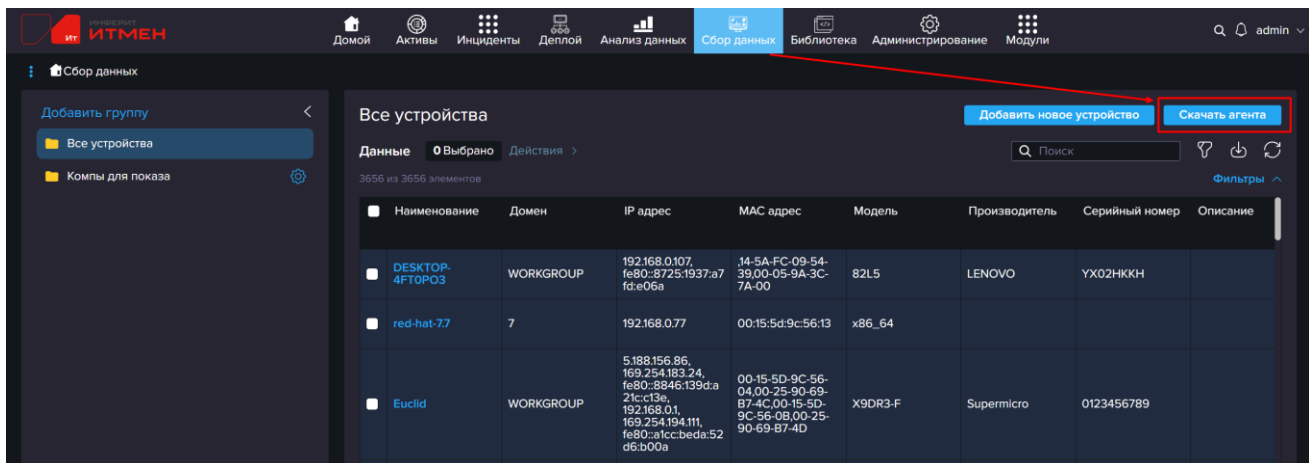
- DiscoveryAgentNative.msi (агент с функцией сетевой инвентаризации)
- DiscoveryAgentLiteNative.msi (агент без функции сетевой авторизации)

После того как определились какой агент устанавливать переходим в систему.

Затем переходим по ссылке, где у вас развернута ваша система. В окне ввода логина и пароля необходимо авторизоваться.



Вводи ваш логин и пароль чтобы зайти в систему. Например: Логин = demo и Пароль = demo. Откроется главная страница. Переходим в Сбор данных и нажимаем кнопку “Скачать агента”.

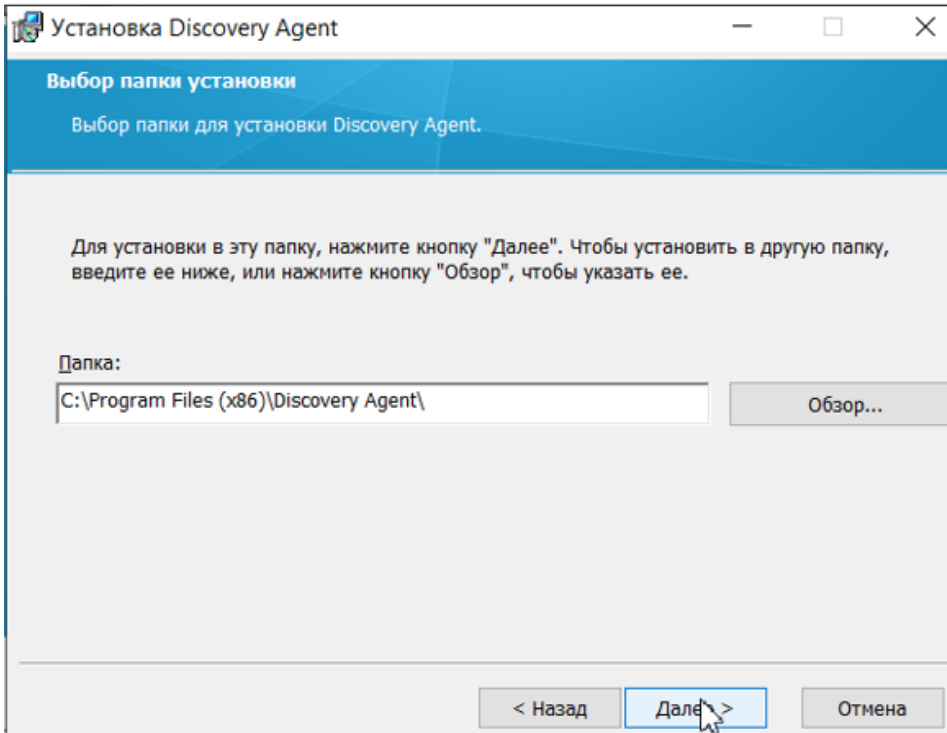


Выбираем скачать msi.

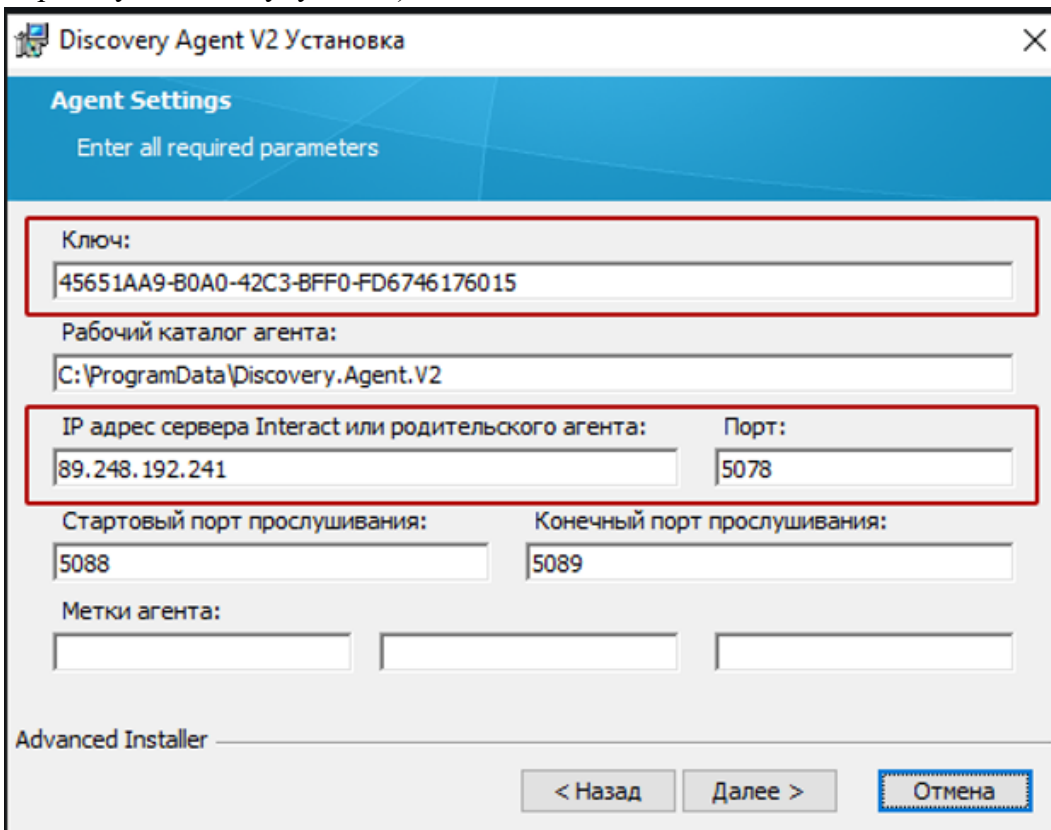
Далее я расскажу, как установить файл с расширением msi:

1. Запускаем файл установки с расширением msi
2. Затем у вас отобразится окно установки, в котором необходимо подтвердить условия пользования, после подтверждения выбираем «Далее»
3. После того как вы нажали «Далее» у вас открылось окно, в котором указан адрес установки (адрес можно оставить по умолчанию, либо изменить на свой). Если все указано верно

нажимаем на кнопку «Далее»

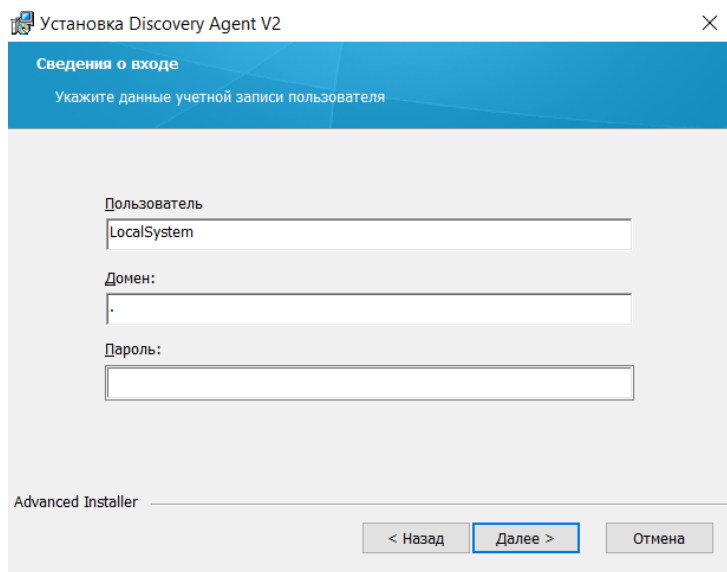


4. На следующем шаге необходимо ввести следующие данные: Company Guid(он был вам предоставлен вместе с данными при открытии Demo), Interact Server Address (указываем ваш адрес), в поле Interact Port ввести значение last port или first port, Стартовый порт прослушивания и Конечный порт прослушивания можно оставить по умолчанию (на скриншоте указан пример портов, у вас они будут свои).



5. После того как все ввели нажимаем «Далее»

6. Далее система попросит указать учетные данные, под которой будет проходить инвентаризация. Если есть возможно, то лучше оставить учетные данные по умолчанию.



Установка Discovery Agent V2

Сведения о входе  
Укажите данные учетной записи пользователя

Пользователь  
LocalSystem

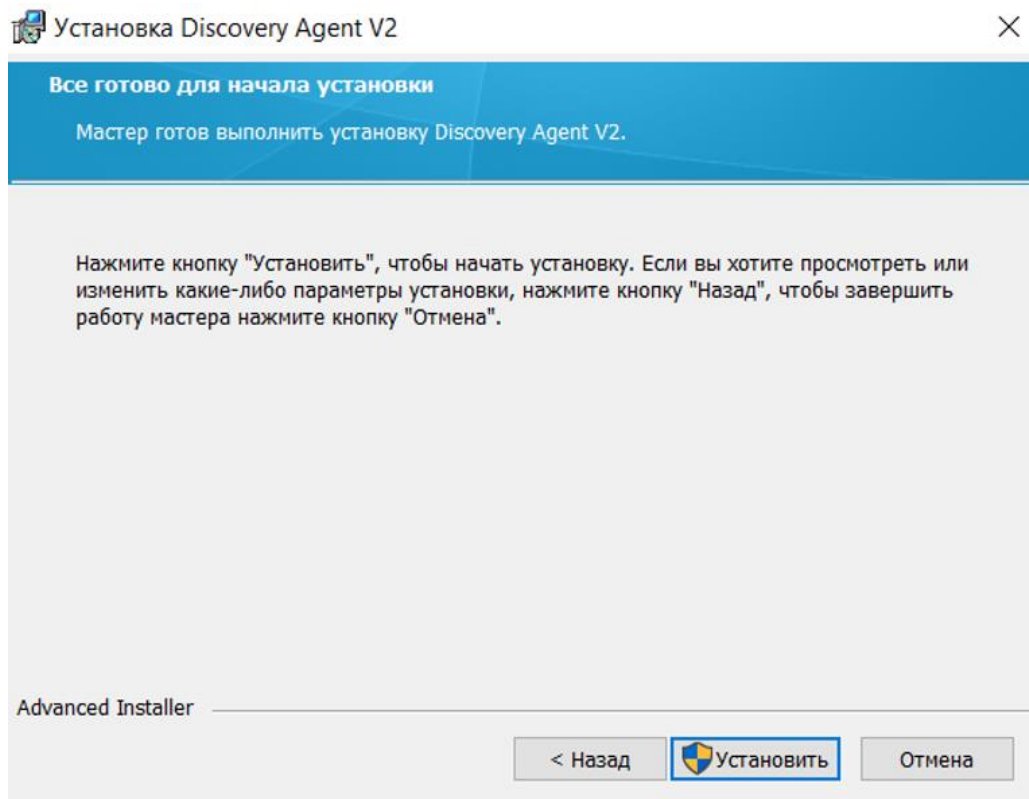
Домен:  
.

Пароль:

Advanced Installer

< Назад **Далее >** Отмена

7. У вас отобразилось окно запуска Установки, в котором нажимаем на кнопку



Установка Discovery Agent V2

Все готово для начала установки  
Мастер готов выполнить установку Discovery Agent V2.

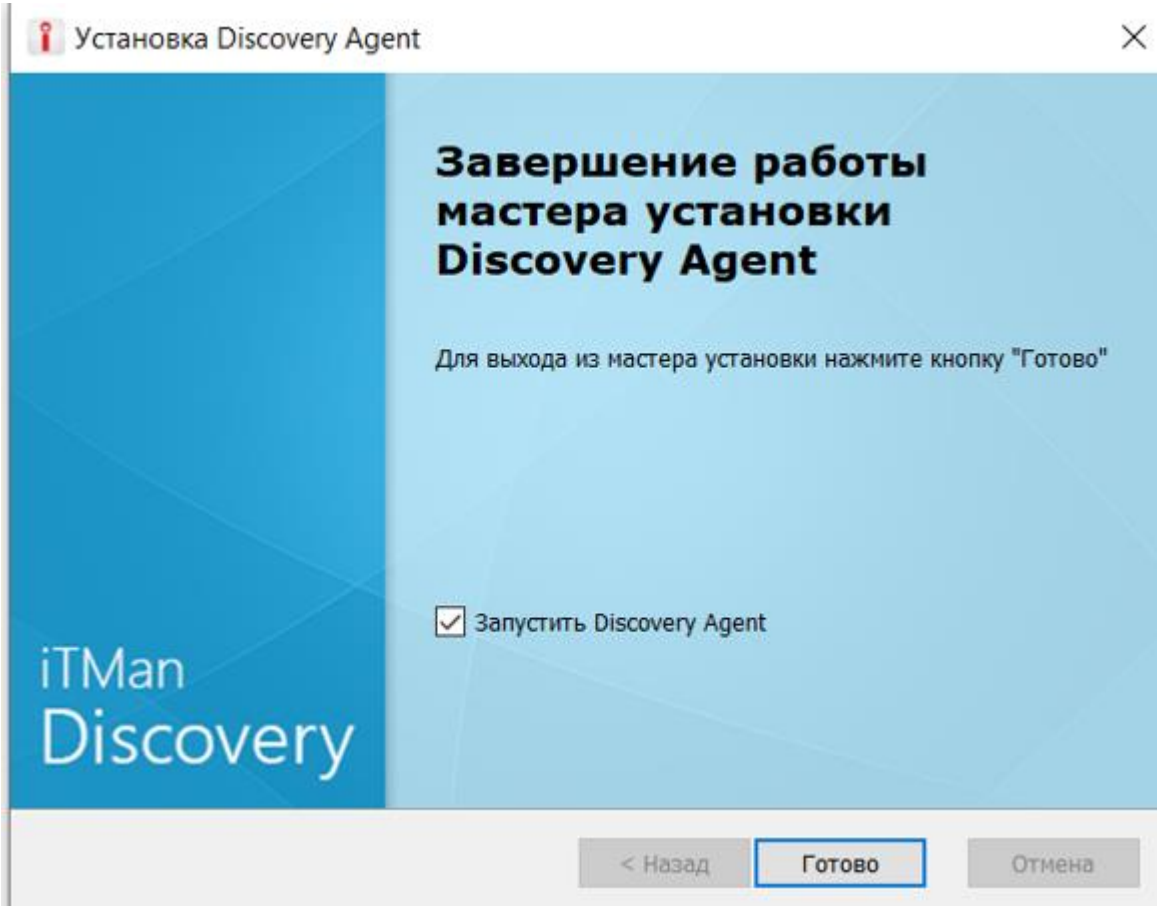
Нажмите кнопку "Установить", чтобы начать установку. Если вы хотите просмотреть или изменить какие-либо параметры установки, нажмите кнопку "Назад", чтобы завершить работу мастера нажмите кнопку "Отмена".

Advanced Installer

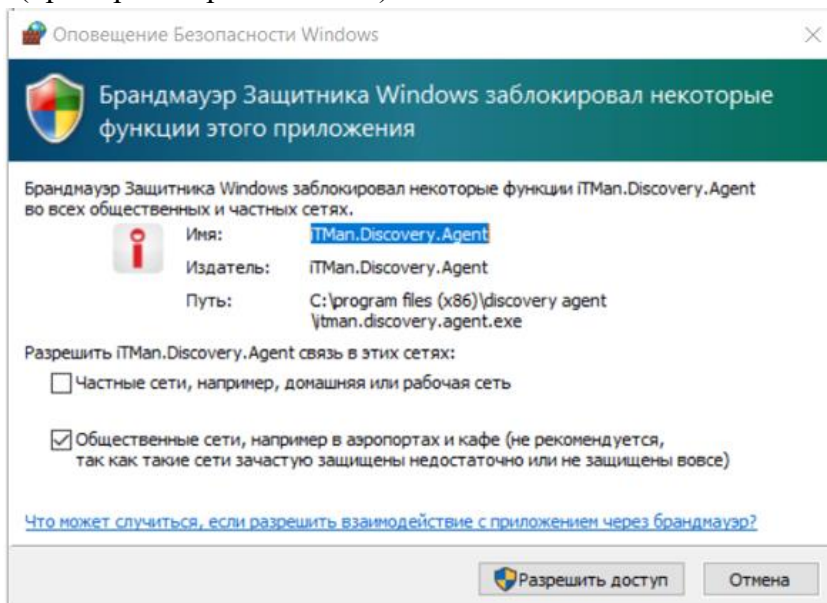
< Назад **Установить** Отмена

«Установить»

8. После установки Агента в окне Завершения установки нажать на кнопку «Готово»



9. После чего у вас появится окно Брандмауэр Защитника, где необходимо дать доступ для приложения ( как говорилось раньше приложение должно иметь права передачи данных по порту которые вам были предоставлены с пакетом учетных данных), чтобы агент смог провести сканирование и передать данные на сервер. Как все настроите нажать на кнопку «Разрешить доступ» (пример на картинке ниже)



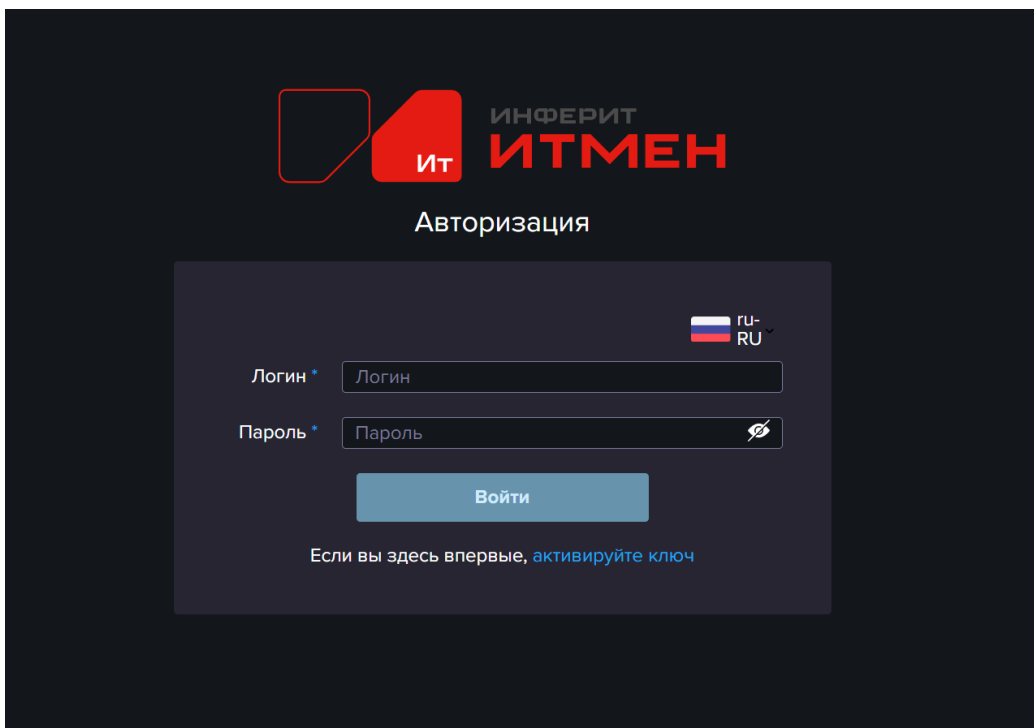
## 2. Установка агента на Linux

Чтобы установить агент необходимо понять какие функции он будет исполнять, а именно будет он работать для инвентаризации сети или нет. Виды агентов:

- DiscoveryAgentNative.deb (агент с функцией сетевой инвентаризации)
- DiscoveryAgentLiteNative.deb (агент без функции сетевой авторизации)
- DiscoveryAgentNative.rpm (агент с функцией сетевой инвентаризации)
- DiscoveryAgentLiteNative.rpm (агент без функции сетевой авторизации)

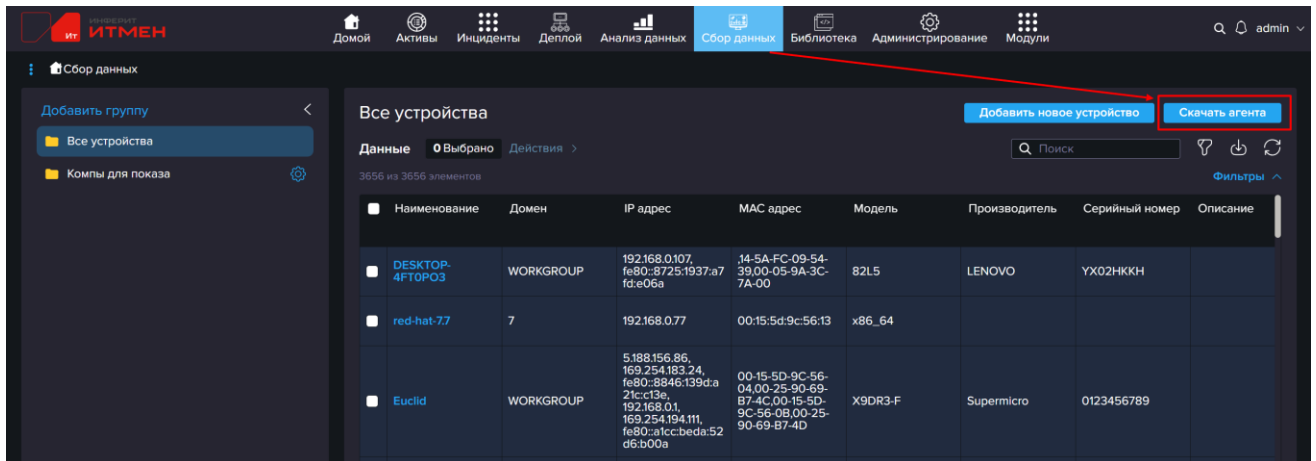
После того как определились какой агент устанавливать переходим в систему.

Затем переходим по ссылке, где у вас развернута ваша система. В окне ввода логина и пароля необходимо авторизоваться.



Вводи ваш логин и пароль чтобы зайти в систему. Например: Логин = demo и Пароль = demo. Откроется главная страница. Переходим в Сбор данных и нажимаем кнопку “Скачать агента”





Выбираем скачать например `***agent.deb`

Чтобы установить Агента на Linux необходимо чтобы у администратора была возможность запустить установку Агента от имени пользователя root.

#### Установка для deb:

```
sudo dpkg -i DiscoveryAgent_LinuxNative_4.19.5.deb && sudo /usr/local/bin/configure-agent.sh --common_directory /var/tmp/discovery-platform/agent/ --company_guid b1751aa9-b0a0-42c3-bff0-fd6746176015 --agent_ip 127.0.0.1 --agent_port 5078 --self_port_is_open false --self_port_first 5088 --self_port_last --agent_tags \"vdi\"
```

#### Установка для rpm:

```
sudo rpm -i /home/ge/rpmbuild/RPMS/x86_64/DiscoveryAgent_LinuxNative_4.18.12.rpm && sudo /usr/local/bin/configure-agent.sh --common_directory /var/tmp/discovery-platform/agent2/ --company_guid b1751aa9-b0a0-42c3-bff0-fd6746176015 --agent_ip 127.0.0.1 --agent_port 5199 --self_port_is_open false --self_port_first 5555 --self_port_last 6666 --agent_tags \"vdi\"
```

Ключи для агента:

- d | `--common_directory` : Путь к каталогу с временными файлами агента.
- c | `--company_guid` : Гуид компании.
- a | `--agent_ip` : ip адрес родительского элемента (agent или interact).
- p | `--agent_port` : Порт родительского элемента (agent или interact).
- o | `--self_port_is_open` : Открывать ли порты на агенте.(возможные значения true/false)
- f | `--self_port_first` : Начальный порт агента.
- l | `--self_port_last` : Конечный порт агента.
- t | `--agent_tags` : Тэги для агента в виде строки (двойные кавычки необходимо экранировать. Например, `\"tag1\", \"vdi\"`).

Дата документа: 29.08.2024

Версия системы: 5.5

`-h | --help` : Показать список доступных параметров и их значения по умолчанию.

Можно использовать как полные имена ключей, так и их длинные параметры. Например `-c` и `--company_guid` равноценные ключи. Можно указывать только нужные параметры, которые необходимо изменить все остальные будут установлены значениями по умолчанию.

Варианты что могло пойти не так:

1. Необходимо проверить создались ли данные в папке, которую вы указали в строчке `CommonDirectory`. Если данные не создались, то возможно у вас нет прав для записи в вашу папку
2. Если данные создались необходимо проверить запустился ли ваш Агент через команду `$ htop`
3. Если данные не создались, а агент запустился. То необходимо проверить корректно ли вы указали адрес в строках `ServerAddress` и `InteractServerAddress`

### 3.2.1 Раздел Администрирование.

Для работы с системой вам потребуется настроить следующие шаги, в зависимости от ваших потребностей:

1. Определить, где будет храниться ваши данные сервера и инвентаризации.
2. Установить БД Postgre — это необходимо для хранения данных.
3. Создать в БД пользователя с правами "Суперадмин", логин и пароль потребуется для ввода в системе
4. Далее этого пользователя добавить в систему ([описание прикрепления пользователя БД к системе](#))

После того как все агенты будут установлены, необходимо ввести персональные данные в разделе "Администрирование".

С чего же начать?

Начать необходимо с ознакомления раздела "Администрирование"

Раздел Администрирование состоит из:

- Справочников
- Отчетности
- Настройки

Подраздел Настройки - необходим чтобы настроить сохранение и отображение данных в системе.

На страницы “Настройки БД” необходимо ввести данные вашей базы, где будет храниться информация. Если база данных не будет подключена система не будет отображать данные по инвентаризации так как ей некуда будет их сохранять.

Учетные данные необходимо указывать с правами администратора БД

### 3.2.1 Настройки

Раздел настройки состоит из трех блоков:

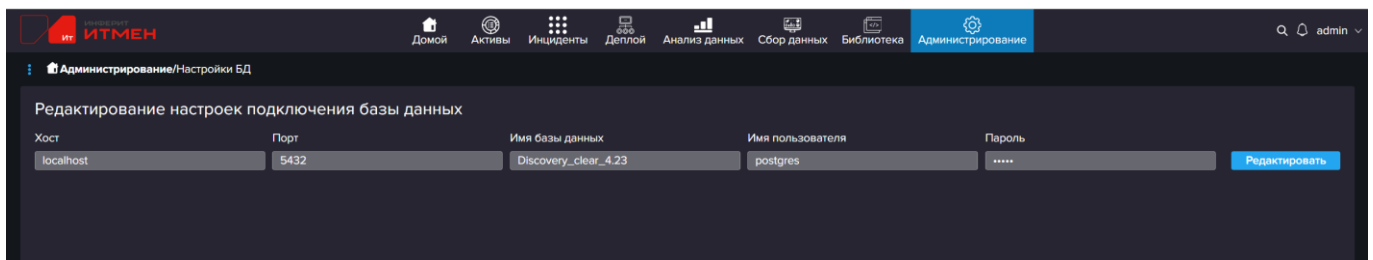
- Настройки БД – в этом справочники хранятся настройки подключения к Базе данных, где хранятся данные системы и инвентаризации
- Экспорт данных – настройки экспорта изменения данных по средствам задач
- Общие настройки – раздел, где настраиваются парольные политики, подключение к системе с помощью Active Directory и доп. настройки
- Настройки логирования – на этой странице можно выбрать какие действия будут записываться в логи.
- Ключ лицензии – страница загрузки ключа лицензии.

#### 3.2.1.1 Настройки БД

Для изменения настроек БД необходимо перейти в раздел Администрирования – Настройки БД.

Для сохранения данных и отображения их в активах, необходимо ввести данные PostgreSQL:

- Хост
- Порт
- Имя базы данных
- Имя пользователя - у пользователя должны быть права суперадмина
- Пароль



После того как ввели свои данные необходимо выйти из системы и зайти заново.

Чтобы проверить что все установилось корректно и база развернулась, можно зайти в раздел Администрирования – Справочники – Типы устройств. После правильной настройки у вас появятся предустановленные справочники.

#### Полезная информация:

Установка PostgreSQL на linux:

```
$ sudo apt update
```

```
$ sudo apt-get install postgresql-12
```

Запускаем сервис:

```
$ sudo systemctl start postgresql.service
```

Проверка статуса сервиса:

```
$ sudo systemctl status postgresql.service
```

При установке PostgreSQL по умолчанию создается пользователь postgres, но можно и создать своего

```
$ sudo -u postgres createuser -s -i -d -r -l -w superadmin
```

```
$ sudo -u postgres psql -c "ALTER ROLE <> WITH PASSWORD '<>';"
```

```
sudo -u postgres createuser
```

### 3.2.1.2 Общие настройки

В каждой компании есть свои требования по созданию учетных данных и паролей. Если вам необходимо указать свою политику, то в системе предоставлено два уровня настройки:

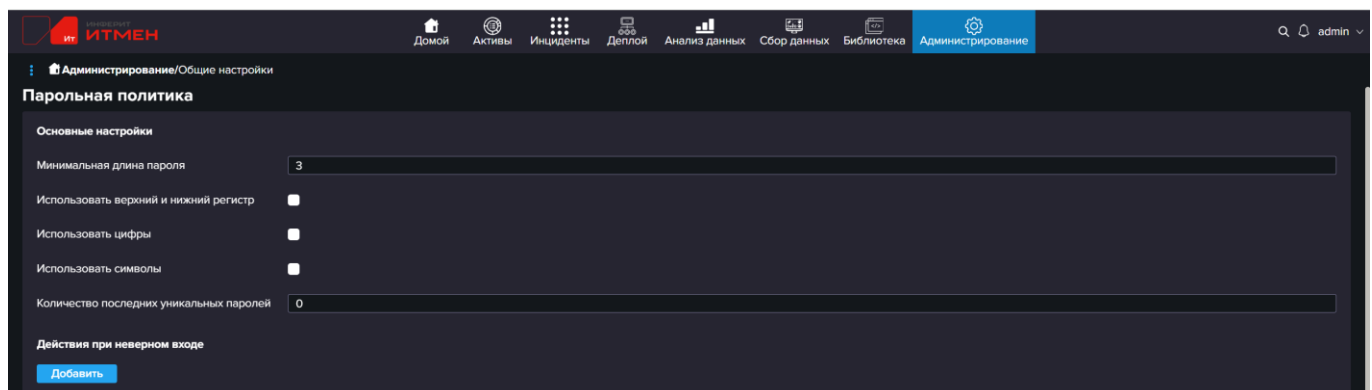
- На всю систему
- На определенную группу пользователей

**Рассмотрим настройку парольной политики на всю систему сразу.**

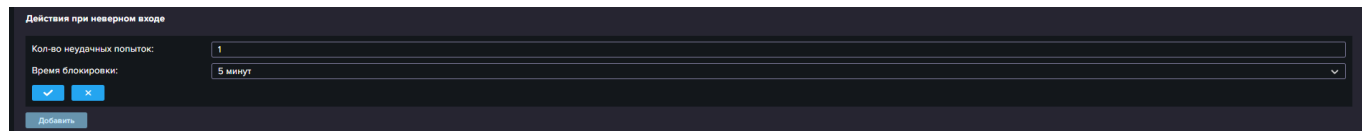
Для это нам необходимо перейти в раздел Администрирование – Настройки – Общие настройки

В этом подразделе мы настраиваем основные настройки, касающиеся пароля, а именно:

- Минимальная длина пароля
- Использовать верхний и нижний регистр
- Использовать цифры
- Использовать символы
- Количество последних уникальных паролей



Так же вы можете указать поведение системы при вводе неверного пароля. Для этого в блоке «Действия при неверном входе» нажимаем кнопку «Добавить». После этого действия у вас откроется блок настройки, в котором вы введете «Количество неудачных попыток» и «время блокировки». Для сохранения действий при неверном входе не забываем нажать на кнопку с изображением Галочки.



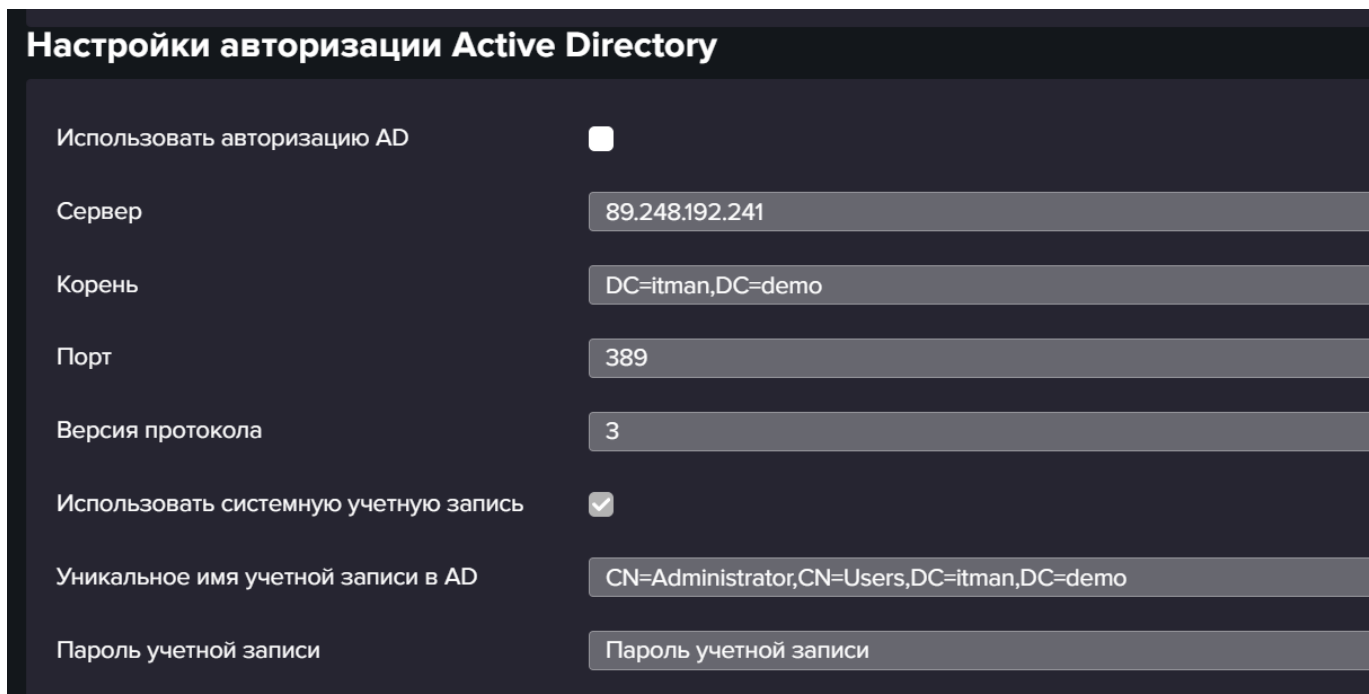
Затем, когда все данные будут введены в правом нижнем углу нажимаем «Сохранить».

### Настройки авторизации через Active Directory.

Для настройки входа через Active Directory вам потребуются следующие данные:

- Имя сервера
- Корень
- Порт
- Версия протокола
- Уникальное имя учетной записи в AD (учетная запись должна быть администратора, чтобы система смогла подключиться ко всем учетным записям)
- Пароль учетной записи

Далее заполняем нашу форму в Общих настройках (пример заполнения указан на скриншоте):



После того как данные будут введены нажимаем кнопку «Сохранить» и пробуем авторизоваться под любой учетной записью из AD.

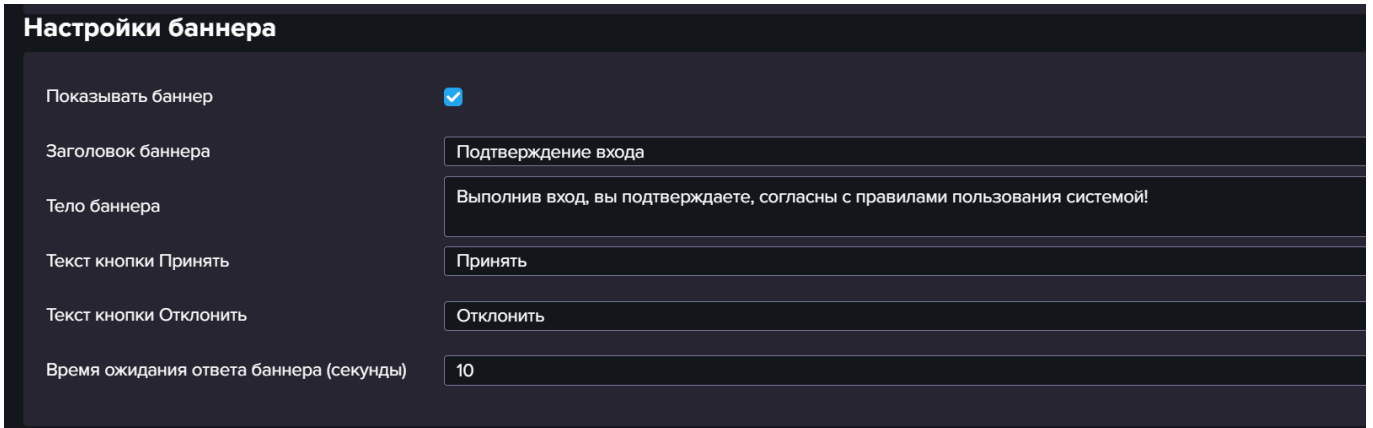
### Настройки Баннера.

В системе так же можно настроить подтверждающий баннер с соглашением.

Для этого вам необходимо в общих настройках ввести свой текст пользовательского соглашения.

Чтобы ввести данные включаем галочку «Показывать баннер», затем заполняем:

- Заголовок баннера
- Тело баннера – в этом поле указываем основной текст
- Текст кнопки «Принять» - можете указать любой текст кнопки
- Текст кнопки «Отклонить» - можете указать любой текст кнопки
- Время ожидания ответа баннера (секунды)

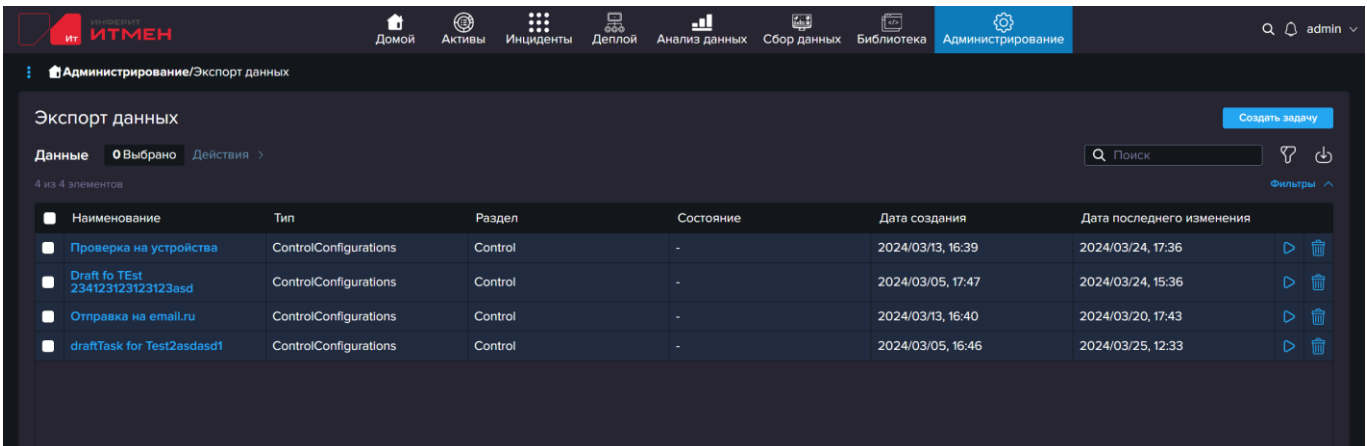


После всех настроек нажимаем кнопку «Сохранить».

### 3.2.1.3 Экспорт данных

На странице экспорта данных можно настроить задачи сигнализации. Это необходимо для того, чтобы вам приходили данные, которые были изменены при проведении новой инвентаризации. Например, вы хотите отслеживать изменение объема Оперативной памяти.

Для этого необходимо нажать на кнопку "Создать задачу"



Наименование	Тип	Раздел	Состояние	Дата создания	Дата последнего изменения
Проверка на устройства	ControlConfigurations	Control	-	2024/03/13, 16:39	2024/03/24, 17:36
Draft fo TEst 234123123123123asd	ControlConfigurations	Control	-	2024/03/05, 17:47	2024/03/24, 15:36
Отправка на email.ru	ControlConfigurations	Control	-	2024/03/13, 16:40	2024/03/20, 17:43
draftTask for Test2asdasd1	ControlConfigurations	Control	-	2024/03/05, 16:46	2024/03/25, 12:33

Далее в открывшемся окне заполняем данные для Экспорта:

1. Вводим «Наименование задачи»
2. Далее выбираем тип отправки результата

Дата документа: 29.08.2024

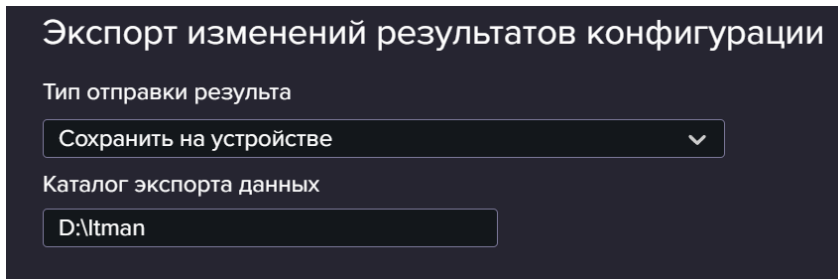
Версия системы: 5.5

- Сохранить на устройстве
- Отправить по REST API
- Отправить на почту

3. Далее заполняем данные в соответствии с вашими требованиями в каком виде будут экспортироваться данные.

- Сохранить на устройстве.

При выборе этого значения необходимо указать путь куда будет сохранен отчет. Данные сохраняются на устройстве, где установлена система ИТМЕН.



Экспорт изменений результатов конфигурации

Тип отправки результата

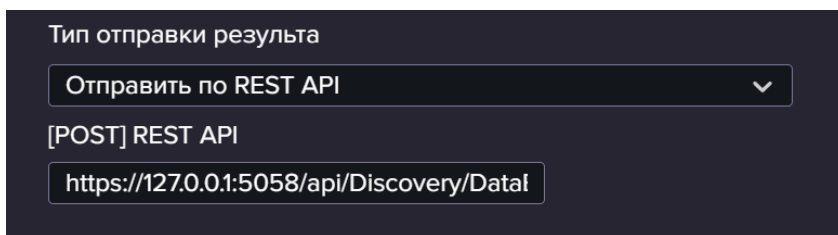
Сохранить на устройстве

Каталог экспорта данных

D:\ltman

- Отправить по REST API.

Указывает POST запрос для сохранения



Тип отправки результата

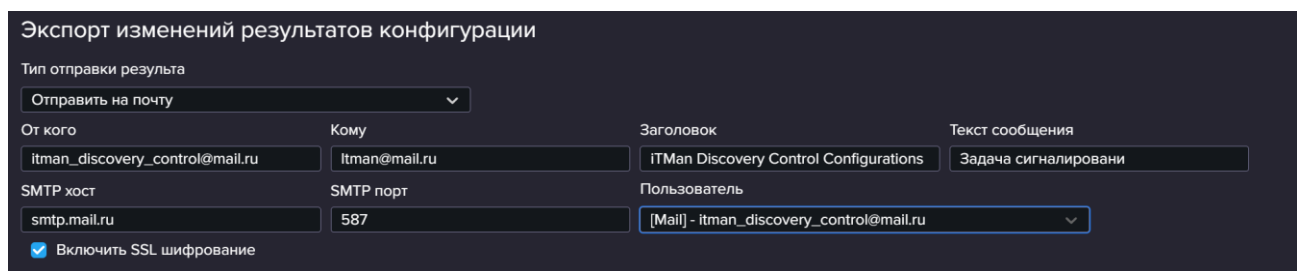
Отправить по REST API

[POST] REST API

https://127.0.0.1:5058/api/Discovery/Data1

- Отправить на почту

При выборе этого значения необходимо указать почту от кого будут отправляться данные и кому, а также указать учетные данные от почты, с которой будут отправлены письма.



Экспорт изменений результатов конфигурации

Тип отправки результата

Отправить на почту



От кого	Кому	Заголовок	Текст сообщения
itman_discovery_control@mail.ru	ltman@mail.ru	ITMan Discovery Control Configurations	Задача сигнализировани
SMTP хост	SMTP порт	Пользователь	
smtp.mail.ru	587	[Mail] - itman_discovery_control@mail.ru	


Включить SSL шифрование

4. Затем выбираем интервал как часто будут отправляется данные.

5. После выбрать Задачи-Триггеры. Это задачи инвентаризации и соответственно на сравнении данных из этих задач система вам будет присылать уведомления.

**Задачи-триггеры**  
 Выбранные задачи инвентаризации после завершения своей работы будут также запускать данную задачу отслеживания изменений конфигураций помимо ее выставленного расписания выполнения

Данные   

15 из 15 элементов Фильтры 

<input type="checkbox"/>	Наименование	Тип	Раздел	Состояние	Дата создания	Дата последнего изменения
<input type="checkbox"/>	Все задачи					
<input type="checkbox"/>	RTBase	LocalSensors	Инвентаризация	-	2024/01/19, 16:58	2024/03/22, 16:21
<input type="checkbox"/>	Локальный сбор	LocalSensors	Инвентаризация	-	2023/12/26, 17:07	2024/03/22, 16:21
<input type="checkbox"/>	SoftwareRedOS	LocalSensors	Инвентаризация	-	2024/02/13, 16:25	2024/03/22, 16:22
<input type="checkbox"/>	erwtrt	LocalSensors	Инвентаризация	-	2024/02/27, 17:06	2024/03/22, 16:22
<input type="checkbox"/>	Сетевая	NetworkScan	Инвентаризация	-	2023/12/26, 15:13	2024/03/22, 16:22
<input type="checkbox"/>	SNMP-office	NetworkScan	Инвентаризация	-	2024/01/23, 13:36	2024/03/22, 16:22
<input type="checkbox"/>	alt-time	LocalSensors	Инвентаризация	-	2024/02/06, 17:23	2024/03/22, 16:22
<input type="checkbox"/>	fgdsgds	ActiveDirectory	Инвентаризация	-	2024/01/18, 17:30	2024/03/22, 16:22

6. Как все данные будут выбраны нажимаем кнопку «Далее»
7. Затем на следующем шаге выбираем, например, Оперативную память- Объем

Создать задачу ✕

1 — 2

**Контролируемые объекты конфигурации**  
 Выберите свойства в объектах по которым необходимо отслеживать изменения

> Процессоры

▼ Оперативная память Выбрано: 1

- Название платы
- Наименование
- Наименование
- Объем
- Производитель
- Серийный номер
- Тип памяти
- Форм-фактор
- Разъем
- Позиция
- Скорость
- Ширина данных

> Материнские платы

> BIOS

> Видеокарты

▼ Дисковые накопители Выбрано: 1

Наименование

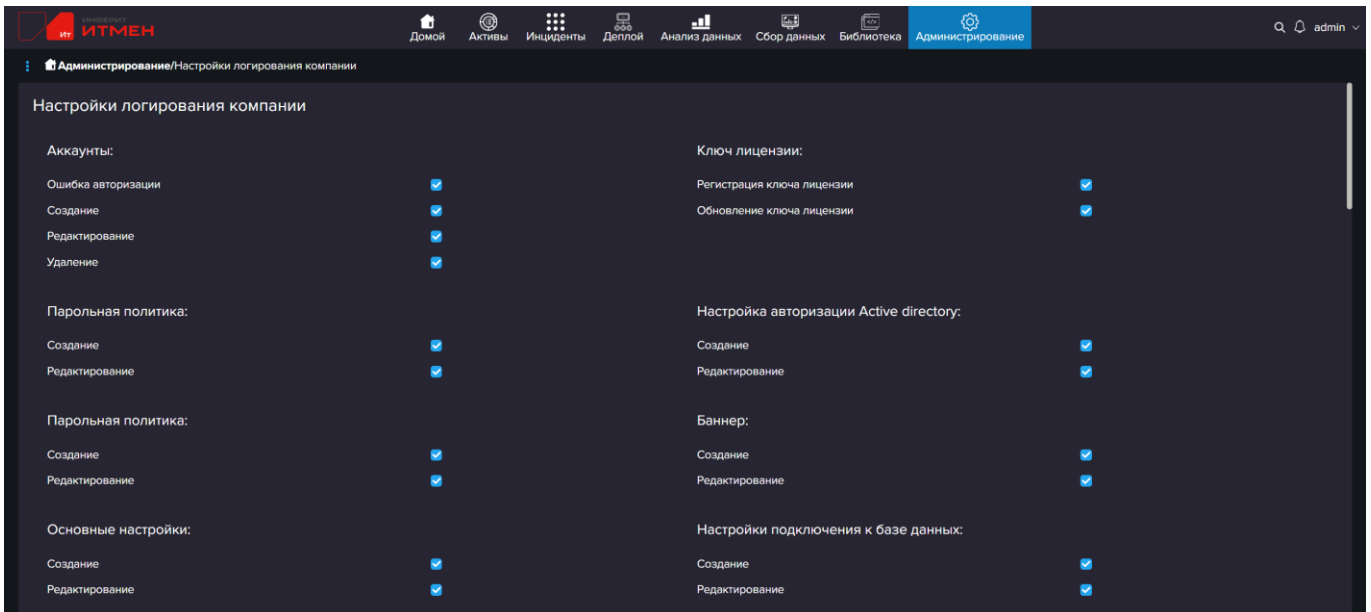
8. После нажимаем кнопку «Сохранить».

Задача сохранена и в случае изменения объема оперативной памяти вам придет отчет с данными на каком устройстве произошло изменение.

### 3.2.1.4 Настройки логирования

В этом разделе можно выбирать какие действия будут отображаться в логах





Где же можно посмотреть логи? Для этого вам необходимо вспомнить что вы указывали в конфигурационных файлах при установке системы, интеракта и агента. По умолчанию они сохраняются:

Для Windows:

- Логи Ридера и Writer в каталоге C:\ProgramData\Discovery.Reader
- Логи Сервера в каталоге C:\ProgramData\Discovery.Server
- Логи Интеракта в каталоге C:\ProgramData\discovery-platform\interact
- Логи Агента в каталоге C:\ProgramData\Discovery.Agent.V2 или C:\ProgramData\Discovery.Agent.Light.V2 в зависимости от типа агента.

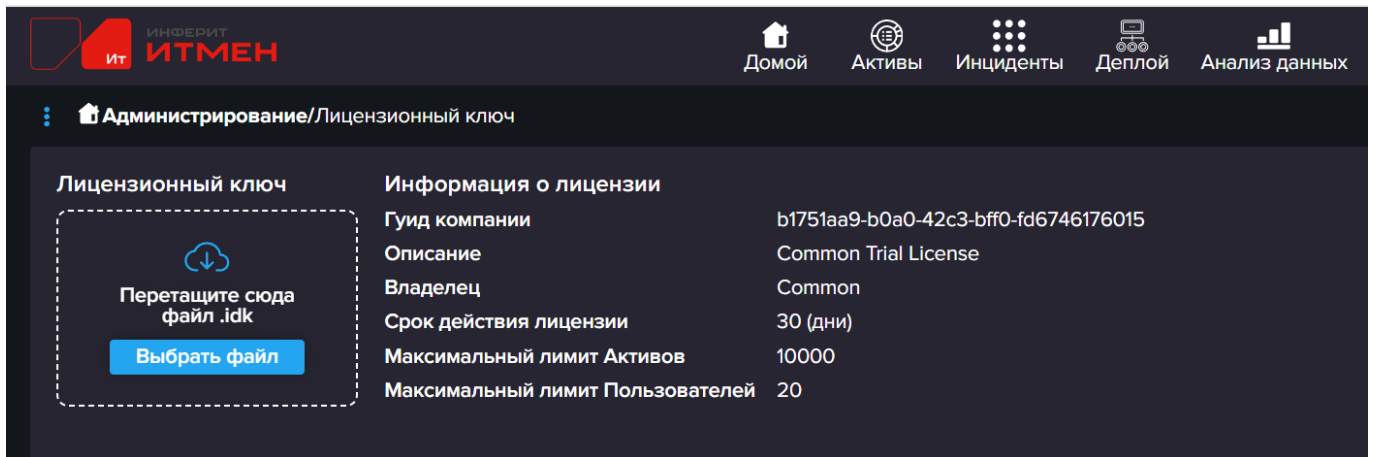
Для Linux если вы не помните куда указывали путь сохранения логов их всегда можно будет посмотреть в следующих файлах (каталог может отличаться в зависимости от места установки):

- Данные Ридера в каталоге /opt/Discovery.Reader/Settings/ReaderConfig.json
- Данные Сервера в каталоге /opt/Discovery.Server/Settings/ServerConfig.json
- Данные Writer в каталоге /opt/Discovery.Writer/Settings/WriterConfig.json
- Логи Интеракта в каталог var/tmp/discovery-platform/interact или /ect/discovery-platform/interact
- Логи Агента в каталог var/tmp/discovery-platform/agent или /ect/discovery-platform/agent

### 3.2.1.4 Ключи лицензии

На этой странице расположена информация о вашей компании:

- Ключ лицензии
- Описание
- Количество допустимых активов
- Срок действия лицензии
- Блок продления лицензии



### 3.2.2 Справочники

Состоит из следующих справочников:

- Группы устройств
- Группы пользователей
- Пользователи
- Тип устройств
- Поля устройств
- Статусы устройств
- IP размещение
- Расположения устройств
- Учетные данные
- SSH ключи

Выделим справочник Пользователи в нем отображается список наших пользователей, которые могут пользоваться системой.

Создать пользователя имеет права только пользователь с ролью Administrator с помощью кнопки “Создать пользователя”.

Перейдем к следующим справочникам в разделе Администрирование. Они отображаются как поля в ИТ активах:

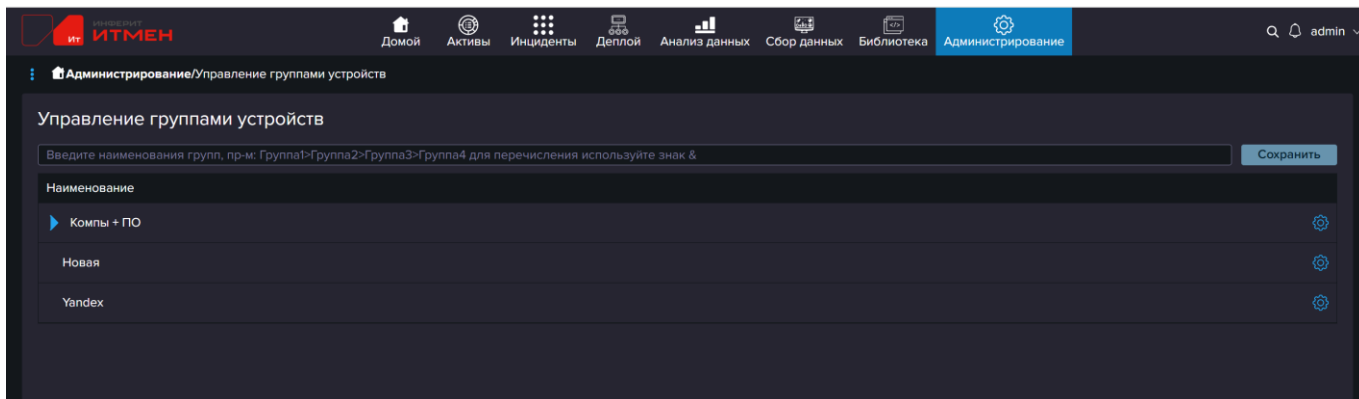
- Группы устройств - справочник в котором вы добавляете свои группы устройств.
- Группы пользователей - если у вас есть деление пользователей по группам или уровням доступа, можно добавить эти значения в этот справочник.
- Пользователи – в этом справочнике добавляются пользователи, которые будут иметь доступ в систему ИТМЭН.
- Типы устройств - в этом справочнике вы можете настраивать какие поля будут отображаться в «Карточке устройства»
- Статусы устройств – справочник, в котором указан статус устройства, он заполняется самостоятельно, поэтому можно использовать справочник по своему назначению. Например: указывать статус: «На руках» или «В офисе».

- Поля устройств - если вам необходимо добавить дополнительные поля, которые вам необходимы, но их нет в системе, то можно воспользоваться этим справочником.
- IP размещение – технический справочник, по которому можно сделать группировку по IP адресам в системе.
- Расположения устройств - этот справочник предназначен для удобства отслеживания, где было выдано устройство или за каким подразделением закреплено.
- Учетные данные – Это справочник, в котором расположены данные от устройств, на которых будет проходить сетевая инвентаризация.
- SSH ключи – Это справочник, в котором расположены учетные SSH ключи от устройств на которых будет проходить сетевая инвентаризация.

### 3.2.2.1 Группы устройств

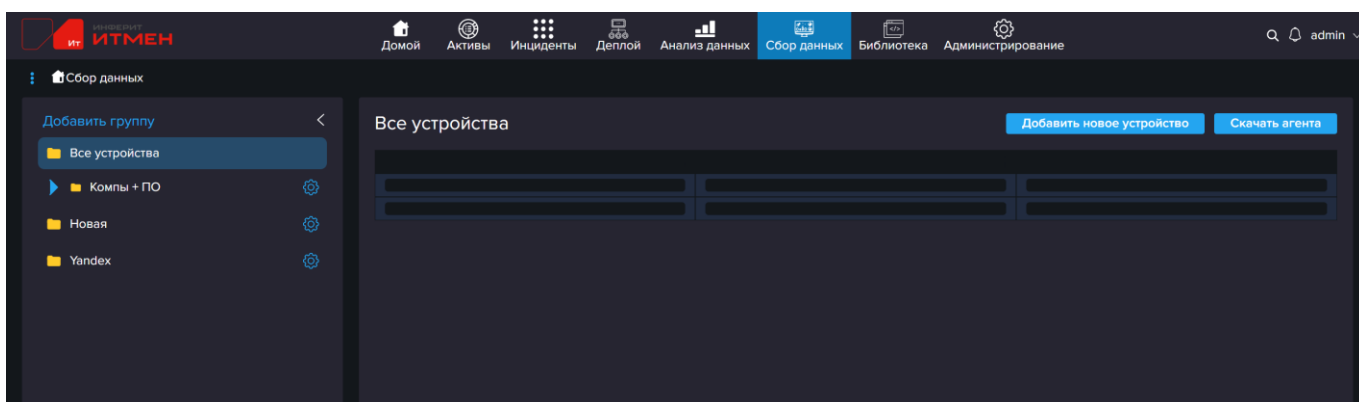
Это справочник в котором вы добавляете свои группы устройств.

Для добавления вам необходимо ввести название группы и нажать на кнопку "Добавить"



Так же эту группу можно отредактировать или удалить.

Далее эти группы будут отображаться в разделе Сбор данных- Все устройства в виде бокового меню.



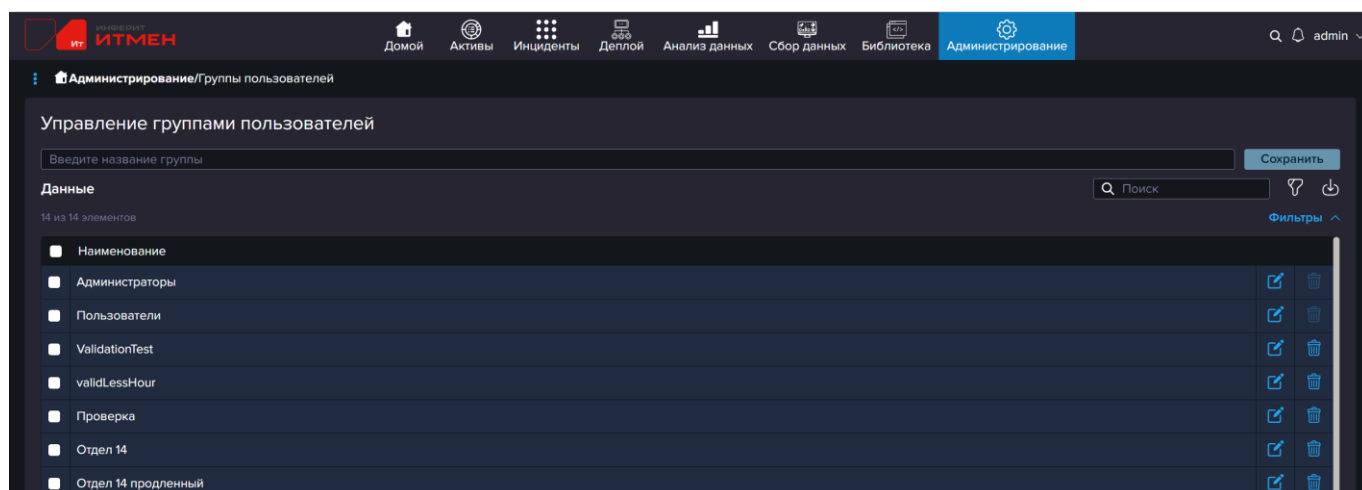
### 3.2.2.2 Группы пользователей

Раздел "Группы пользователей" необходим для разделения пользователей, а также настройки Парольной политики для отдельной группы.

Дата документа: 29.08.2024

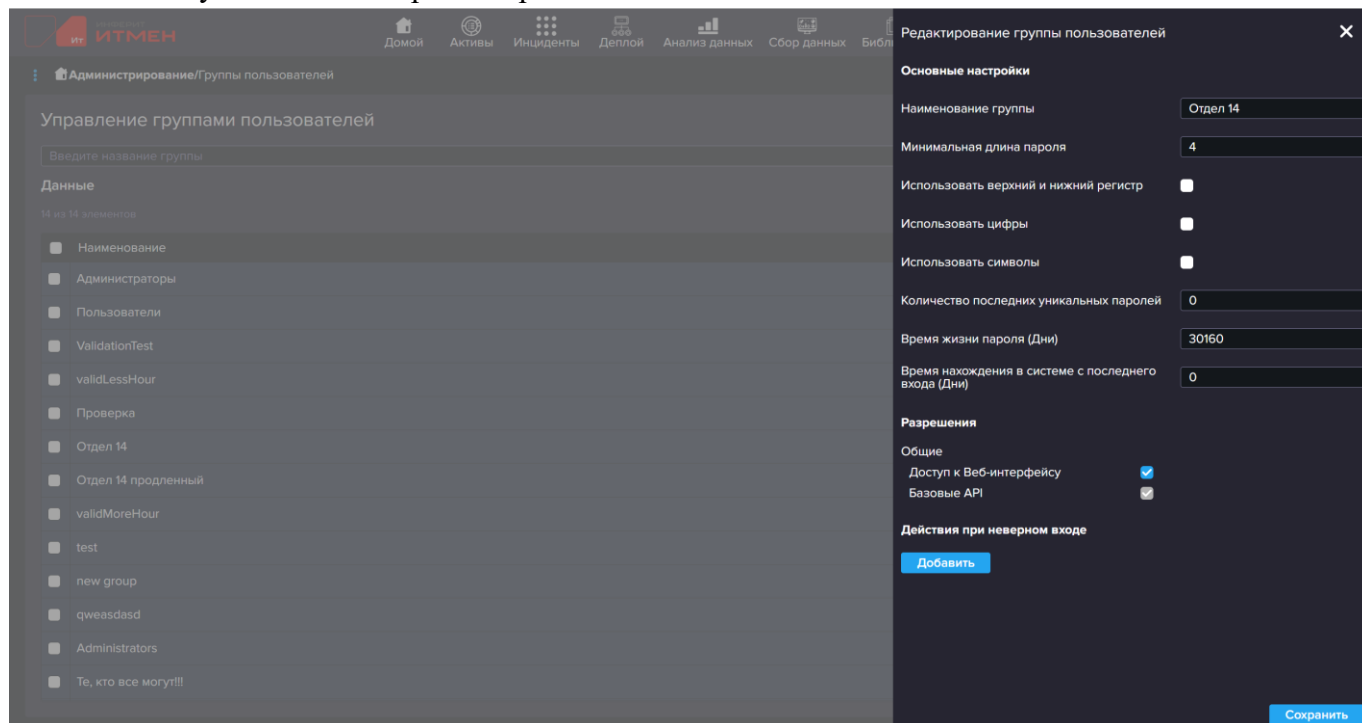
Версия системы: 5.5

Для настройки парольных политик на отдельные группы необходимо перейти в раздел Администрирование – Справочники – Группы пользователей.



По умолчанию в системе уже есть две группы пользователей это Администраторы и Пользователи их редактирование доступно только Администратору из группы Администраторы, поэтому в целях безопасности эти две группы нельзя удалить и нельзя редактировать, и они подчиняются только общей парольной политики. Но если хотите всегда можете создать дополнительно свои группы и прописать под них свои дополнительные настройки.

Для создания своей группы пользователей в верхнее поле вводим наименование группы и нажимаем «Сохранить». После группа сохранится и отобразится в общей таблице, где необходимо будет нажать на редактирование.



В открывшейся панели можем настроить:

- Минимальную длину пароля
- Использовать верхний и нижний регистр

- Использовать цифры
- Использовать символы
- Количество последних уникальных паролей
- Время жизни пароля (Дни)
- Время нахождения в системе с последнего входа (Дни)

**Важно!** Если в подблоке Разрешения вы указали «Базовые API», но не включили доступ к Веб интерфейсу, то пользователи из этой группы не смогут зайти в веб интерфейс.

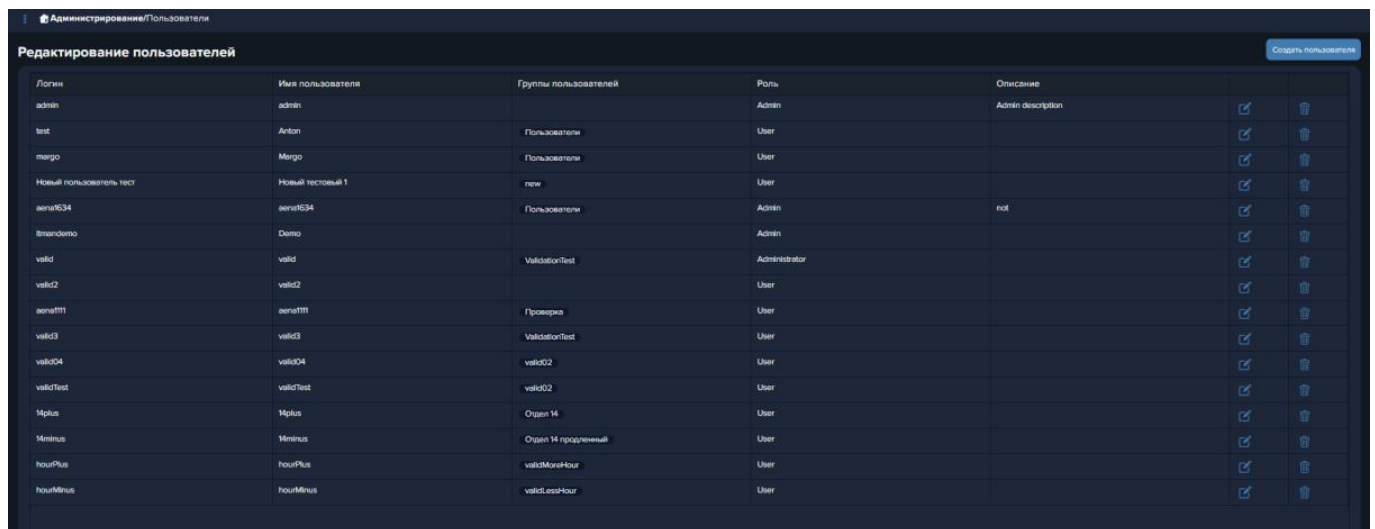
В этом блоке так же можно настроить «Действия при неверном входе» по аналогии, как и настройка для всей компании в целом.

После того как ввели все настройки не забываем нажать кнопку «Сохранить»

### 3.2.2.3 Пользователи

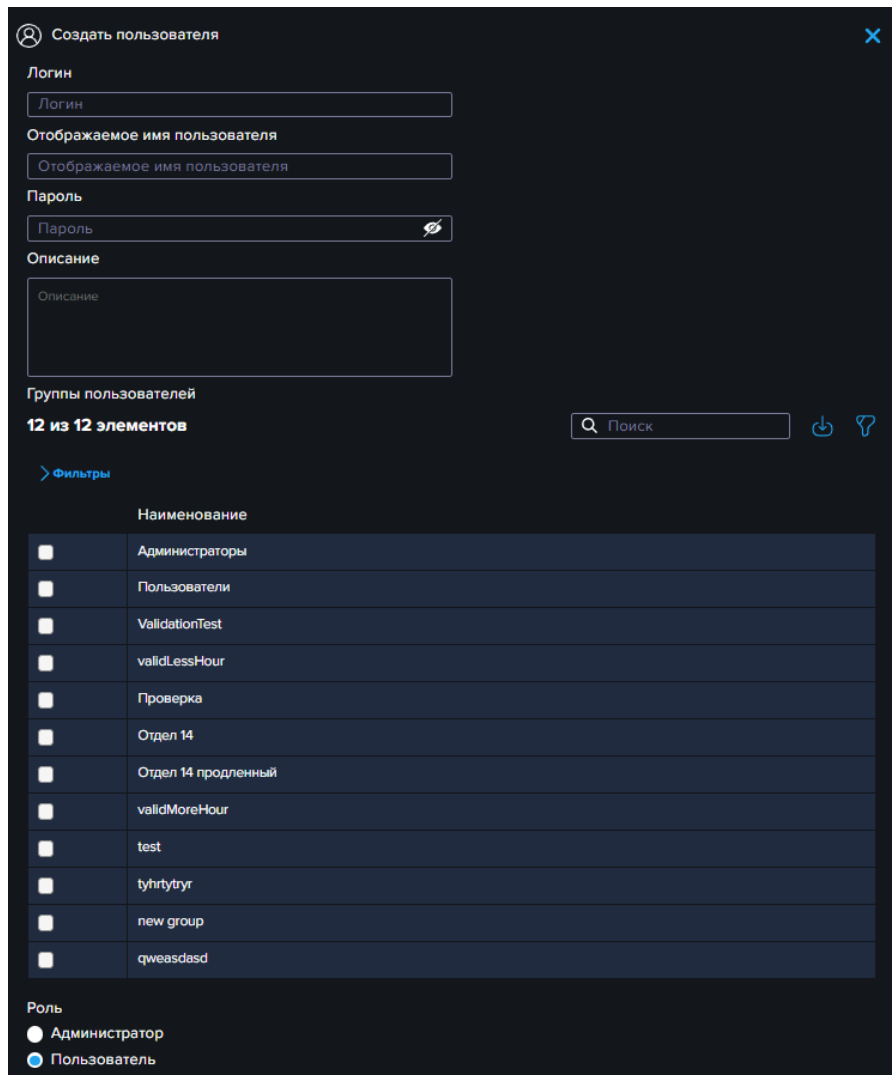
В этом справочнике отображены все пользователи, которые могут зайти в систему.

Нового пользователя могут добавлять только пользователи с ролью "Администратор"



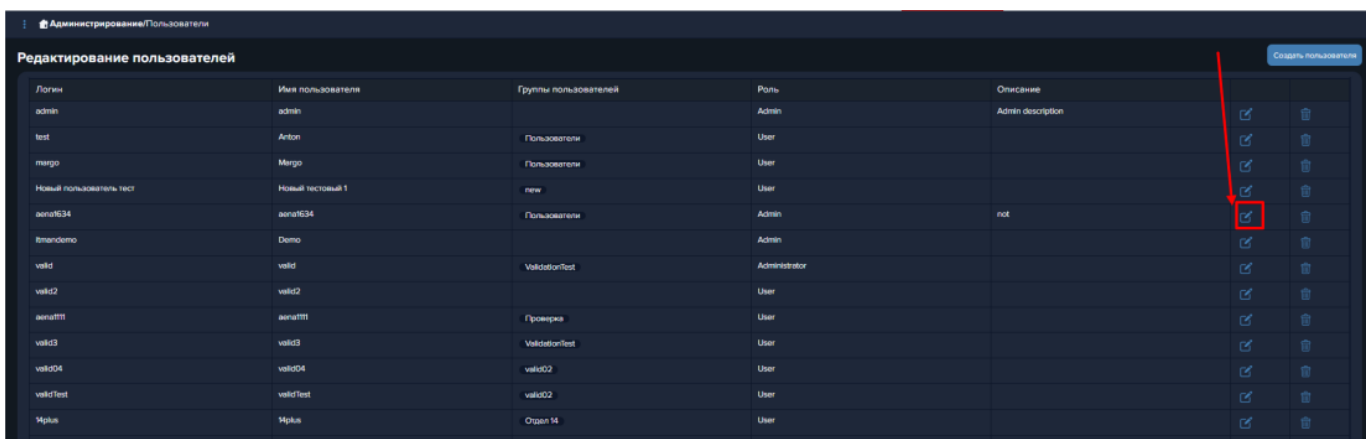
Логин	Имя пользователя	Группы пользователей	Роль	Описание		
admin	admin		Admin	Admin description		
test	Arbon	Пользователи	User			
margo	Margo	Пользователи	User			
Новый пользователь тест	Новый тестовый 1	new	User			
admin634	admin634	Пользователи	Admin	not		
itsrandemo	Demo		Admin			
valid	valid	ValidationTest	Administrator			
valid2	valid2		User			
admin111	admin111	Проверка	User			
valid3	valid3	ValidationTest	User			
valid04	valid04	valid02	User			
validTest	validTest	valid02	User			
14plus	14plus	Отдел 14	User			
14minus	14minus	Отдел 14 проделанный	User			
hourPlus	hourPlus	validMoreHour	User			
hourMinus	hourMinus	validLessHour	User			

Для добавления нового пользователя нажимаем на кнопку "Создать пользователя", после чего откроется боковая панель для ввода данных. Далее заполняем поля в соответствии с настроенной политикой компании или группы.



После того как введем данные, не забудьте запомнить пароль, нажимаем на кнопку "Сохранить".

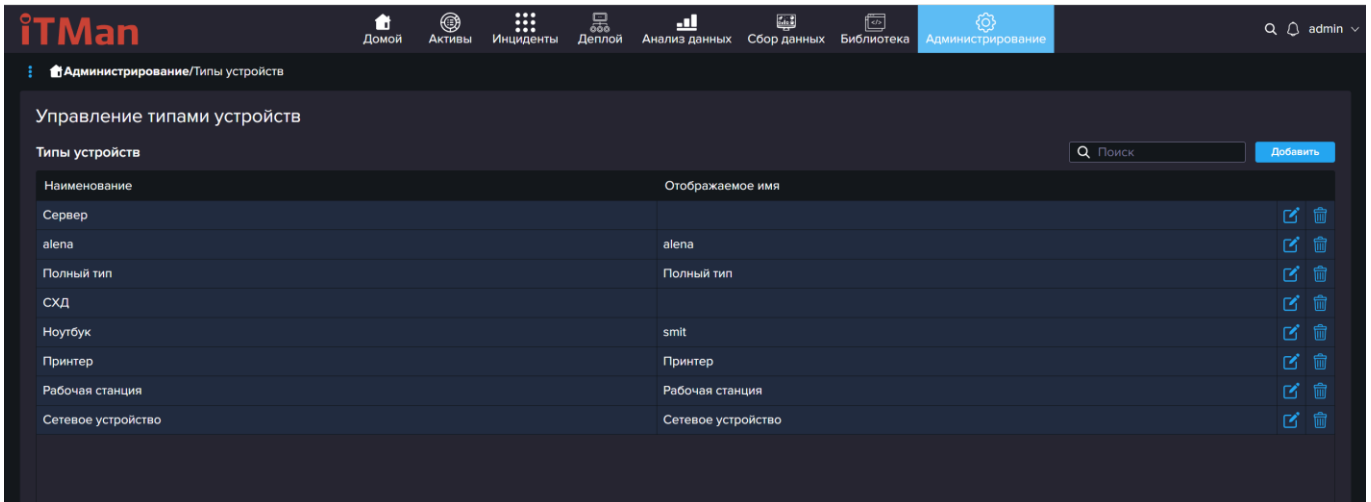
Для редактирования пользователя необходимо нажать на значок редактирование в таблице. И меняем параметры в боковой панели и нажимаем кнопку "Сохранить".



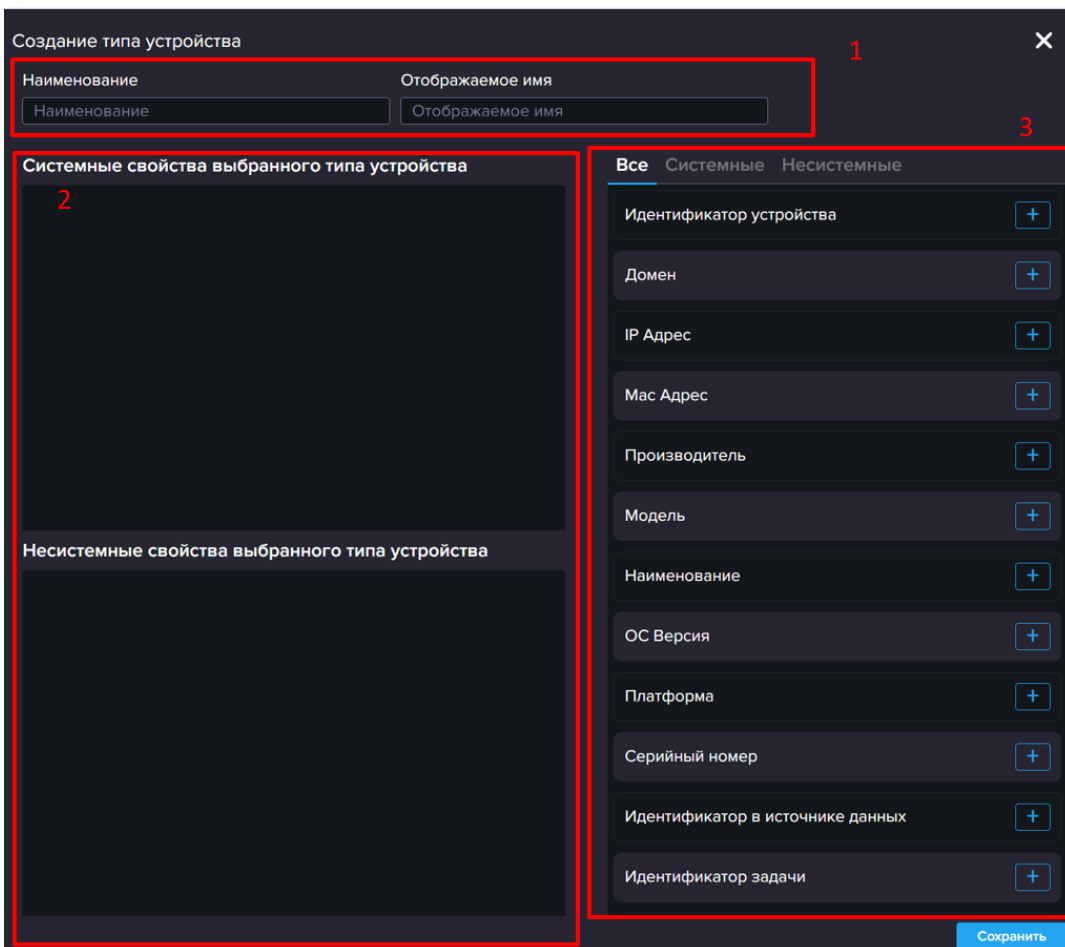
Логин	Имя пользователя	Группы пользователей	Роль	Описание	
admin	admin		Admin	Admin description	
test	Anton	Пользователи	User		
marigo	Margo	Пользователи	User		
Новый пользователь тест	Новый тестовый 1	new	User		
lena1634	lena1634	Пользователи	Admin	not	
Itmandemo	Demo		Admin		
valid	valid	ValidationTest	Administrator		
valid2	valid2		User		
valid111	valid111	Проверка	User		
valid3	valid3	ValidationTest	User		
valid04	valid04	valid02	User		
validTest	validTest	valid02	User		
Мркус	Мркус	Отдел 14	User		

### 3.2.2.4 Тип устройства

В этом справочнике можно настроить отображение полей в карточке устройства в зависимости от «Типа устройства», который вы присвоите.



В системе можно создать свой тип, отредактировать уже существующий или удалить тип. Для того чтобы добавить новый «тип устройства» необходимо нажать на кнопку «Добавить». После чего вам откроется боковая панель с добавлением нового типа.



В боковой панели есть три области:

1. Область наименования типа

2. Область полей, которые уже добавлены в карточку
3. Область полей, которые можно добавить в карточку

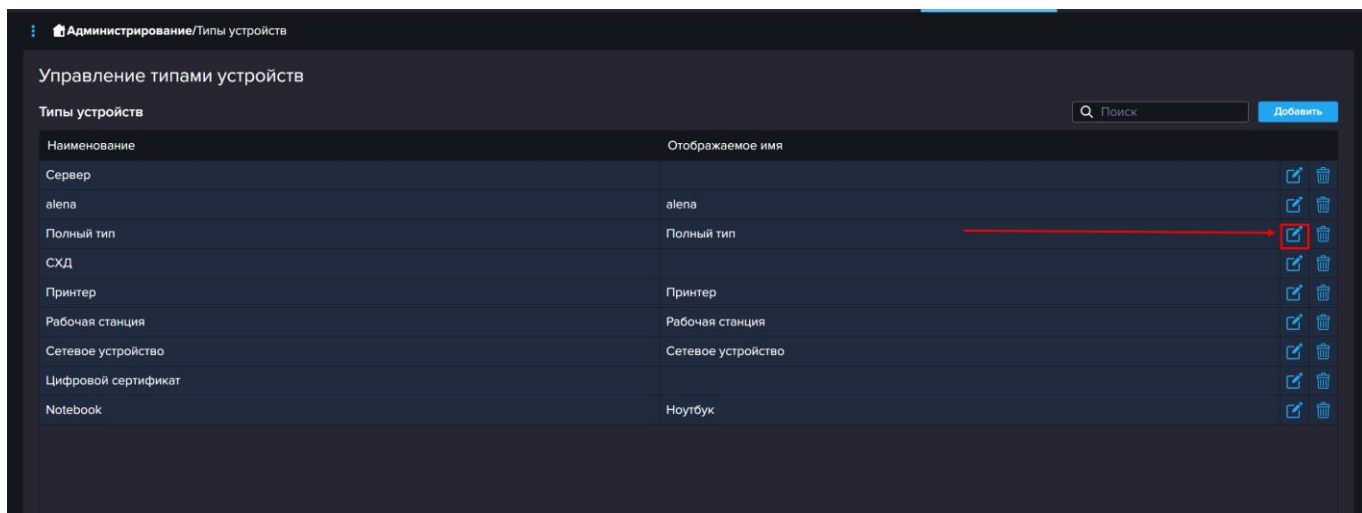
В начале рассмотрим область 3 в ней отображается список системных полей, которые собираются при инвентаризации и несистемных полей, которые можно будет добавить в справочнике «Администрирование» - «Поля устройства».

Вернемся к заполнению, для этого в поле «Наименование» вводим значение, например, «Системный блок», далее в поле «Отображаемое имя» вводим значение, которое мы будем выбирать в нашей «Карточке устройства», например: «Системный блок».

Затем из области 3 выбираем все поля, которые мы хотим видеть в карточке устройства на страницу «Сводной информации». Если какого, то поля нет в списке, то вы можете его добавить в справочнике [«Администрирование»- «Поля устройств»](#). Но важно помнить, что пока в автоматической инвентаризации устройств будут заполняться только те поля, которые уже были в системе, новые поля можно заполнять только в ручном исполнении.

Как вы могли заметить после добавления полей все выбранные поля попадают в область 2 и делятся на два типа: Системные и Несистемные.

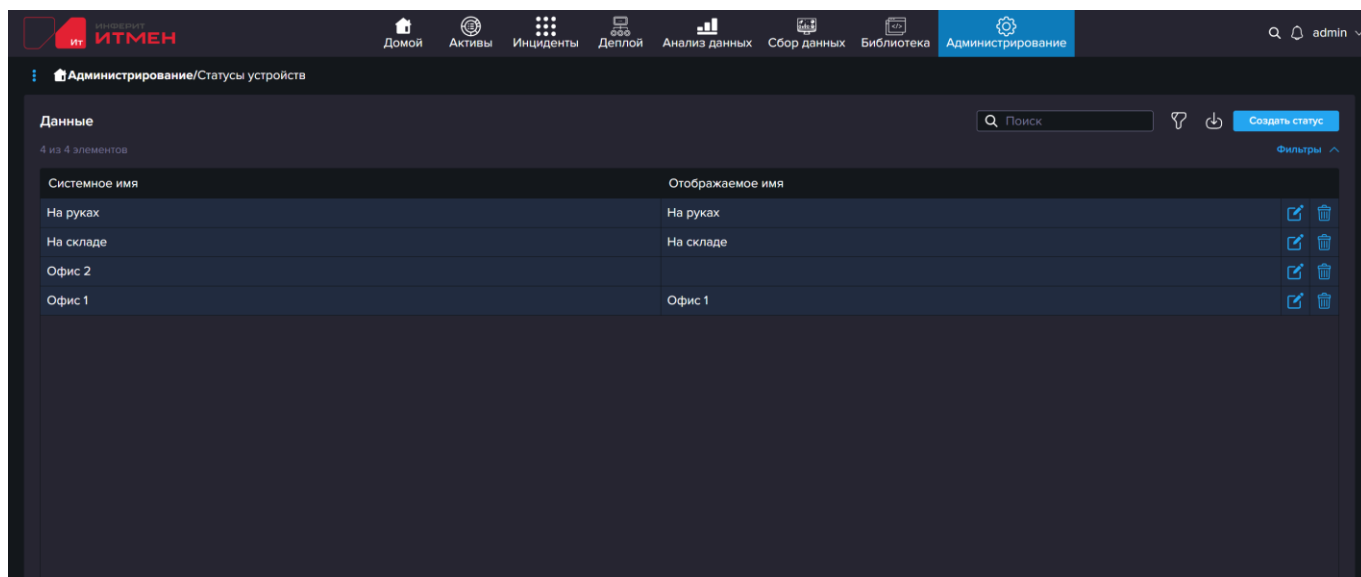
После того как все поля добавлен в наш Тип необходимо нажать кнопку «Сохранить». Если же вы поняли, что допустили ошибку или какого, то поля не хватает, то необходимо нажать на кнопку «Редактирования».



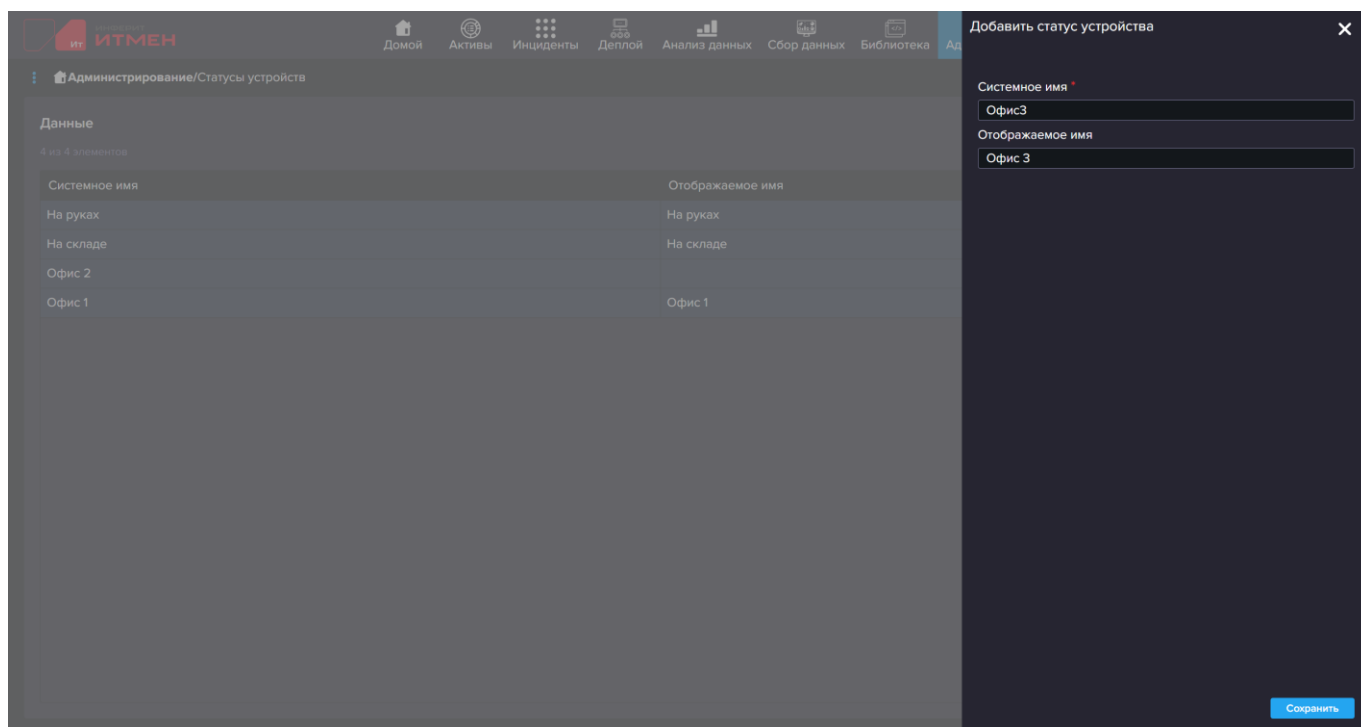
### 3.2.2.5 Статусы устройств

В этом справочнике указываются статусы устройств, которые будут использоваться в ваших устройствах. Для создания статуса необходимо перейти в раздел Администрирование – Статусы устройств.





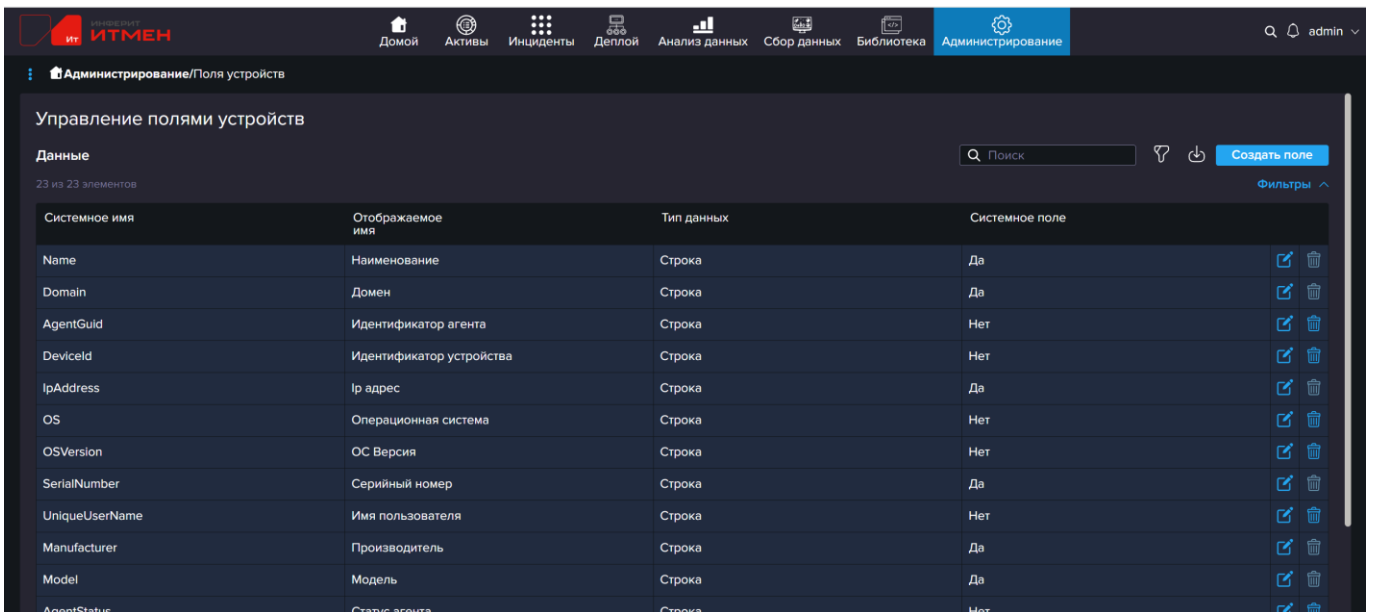
Для создания статуса нажимаем кнопку «Создать статус». После чего у вас откроется боковая панель, в которой необходимо ввести «Системное имя» и «Отображаемое имя».



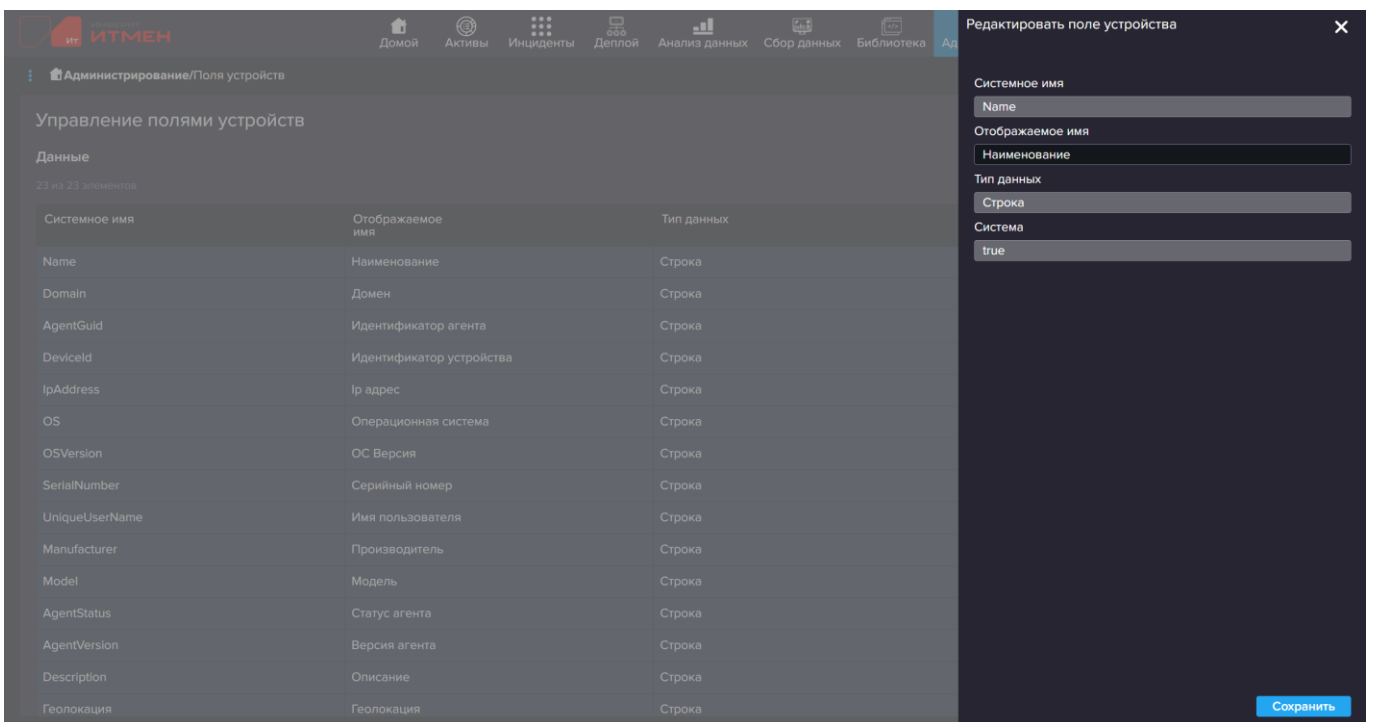
После того как данные будут введены необходимо нажать кнопку «Сохранить». Если вы увидели ошибку в вашем сохранённом статусе, всегда можно будет его отредактировать или удалить и создать новое.

### 3.2.2.6 Поля устройства

В этом справочнике отображены поля, которые будут использоваться в «Карточке устройства». Поля делятся на системные и не системные. Системные это те поля, которые будут использоваться в инвентаризации, не системные это те поля, которые можно добавить дополнительно для ввода информации, которая не будет меняться автоматически при инвентаризации.

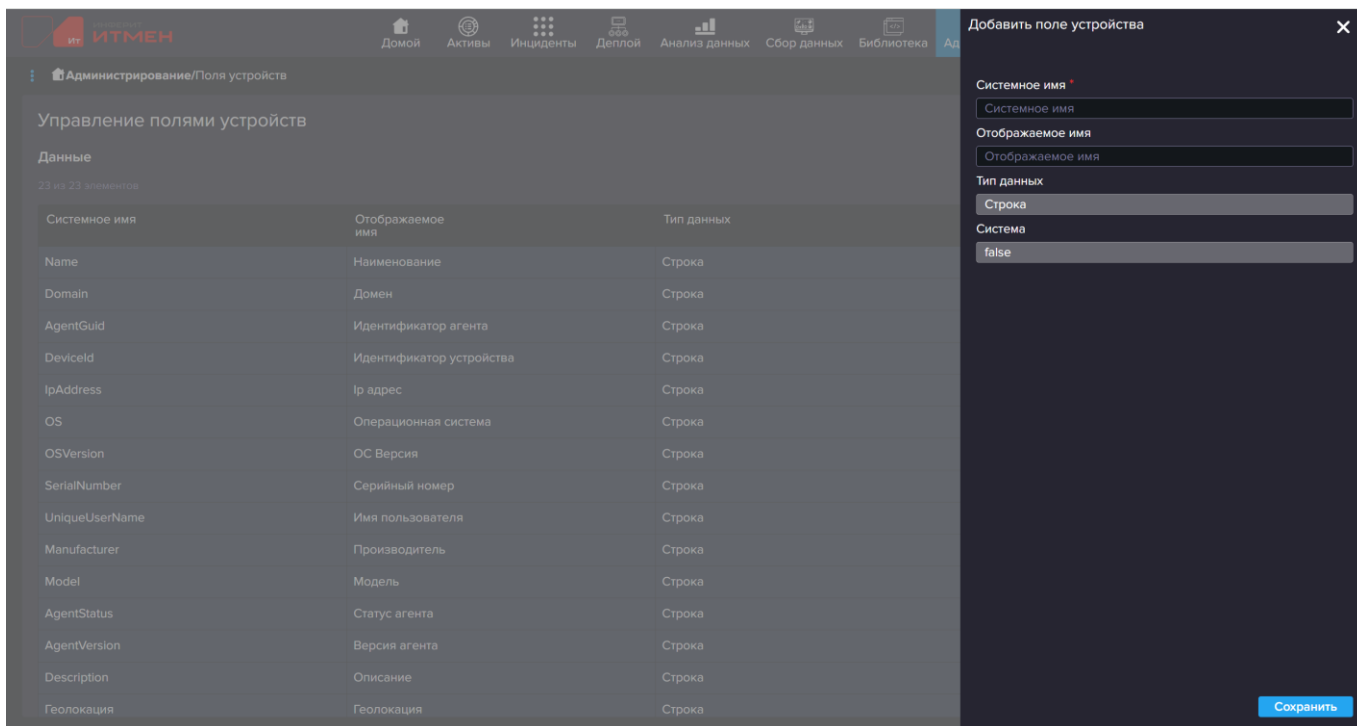


В системных полях можно изменять только «Отображаемое имя». Для этого необходимо нажать на значок редактирования около необходимой записи.



В открывшейся боковой панели изменяем запись и нажимаем кнопку «Сохранить».

Для создания нового поля необходимо нажать на кнопку «Создать размещение».

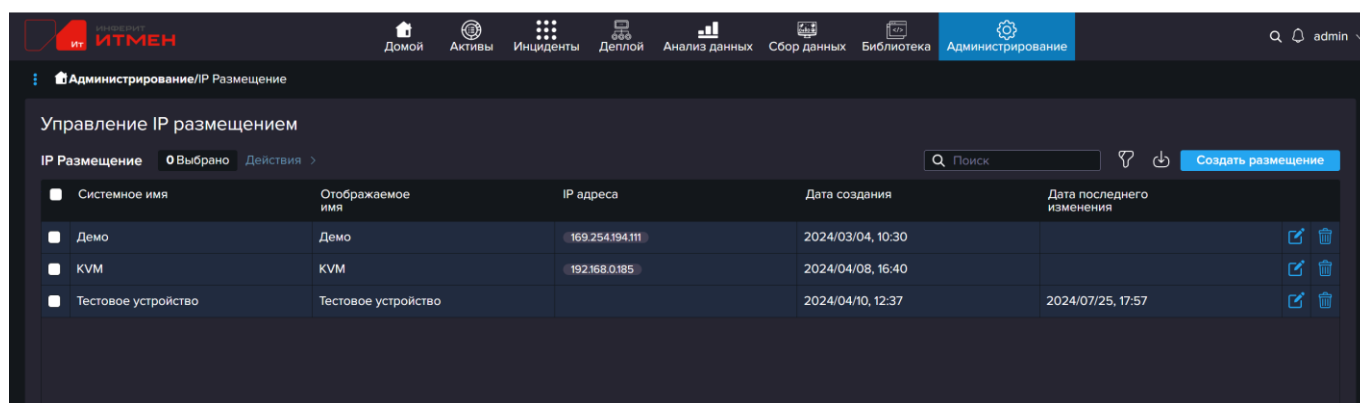


В открывшейся боковой панели вводим «Наименование» и отображаемое имя, значения «Тип» и «Система» не меняются.

Важно! Далее отображение этих полей в карточке у вас будет настраиваться в справочнике «Администрирование» -«Тип устройства».

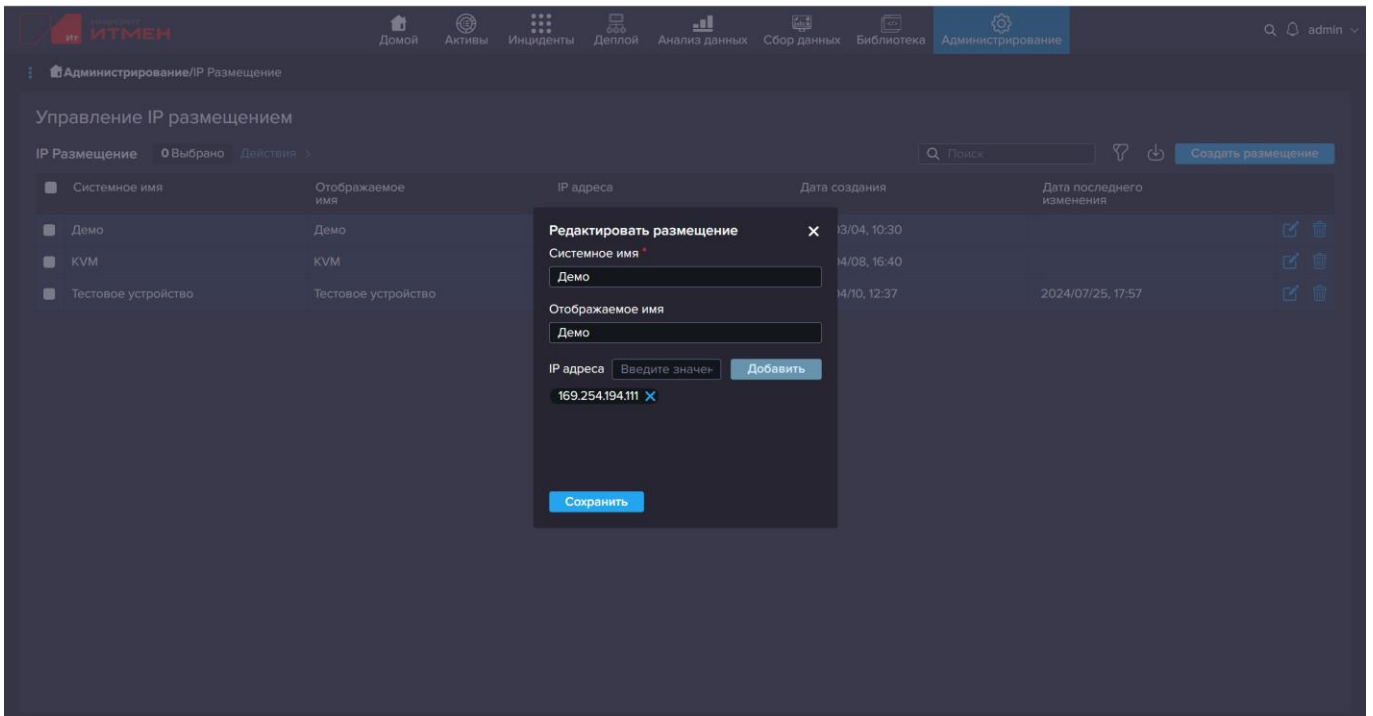
### 3.2.2.7 IP размещение

Это справочник, в котором указываются все IP адреса, которые можно приводить к читаемому виду при инвентаризации.

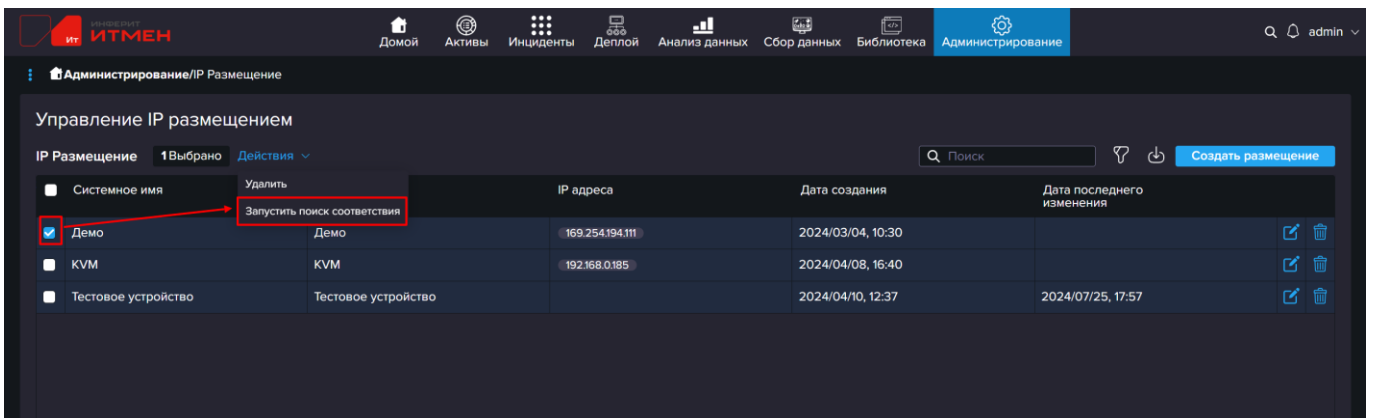


Например, у вас при инвентаризации отображаются адреса, а вам необходимо как-то эти адреса с группировать и отображать читаемы вид, например: «отдел 1».

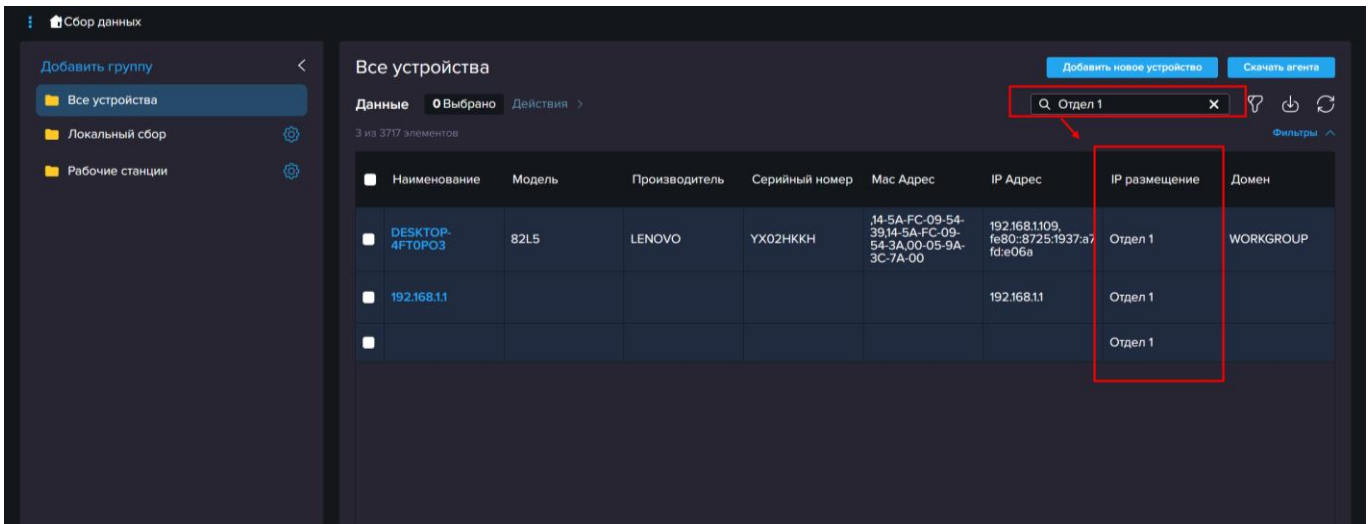
Для этого нажимаем на кнопку «Создать размещение». После этого у вас откроется модальное окно, где мы введем «Наименование» и «Отображаемое имя». Затем в поле IP адрес введем наш диапазон, который нужен или определенный IP, после этого нажмем кнопку «добавить» около поля.



Если необходимо добавить еще адреса в этот отдел их также можно добавить дополнительно. После того как все будет добавлено нажимаем кнопку «Сохранить» и в общем списке появляется наша запись. Теперь для того, чтобы применить нашу запись к нашему инвентаризационному списку в «Сборе данных – Все устройства», нам необходимо выделить нашу запись чек-боксом. Затем нажать на кнопку «Действия» и из выпадающего списка выбрать значение «Запустить поиск соответствия».

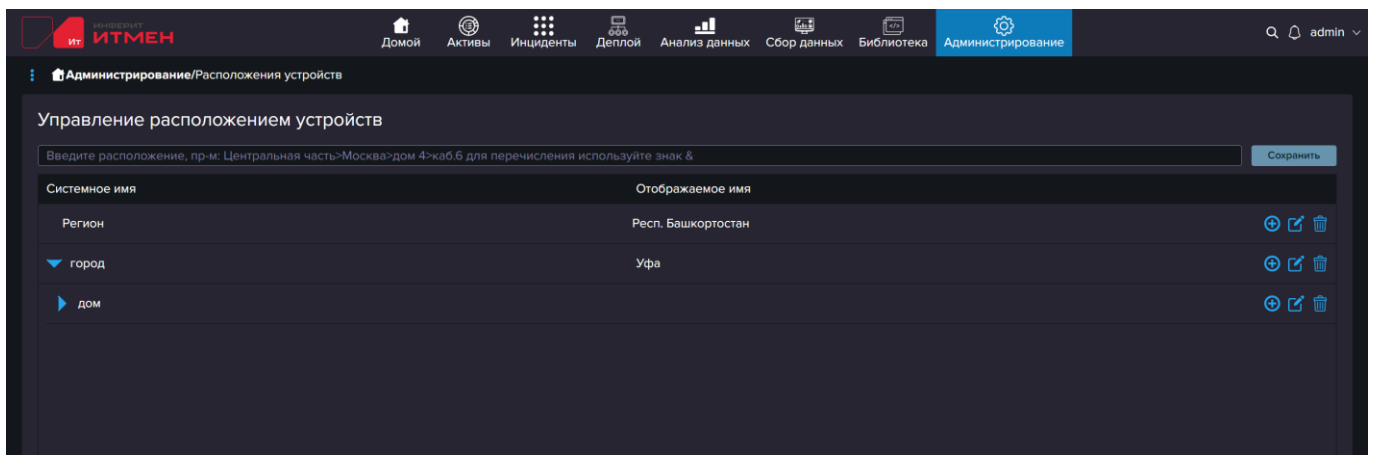


После того как запустили поиск переходим в «Сбор данных – Все устройства». В поиск вводим наше значение например «Отдел 1» и смотрим у всех наших IP адресов из диапазона проставилось значение в столбце «IP размещение».



### 3.2.2.8 Расположение устройств

Справочник, в котором можно указать регионы и в дальнейшем к устройству прикреплять значение расположение устройства.

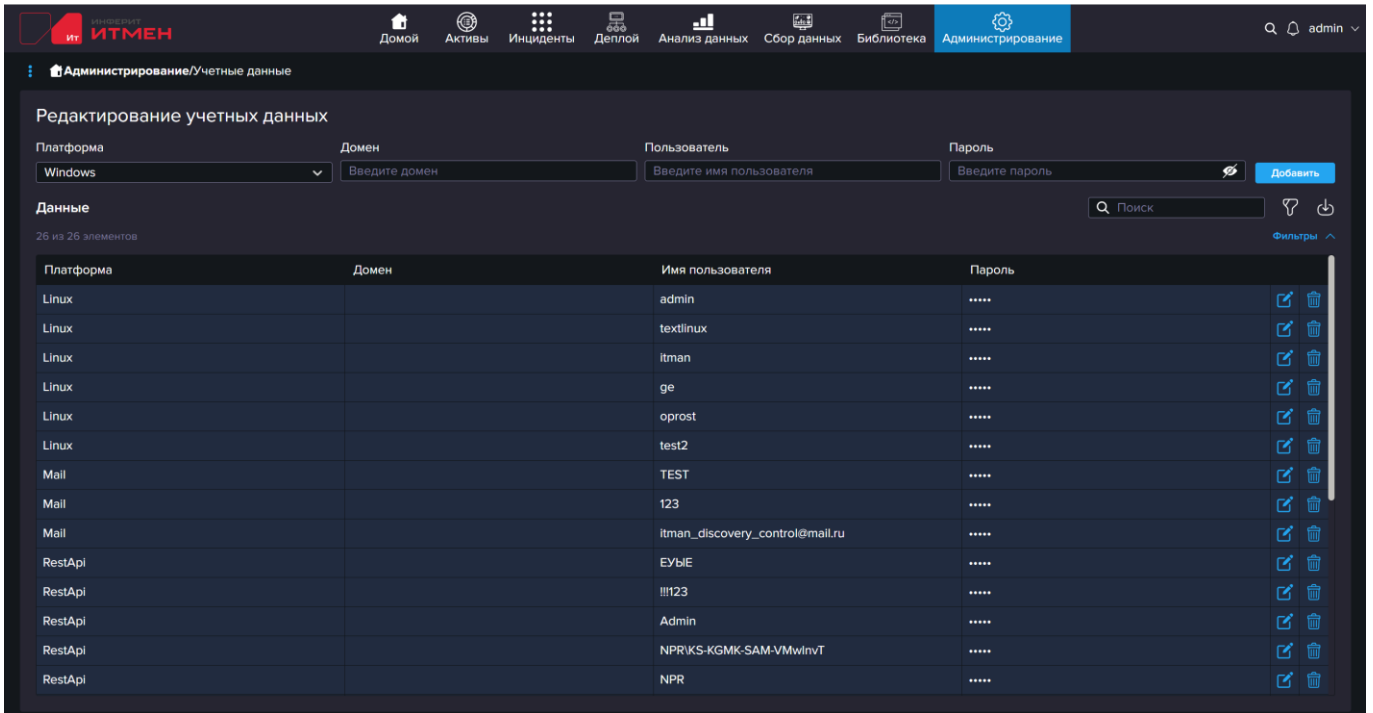


### 3.2.2.9 Учетные данные

В этом справочнике представлены учетные данные для проведения сетевой инвентаризации, SQL. В справочнике представлены 4 типа Учетных данных:

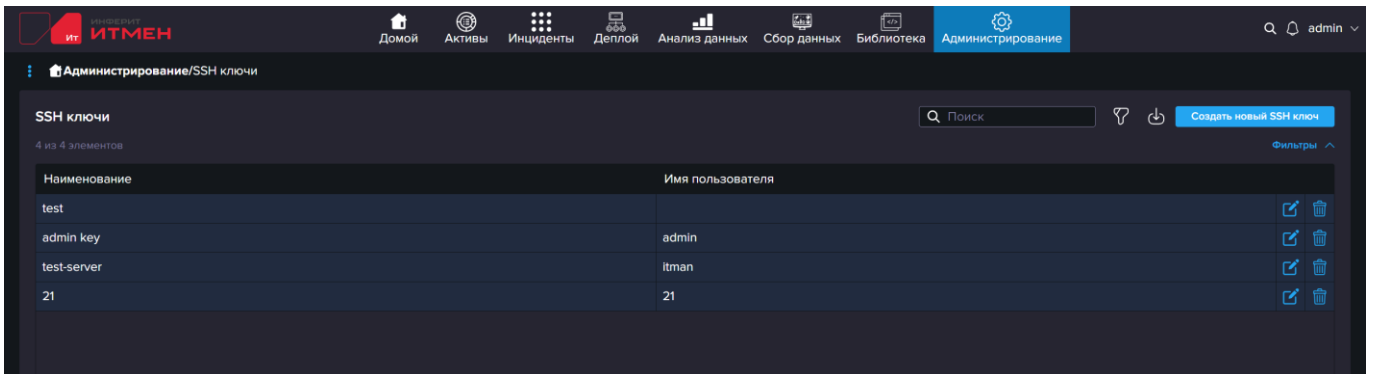
- SQL
- Linux
- Windows
- SNMP
- Mail
- REST API

Так же новые учетные данные можно добавлять напрямую из создания задачи «Сетевой инвентаризации», а в справочнике уже управлять учетными данными.



### 3.2.2.10 SSH ключи

В этом справочнике будут отображаться SSH-ключи, которые вы в дальнейшем сможете использовать для сетевой инвентаризации.

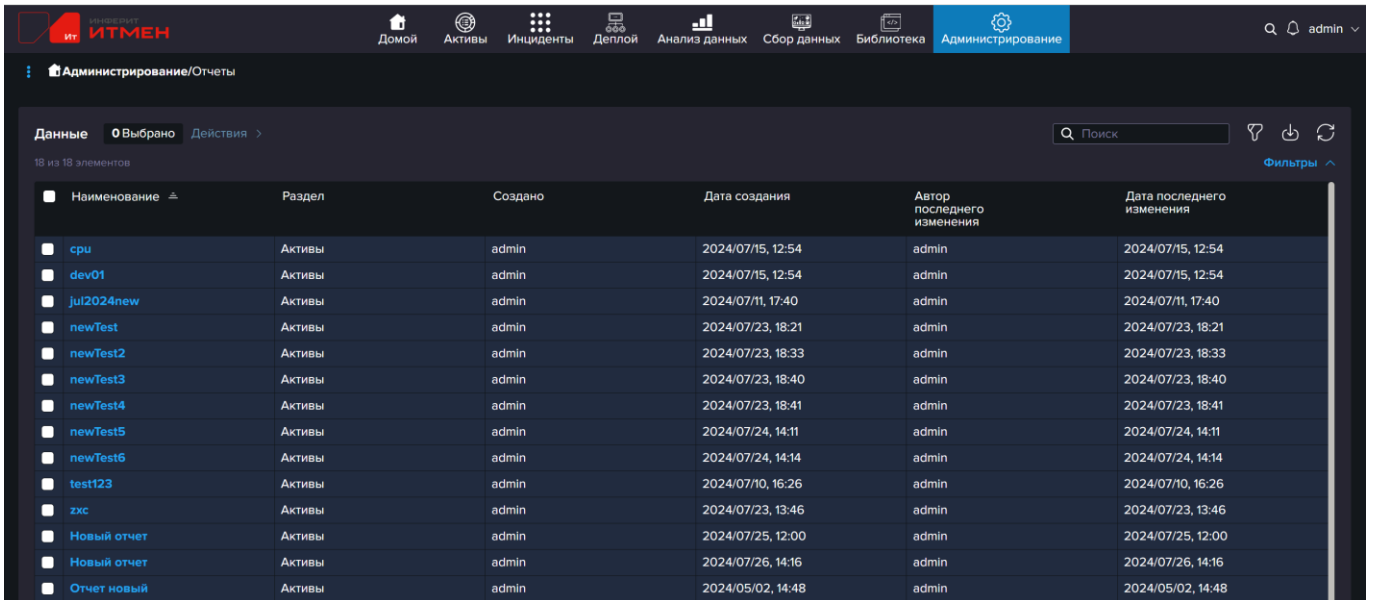


### 3.2.3 Отчетность

В этом подразделе есть два вида Отчеты и Отчеты по программному обеспечению.

#### 3.2.3.1 Отчеты

Рассмотрим вкладку Отчеты. На этой вкладке отображены все созданные отчеты, когда они были созданы, кем были созданы и из какого раздела были созданы. Для того чтобы перейти в отчет необходимо нажать на его "Наименование".



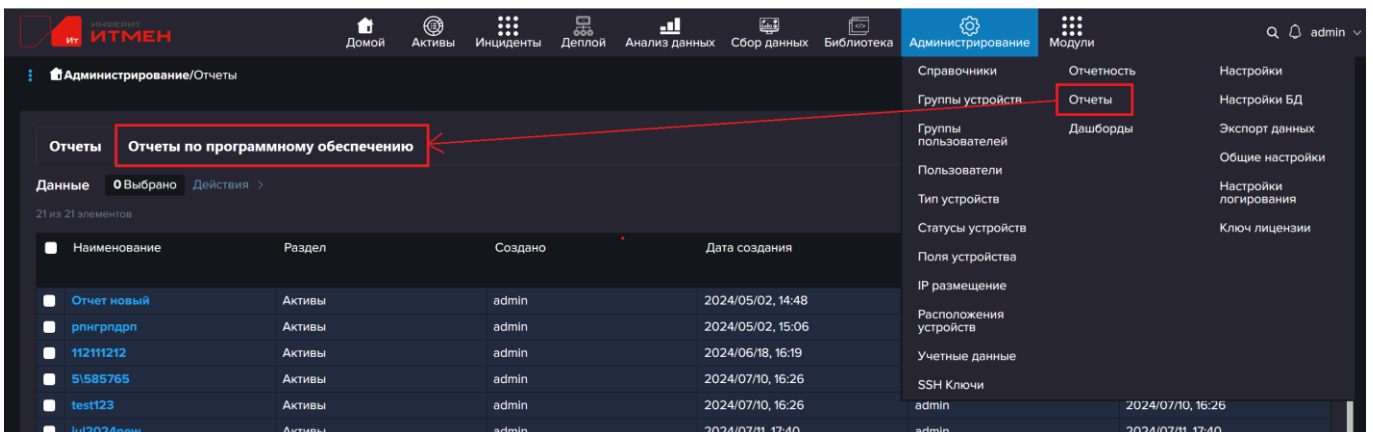
Наименование	Раздел	Создано	Дата создания	Автор последнего изменения	Дата последнего изменения
cpu	Активы	admin	2024/07/15, 12:54	admin	2024/07/15, 12:54
dev01	Активы	admin	2024/07/15, 12:54	admin	2024/07/15, 12:54
jul2024new	Активы	admin	2024/07/11, 17:40	admin	2024/07/11, 17:40
newTest	Активы	admin	2024/07/23, 18:21	admin	2024/07/23, 18:21
newTest2	Активы	admin	2024/07/23, 18:33	admin	2024/07/23, 18:33
newTest3	Активы	admin	2024/07/23, 18:40	admin	2024/07/23, 18:40
newTest4	Активы	admin	2024/07/23, 18:41	admin	2024/07/23, 18:41
newTest5	Активы	admin	2024/07/24, 14:11	admin	2024/07/24, 14:11
newTest6	Активы	admin	2024/07/24, 14:14	admin	2024/07/24, 14:14
test123	Активы	admin	2024/07/10, 16:26	admin	2024/07/10, 16:26
zxc	Активы	admin	2024/07/23, 13:46	admin	2024/07/23, 13:46
Новый отчет	Активы	admin	2024/07/25, 12:00	admin	2024/07/25, 12:00
Новый отчет	Активы	admin	2024/07/26, 14:16	admin	2024/07/26, 14:16
Отчет новый	Активы	admin	2024/05/02, 14:48	admin	2024/05/02, 14:48

В открывшемся отчете можно отфильтровать данные для поиска. Так же можно отредактировать отчет, для это необходимо нажать на кнопку "Редактировать". Подробнее можно как работать с Отчетом можно ознакомиться в разделе "Анализ данных".

### 3.2.3.2 Отчеты по программному обеспечению

В этом отчете приведены данные сбора задачи трекинга.

Рассмотрим по подробнее, для этого нажимаем вкладку «Отчеты по программному обеспечению».

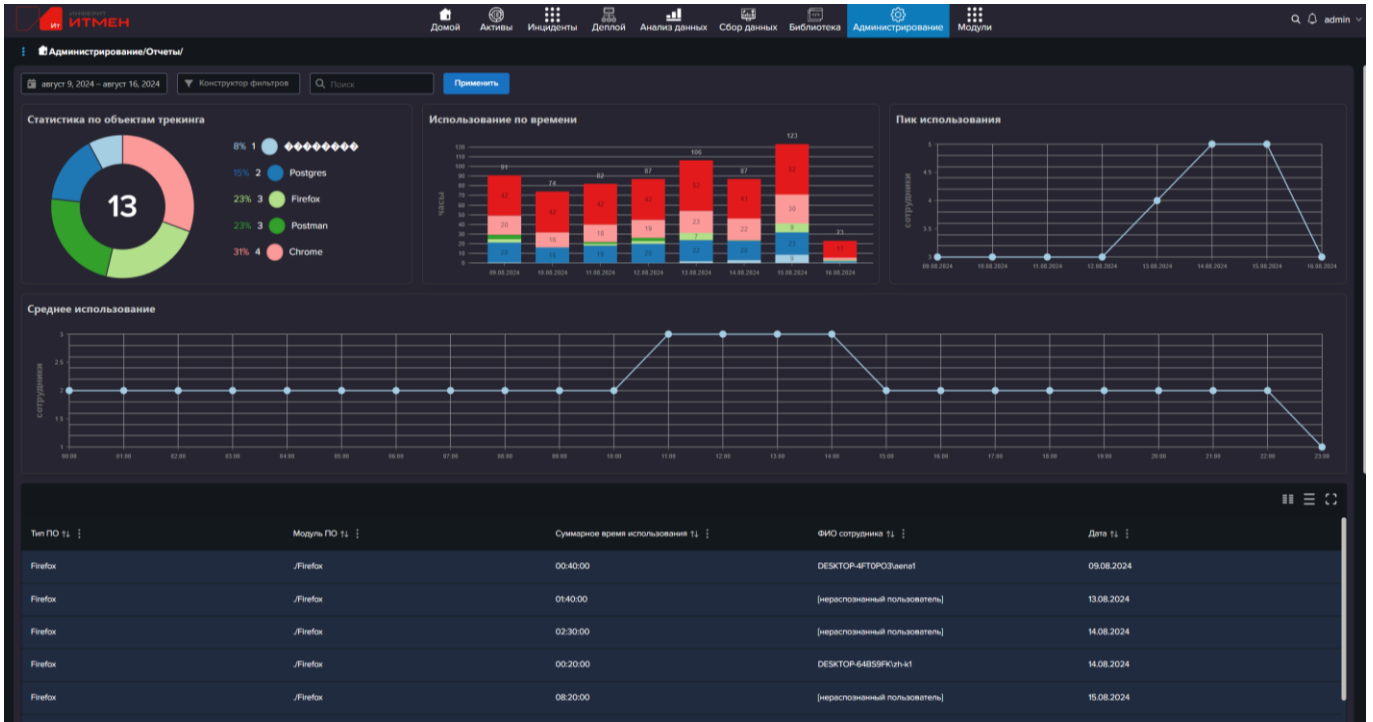


Наименование	Раздел	Создано	Дата создания
Отчет новый	Активы	admin	2024/05/02, 14:48
plngrpdrp	Активы	admin	2024/05/02, 15:06
112111212	Активы	admin	2024/06/18, 16:19
51585765	Активы	admin	2024/07/10, 16:26
test123	Активы	admin	2024/07/10, 16:26
jul2024new	Активы	admin	2024/07/11, 17:40

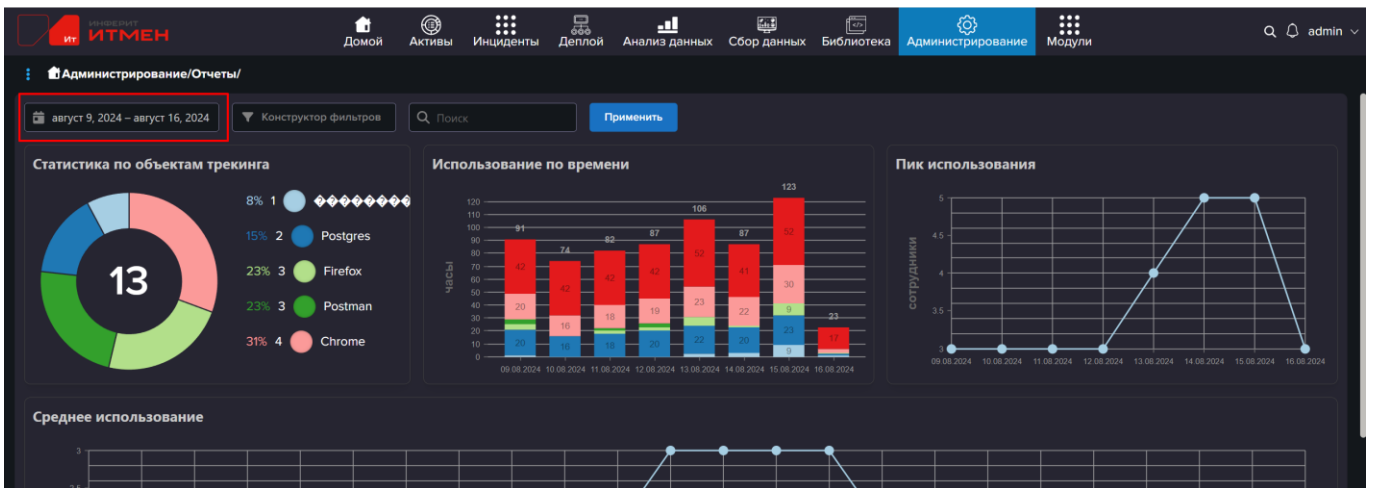
В открывшейся вкладке мы видим Таблицу, где нажимаем на пока единственный отчет «Отчет по программному обеспечению». В котором мы видим три блока:

- Настройки фильтрации
- Графики
- Таблица

Все три блока взаимосвязаны. Например, в зависимости что мы выберем в блоке фильтрации то и будет отображено в графиках и в таблице.



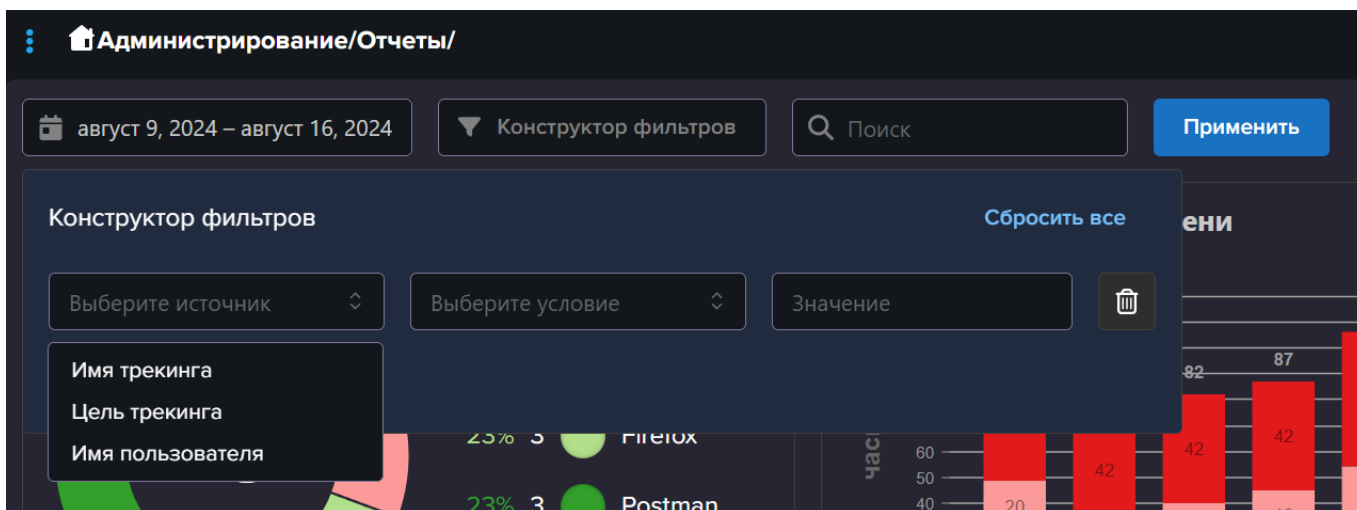
Если данные не отображаются необходимо будет установить правильные даты, когда работала задача трекинга. Поэтому важно корректно указывать даты в верхнем фильтре.



Далее в конструкторе фильтров можно фильтровать по:

- Имя трекинга
- Цель трекинга
- Имя пользователя



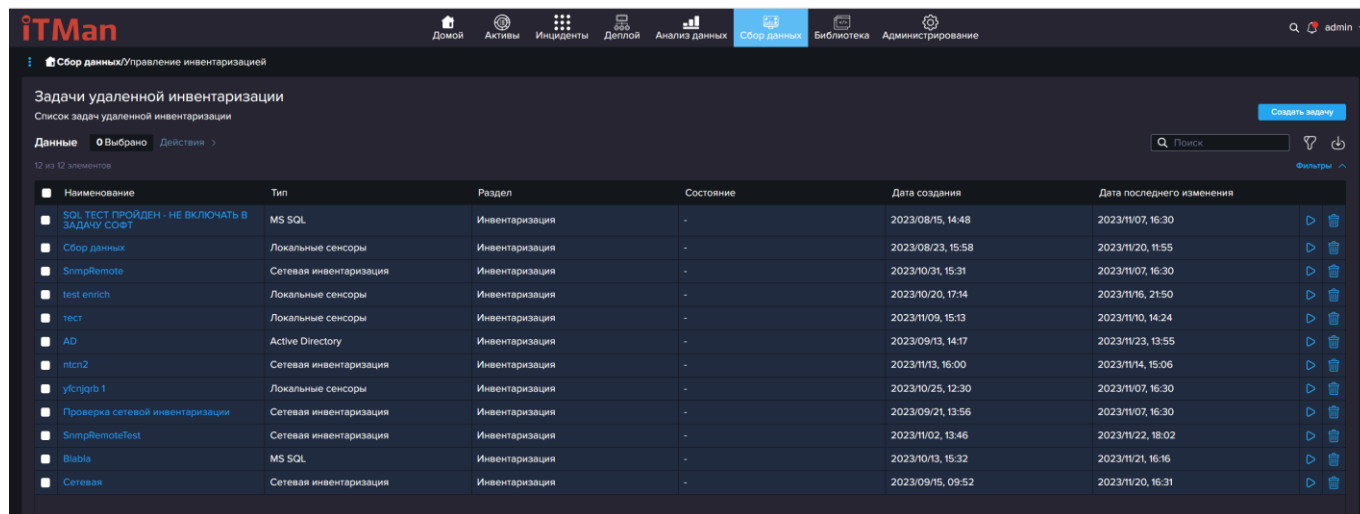


После того как данные фильтра будут выбраны необходимо будет нажать кнопку «Применить», чтобы данные отобразились в графиках и таблице.

Так же в блоке фильтров есть глобальный поиск, в котором можно ввести необходимую фразу, например: Postman, затем нажать кнопку «Применить». После все данные на графе и таблице, перестроятся с учетом выбранной даты.

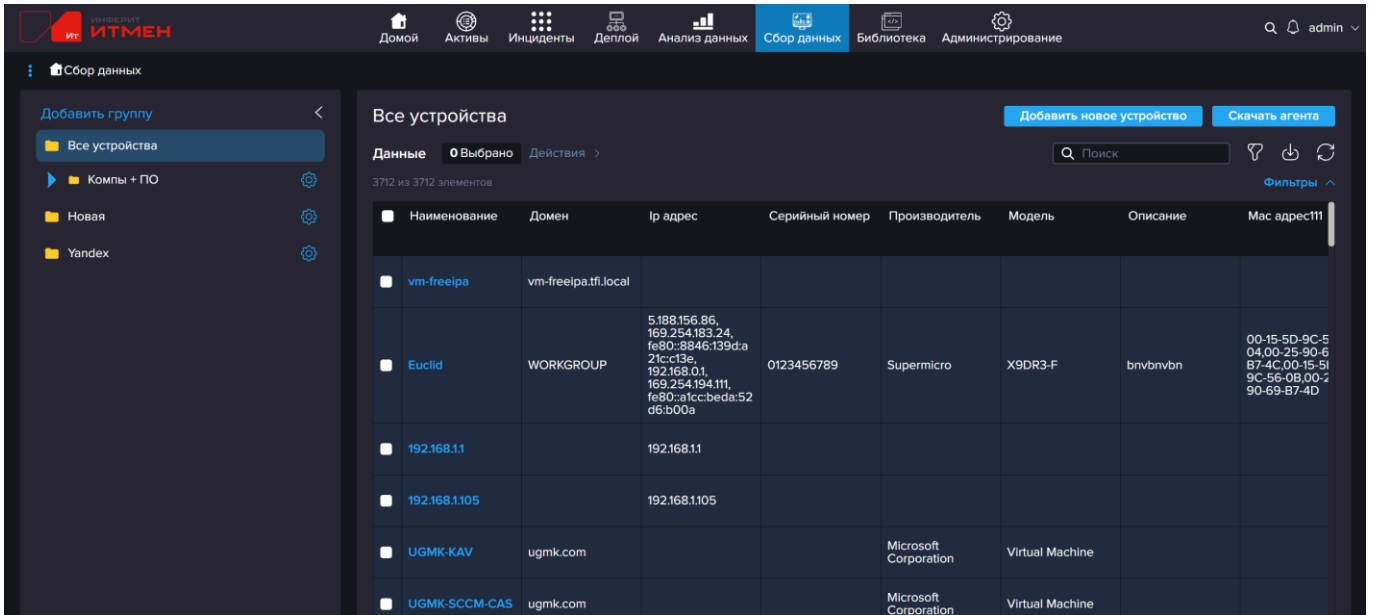
### 3.3 Сбор данных

Это новый раздел, в котором идет сбор инвентаризации по новому типу сенсоров. С помощью него можно опробовать Сбора данных и процесс сохранения в БД.

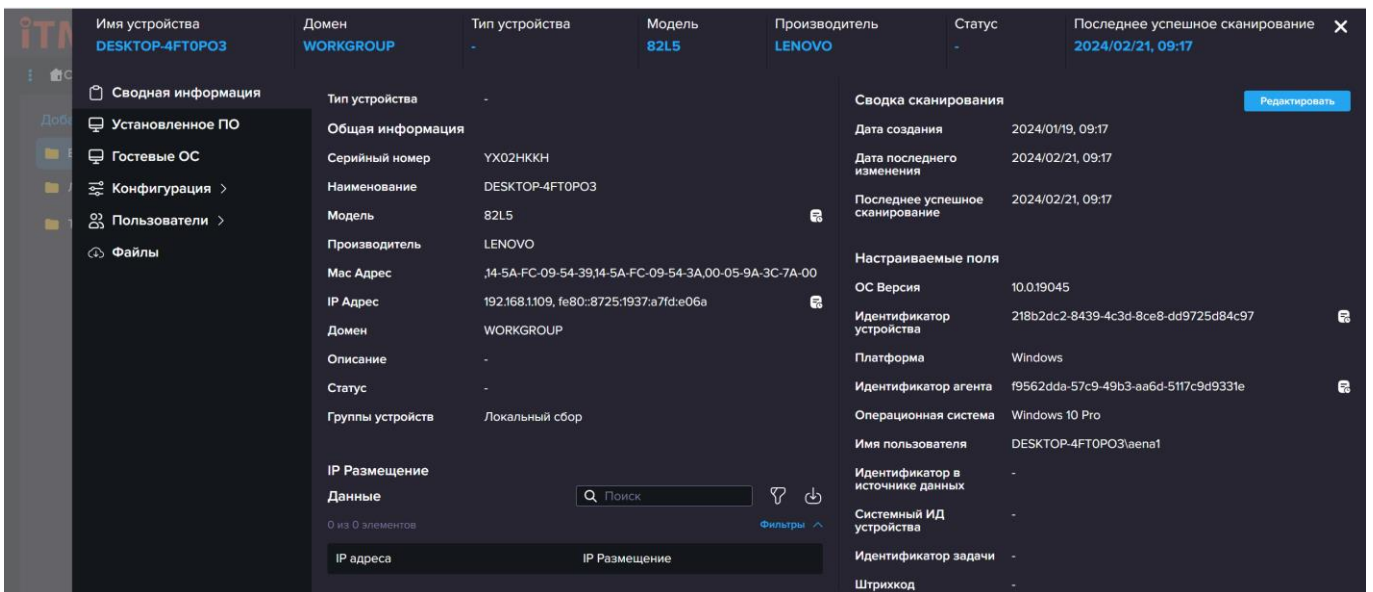


#### 3.3.1 Все Устройства

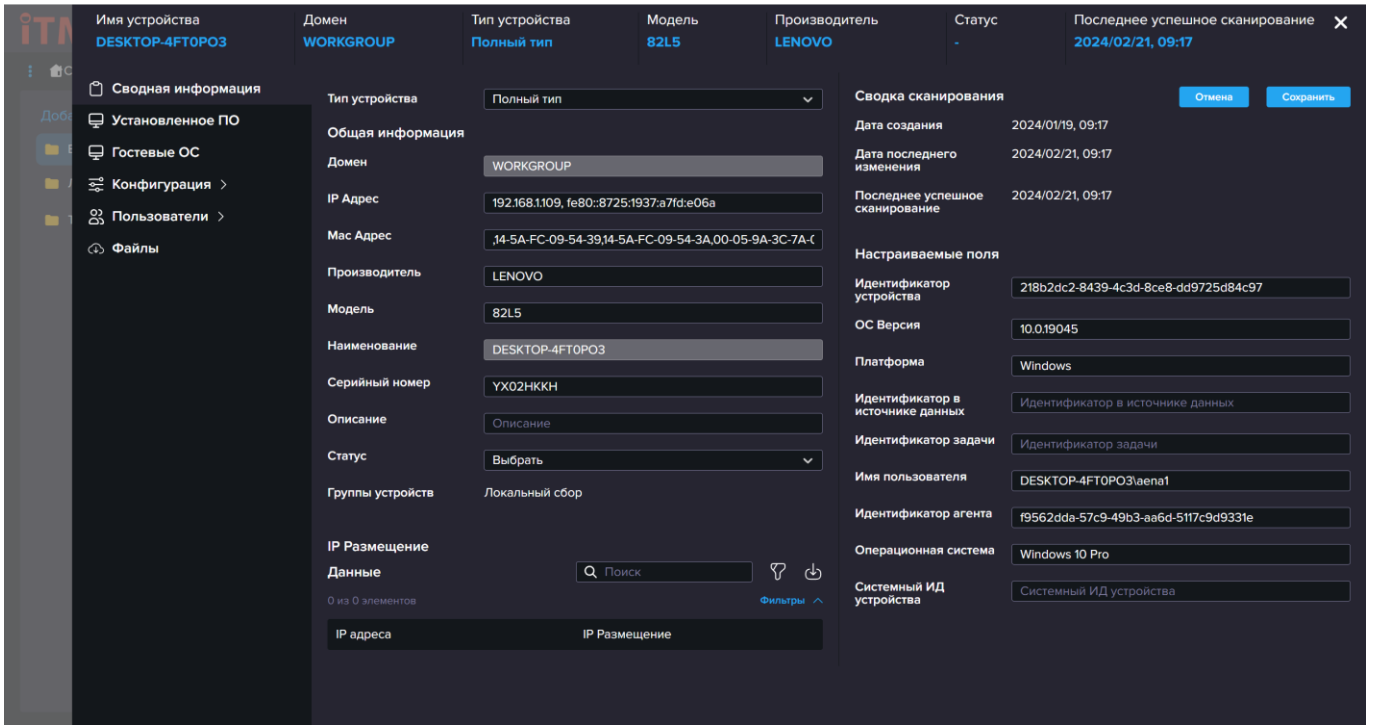
В этом подразделе отображаются все устройства, у которых настроены задачи «Сбора данных», если какое-то устройство еще не отобразилось необходимо подождать некоторое время чтобы инвентаризация завершила свою работу и создала Устройство.



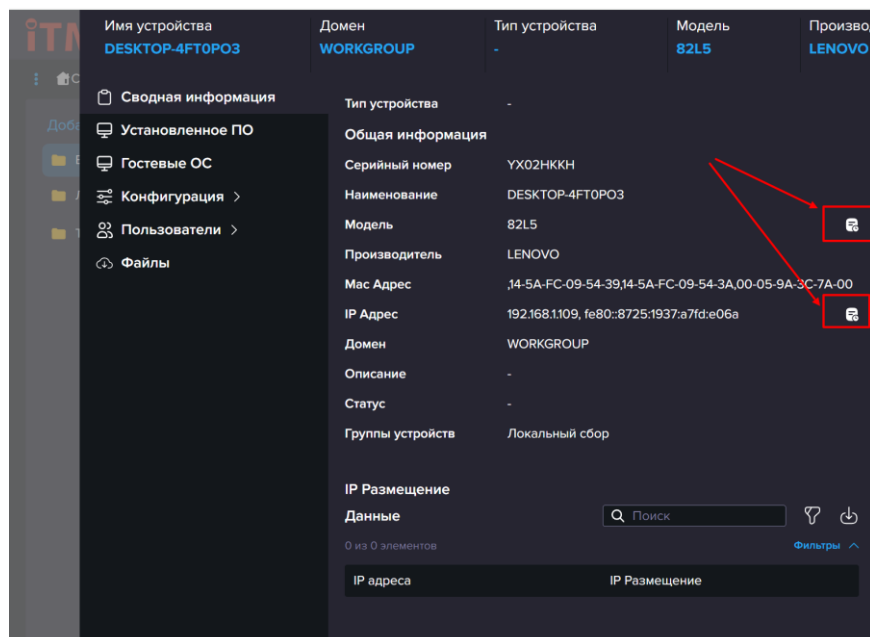
После того как устройства отобразятся мы можем открыть любое устройство. Для этого необходимо нажать на «Наименование» устройства. В открывшемся модальном окне мы видим данные: Сводную информацию, Установленное ПО, Гостевые ОС, Конфигурации, Пользователи, Файлы.



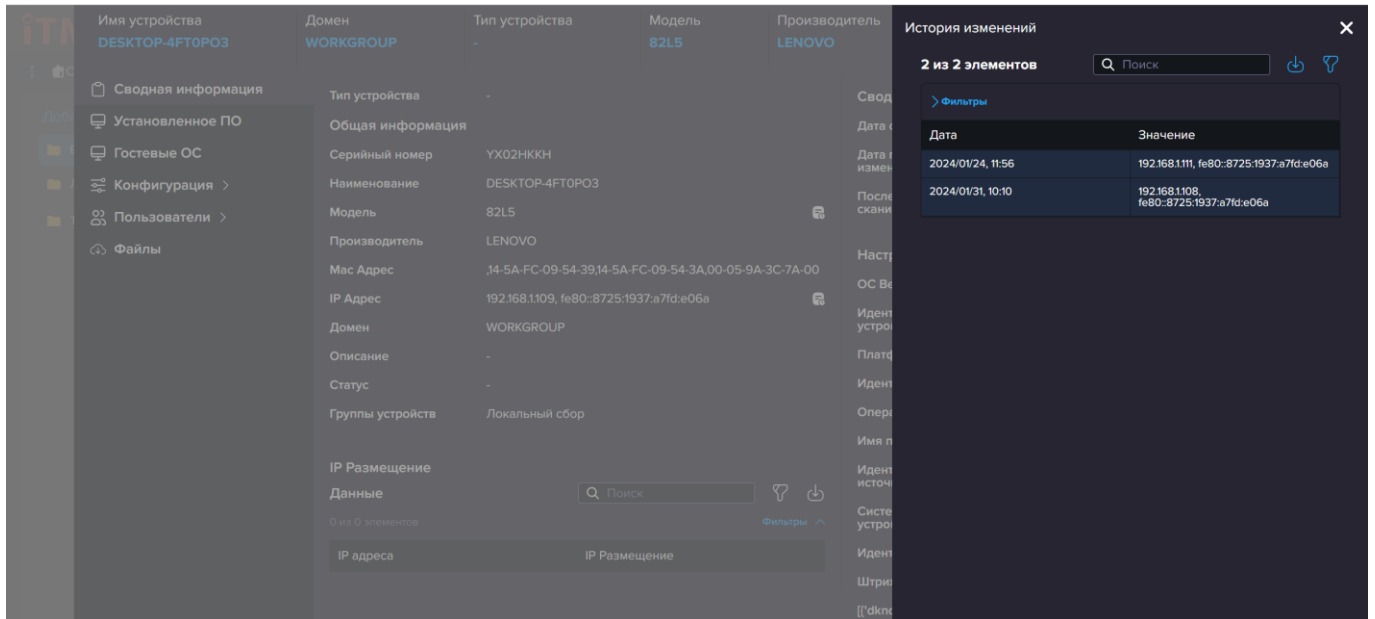
Рассмотрим страницу «Сводной информации». В ней будет представлен набор полей в зависимости от «Типа устройства», который Вы выберете. Описание настройки «Типа устройств» представлено в разделе [«Администрирование»- «Тип устройств»](#). Рассмотрим поля по подробнее.



Поля, уже существующие в системе, будут заполняться автоматически при прохождении инвентаризации. Как это происходит кратко: в системе создается задача, например: «Сбор данных», эта задача посылает сигнал агенту, затем агент принимает этот сигнал и начинает сбор данных, когда данные будут собраны он создает результат, который система через n-ный промежуток времени заберет и сохранит в Базе Данных. После этих действий ваше устройство или обновления отобразятся в разделе «Все устройства» или в вашем устройстве. Если вы отредактируете поле, которое обновляется при инвентаризации, то значение будет изменено на значение, пришедшее от агента. Поэтому лучше редактировать поля, которые вы создадите сами в разделе [«Администрирование»](#)- [«Поля устройства»](#). При изменении любого поля на странице «Сводной информации» у вас отобразится значок истории.



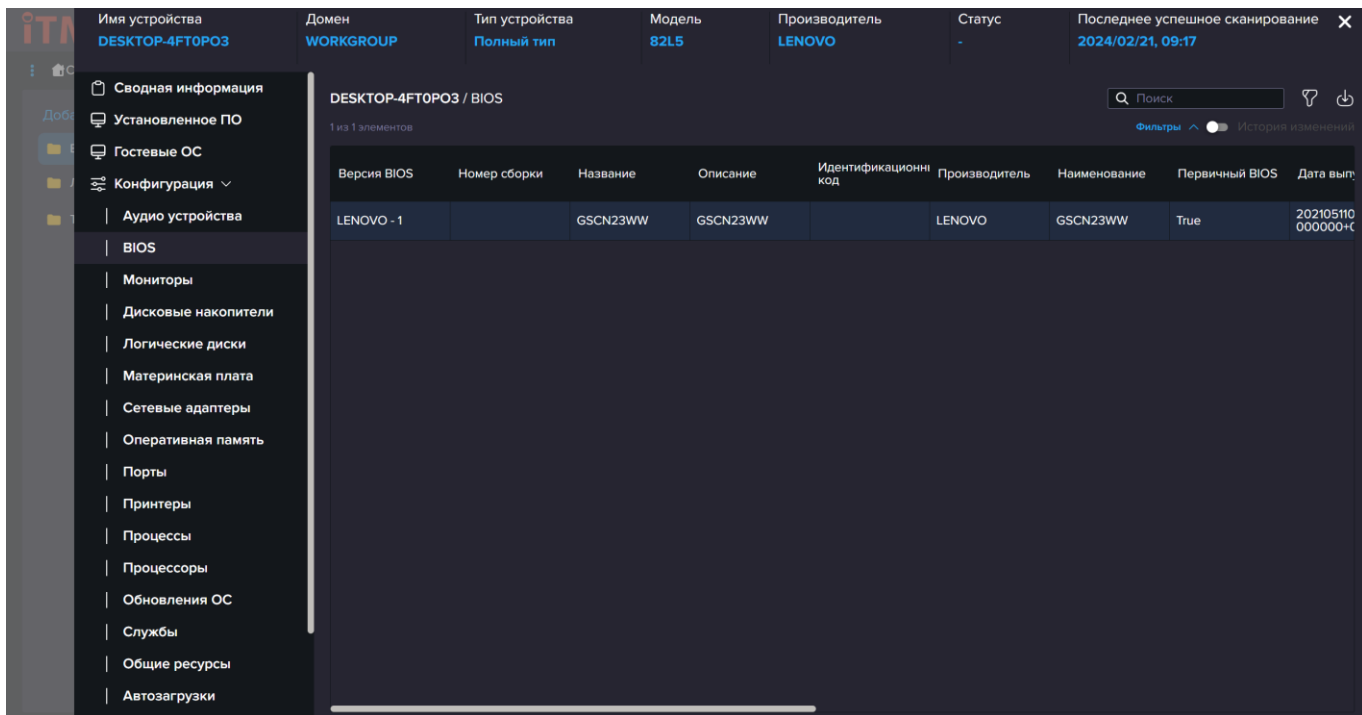
При нажатии на него откроется информация об изменении.



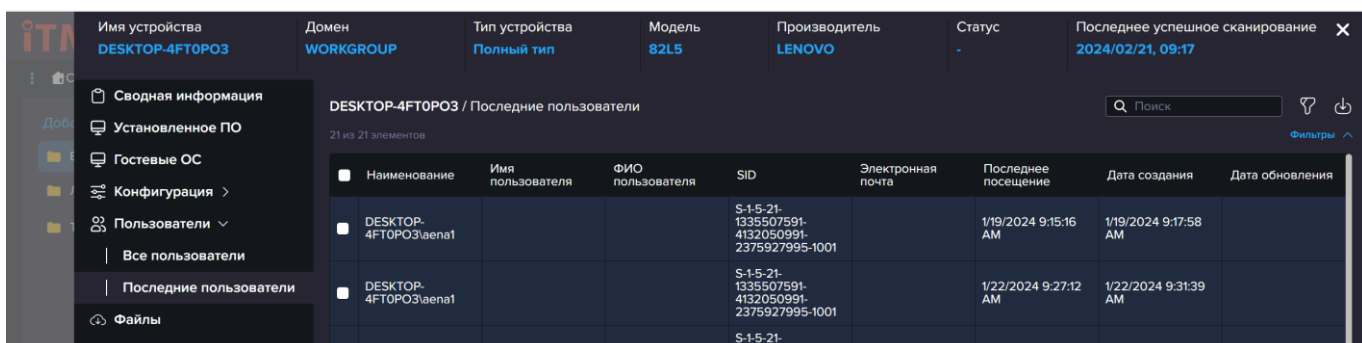
Перейдем к странице «Конфигурации». В конфигурациях представлены данные только те, что смог собрать агент. А также набор может меняться в зависимость от операционной системы.

Например, следующие разделы:

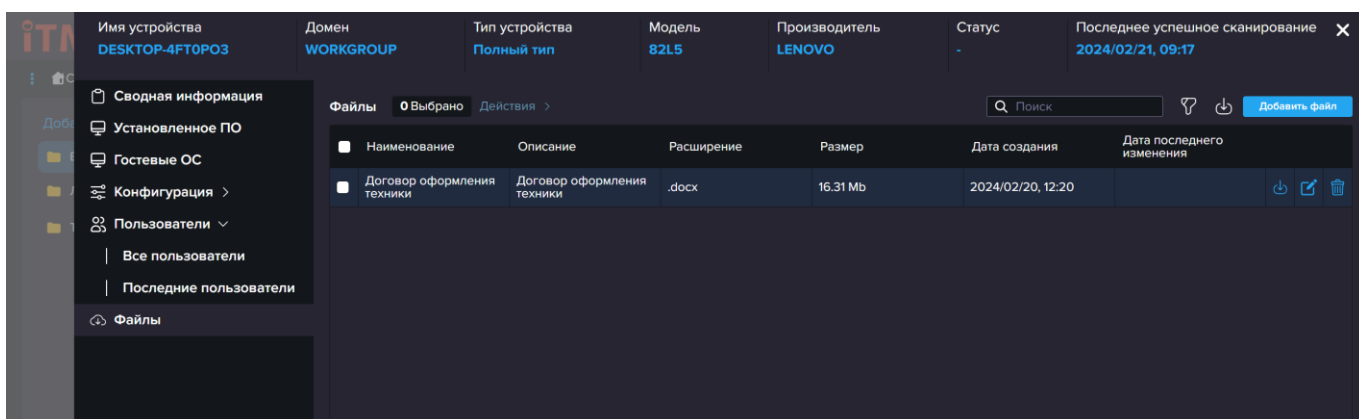
- Аудио устройства
- BIOS
- Мониторы
- Дисковые накопители
- Логические диски
- Материнская плата
- Сетевые адаптеры
- Оперативная память
- Принтеры
- Процессы
- Процессоры
- Обновления ОС
- Службы
- Общие ресурсы
- Автозагрузки
- USB устройства
- Видеокарты



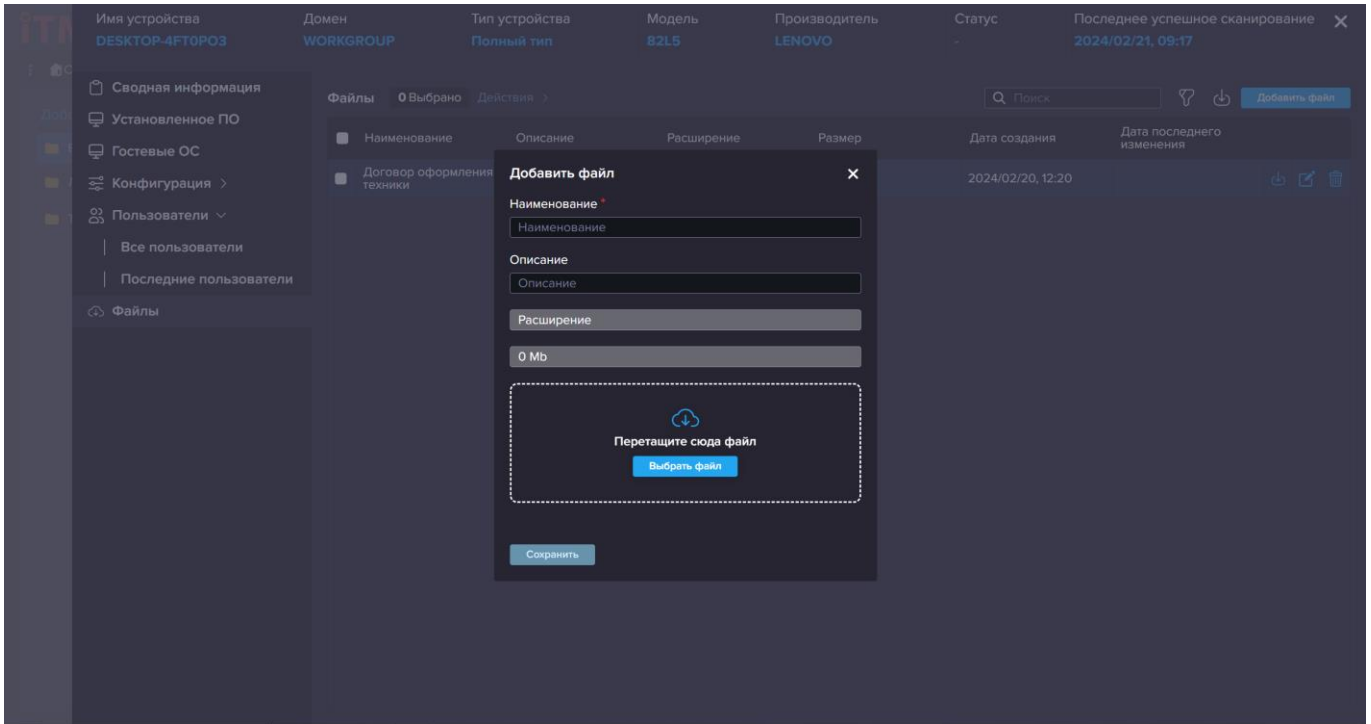
В блоке пользователи так же есть два раздела: Все пользователи и последние пользователи. Эти два блока отличаются тем, что в последних пользователях можно посмотреть, когда последний раз пользователь авторизовывался на устройстве (время отображения зависит от последнего сканирования данного устройства).



Блок файлы, представляет собой блок, в котором можно хранить прикрепленные файлы, которые будут относиться к этому устройству.

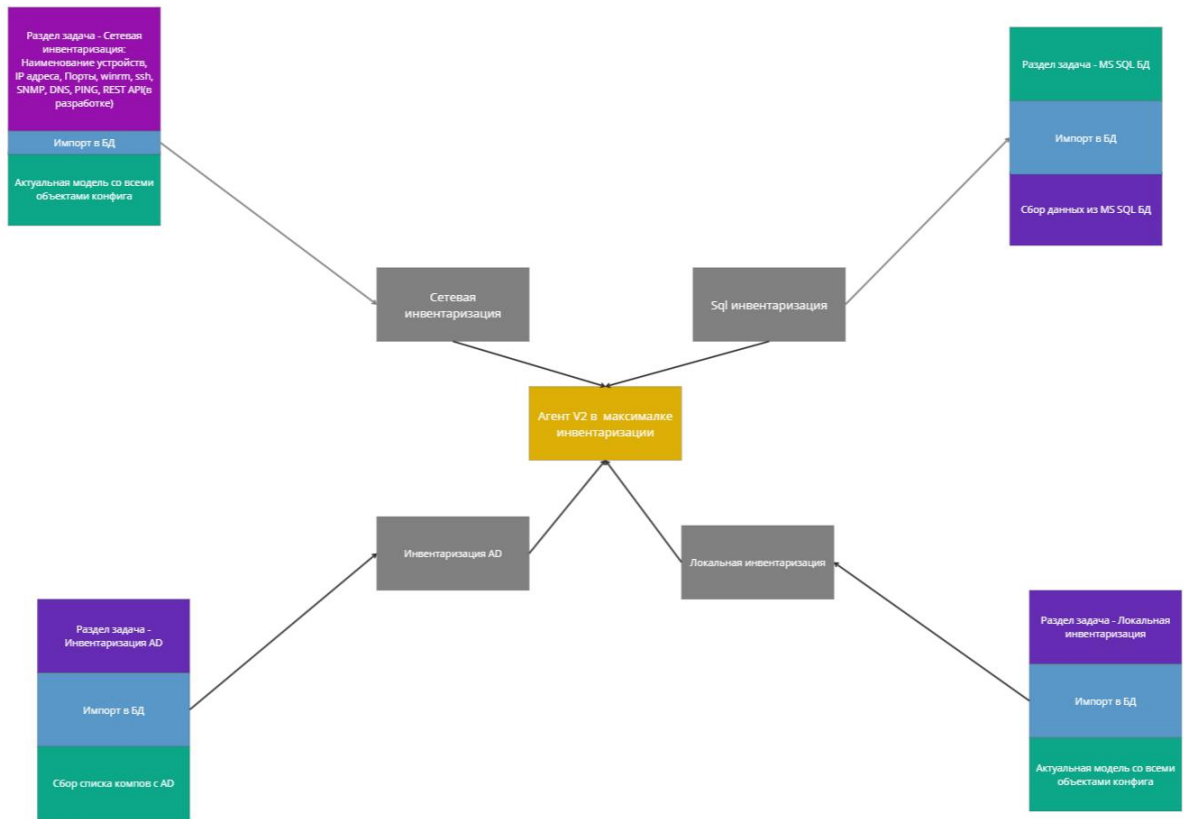


Для того чтобы прикрепить файл необходимо нажать на кнопку «Добавить файл». Перед вами откроется модальное окно. Затем вам необходимо перетащить файл в указанную область или выбрать из списка нажав на кнопку «Выбрать файл». Поля «Наименование», «Размер» и «Расширение» подгружаются автоматически из прикрепленного файла. Все файлы будут сохраняться в вашу прикрепленную Базу Данных. Затем нажимаем кнопку сохранить и ждем загрузки Файла.



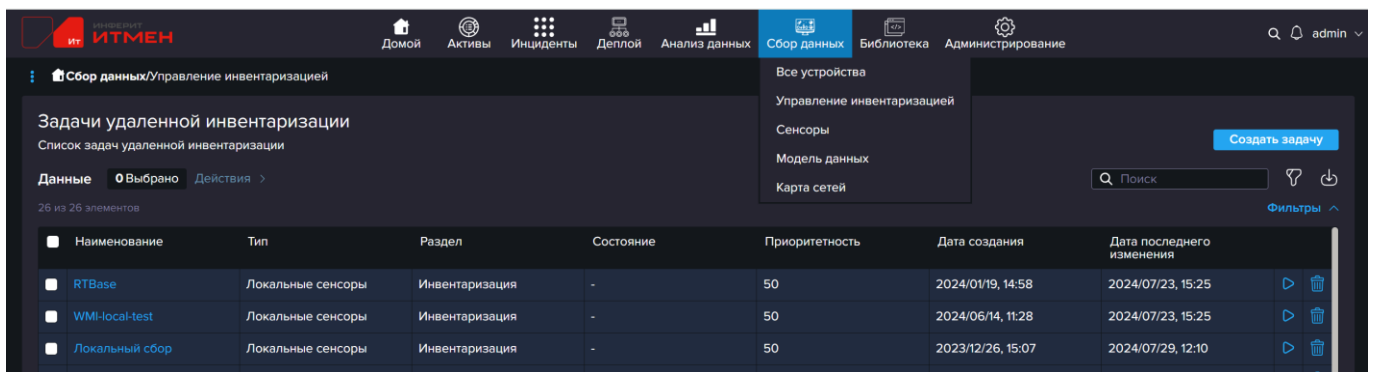
### 3.3.2 Управление инвентаризацией

Это раздел для настройки новых сенсоров по проведению инвентаризации с помощью персональных скриптов. Но прежде, чем перейдем к настройке инвентаризации рассмотрим схему что же собирает система.

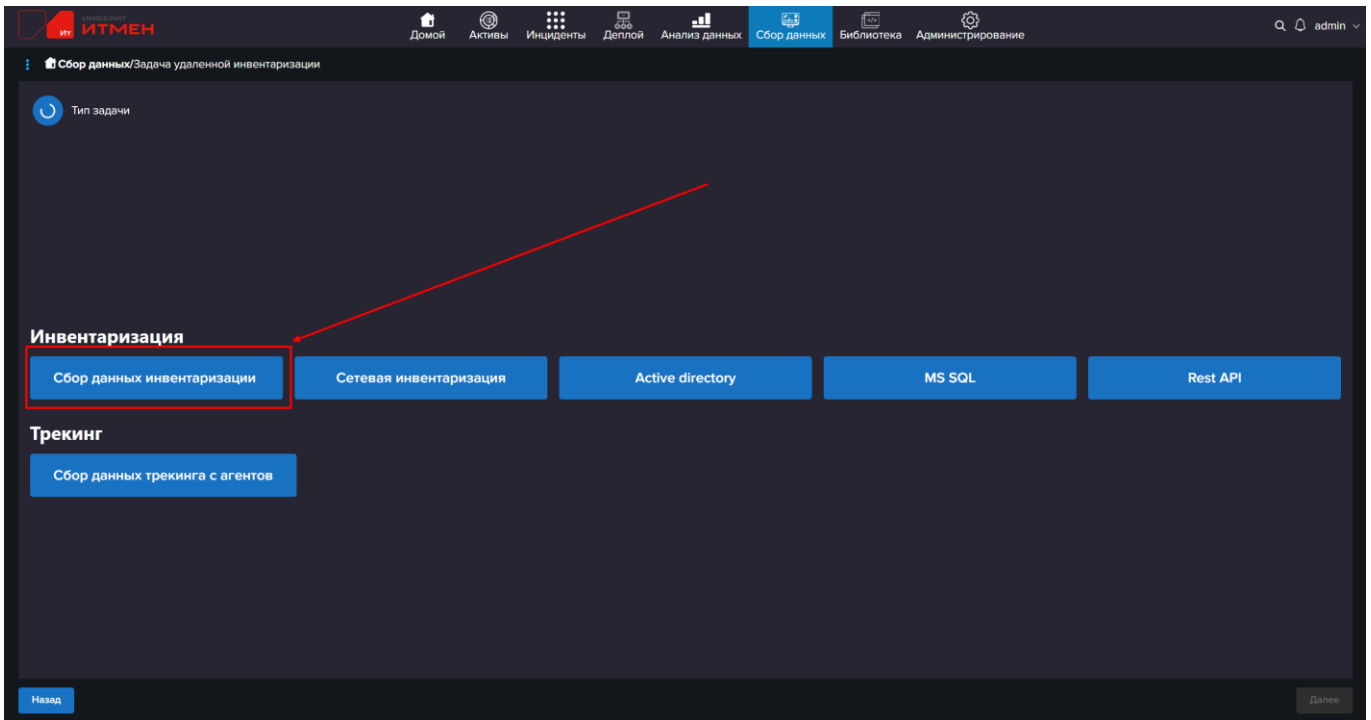


### 3.3.2.1 Рассмотрим настройку Сбора данных с агента.

Переходим в раздел Сбор данных – Управление инвентаризацией и нажимаем кнопку «Создать задачу».

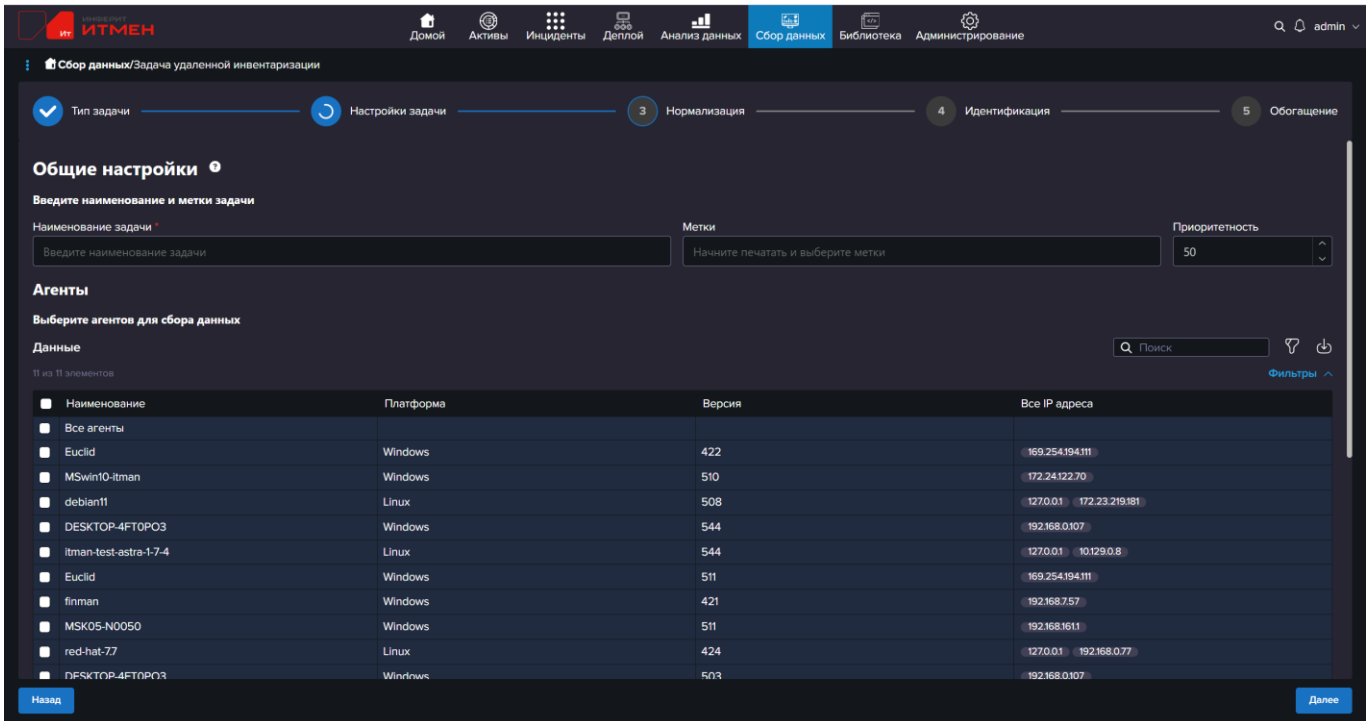


После чего система предложит нам выбрать тип задачи. Рассмотрим подробно создание задачи для типа «Сбор данных». Поэтому нажимаем на кнопку «Сбор данных инвентаризации с агента».



В редакторе создания задачи мы с вами видим основные данные о задаче, которые вы обязательно должны ввести. Поэтому заполняем поле «Наименование». Если вы хотите, чтобы эта задача была приоритетнее над всеми, то в поле «Приоритетность» необходимо выставить большую приоритетность.

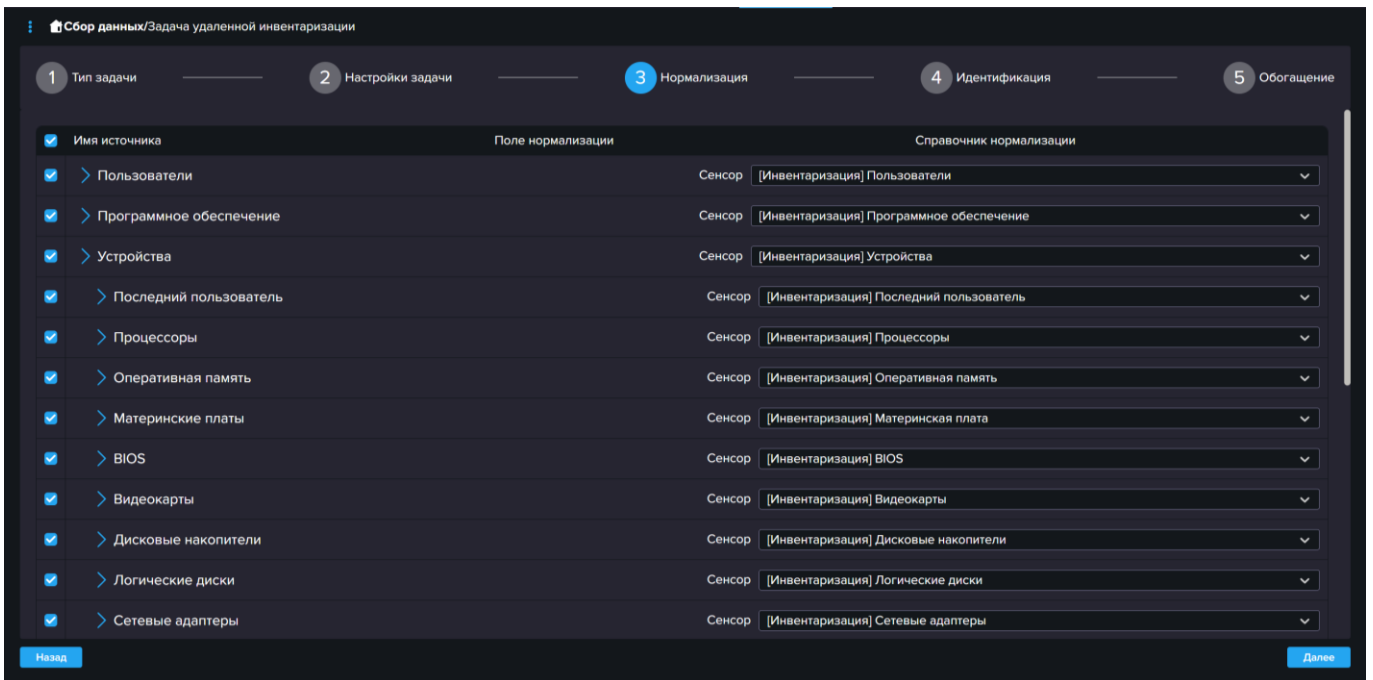
Далее в блоке «Агенты» выбираем свою машину, на которой был установлен агент.



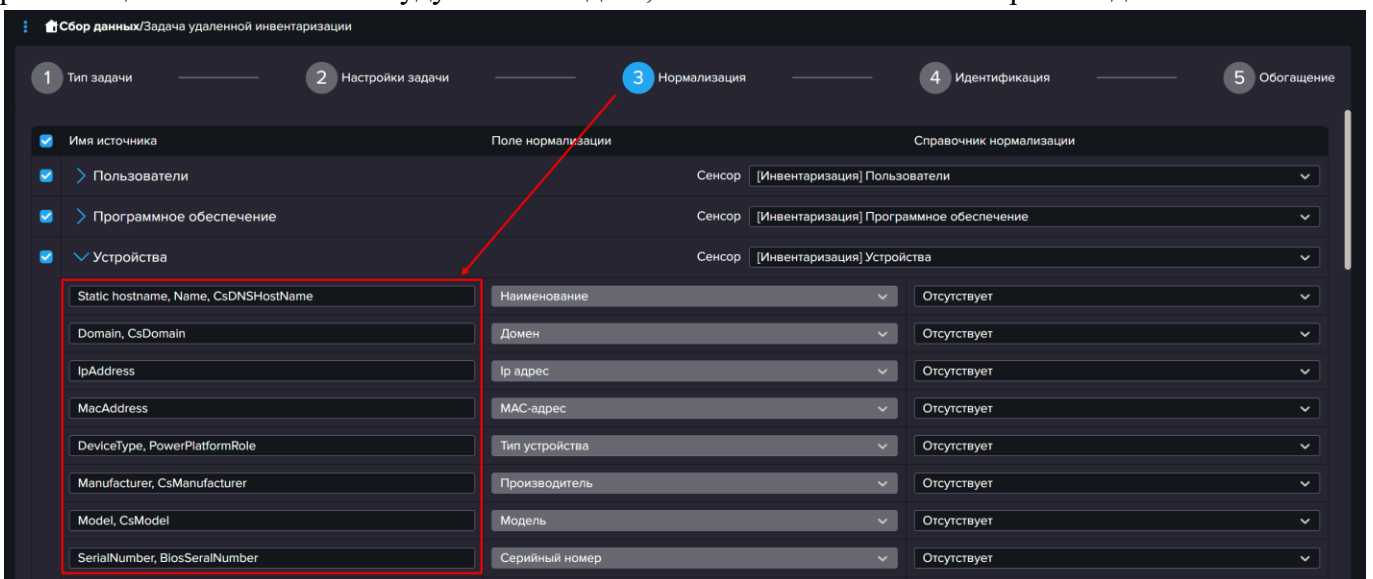
Если хотите изменить интервал расписания запуска, то можете отредактировать его под свои требования. Если пока нет такой необходимости, то можно оставить все по умолчанию и нажать «Далее». После чего переходим на шаг 3 Нормализация. На котором мы выбираем



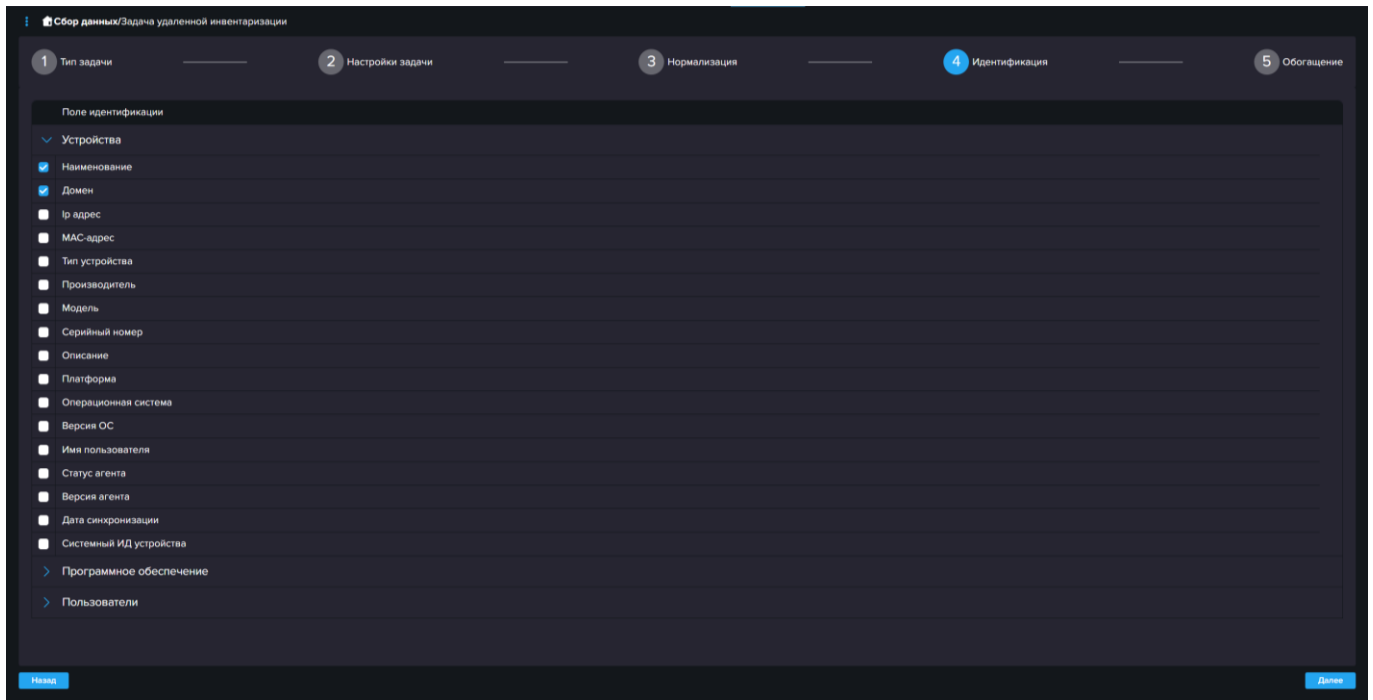
«Сенсоры» для более точного сбора данных. Рассмотреть создания «Сенсоров» можно в разделе [НИЖЕ](#).



Если вы будете использовать персональные сенсоры, которые создали самостоятельно то вам необходимо проверить, чтобы обозначения объектов в сенсоре совпадали с наименованием в нормализации. Если значения будут не совпадать, то система не сможет сохранить данные.



Если все выбранные сенсоры выбраны, то нажмем «Далее» и попадем на шаг 4 Идентификация. На этом шаге необходимо выбрать поля, по которым система будет распознавать уникальность вашего устройства.



По умолчанию стоит Наименование, но можно выбрать любое другое обозначение из списка, представленного в системе. Затем как значения будут выбраны нажимаем «Далее» и переходим на шаг 5 Обогащение.

Этот шаг необходим, когда мы хотим провести инвентаризацию машин с специальными тегами, которые были установлены при установке агента или ввести обогащение с помощью атрибутов или тэгов. Если не хотите вводить настройки обогащения, то можете сразу перейти к сохранению и нажать на кнопку «сохранить».

Если же хотите ввести настройки, то рассмотрим следующие два условия:

1. Атрибут устройства соответствует условию фильтра

- при выборе условия отображается:
  - выбора поля устройства
  - выбора типа фильтра
  - значение фильтра



Настройка обогащения

Введите наименование правила \*

Наименование правила

Настройка условий для правила

Атрибут устройства соответствует условию фильтра

Атрибут устройства Выберите условие

Наименование Начинается с WNR

Добавить условие

Настройка действий правила \*

Выставление вида устройства

Вид устройства Рабочая станция

Добавить действие

## 2. Тег агента соответствует условию фильтра

При выборе условия отображается:

- селектор выбора типа фильтра
- значение фильтра

Настройка обогащения

Введите наименование правила \*

Наименование правила

Настройка условий для правила

Теги агента соответствуют условию фильтра

Выберите условие

Начинается с WNR

Добавить условие

Настройка действий правила \*

Выставление вида устройства

Вид устройства Ноутбук

Добавить действие

После того как ввели данные нажимаем сначала кнопку «Применить». А затем нажимаем кнопку «Сохранить».

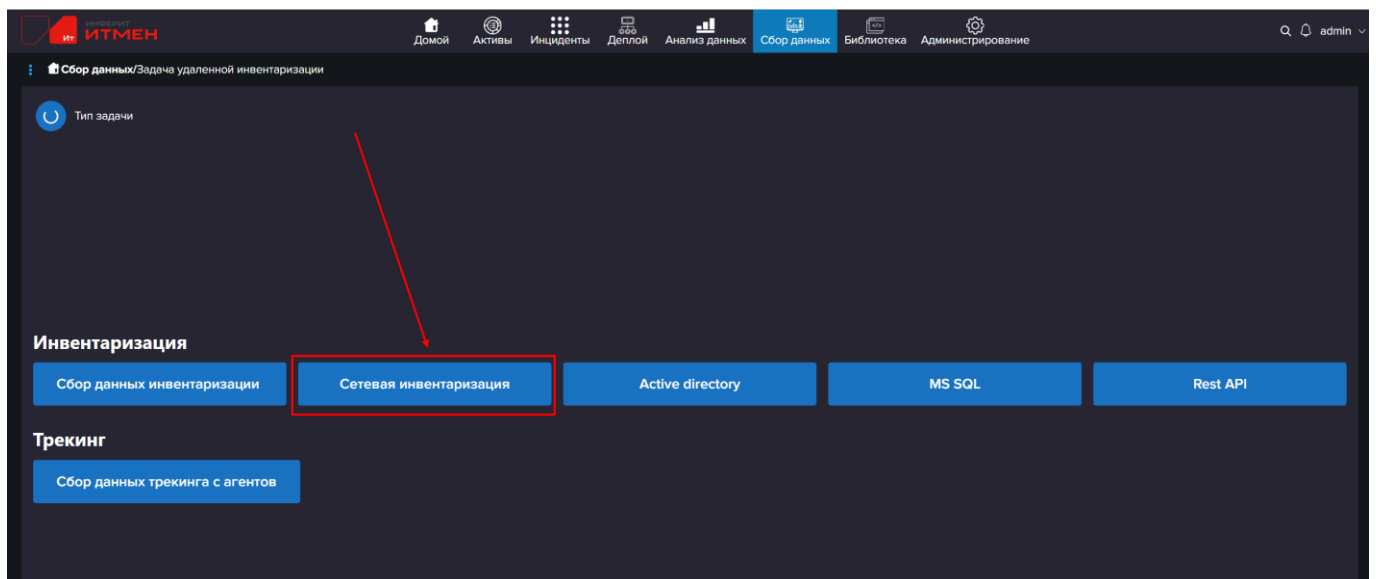
После сохранения задачи нам открылся список наших созданных задач.

### 3.3.2.2 Сбор данных Сетевой инвентаризации.

В блоке сетевая инвентаризация настраивается сканирование сети. Что же собирается при сканировании сети: Наименование устройств, IP адреса, Порты (идут как результат в собранных устройствах), winrm, ssh, SNMP, DNS, PING, REST API (в разработке).

Для этого вам необходимо будет чтобы хотя бы на одной машине стоял агент, у которого будет доступ к сети и его не будет ограничивать антивирус.

Выбираем блок «Сетевая инвентаризация».



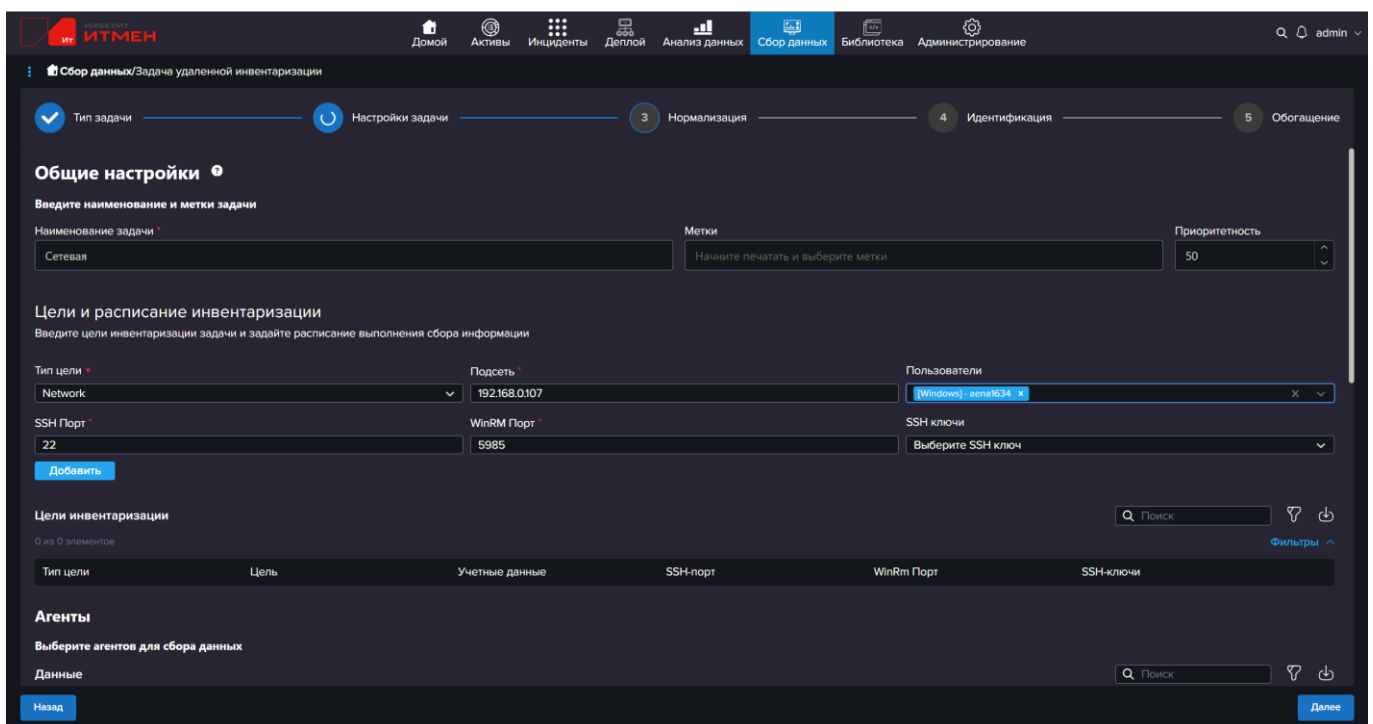
Для создания сетевой инвентаризации вам потребуется следующее:

- Учетные данные: для сбора информации с компьютеров в сети вам понадобятся учетные данные, которые имеют административные привилегии на этих компьютерах. Обычно это учетная запись с правами администратора. Эти учетные данные будут использоваться при настройке агента и при сборе информации с компьютеров. Для сбора данных с SNMP устройств вам потребуется community name.
- Знание подсетей: для сбора информации с компьютеров в сети вам необходимо знать IP-адреса компьютеров и подсетей, в которых они находятся. Это поможет вам определить, какие компьютеры нужно сканировать и какие подсети нужно обойти при сборе информации.

**Важно!** При проведении сетевой инвентаризации Агент будет добавляться в доверенные хосты, и если в вашем антивирусе не будет настроено разрешение для него, то антивирус просигнализирует это действие, как действие вредоносного ПО и удалит. Поэтому при проведении сетевой инвентаризации вам необходимо определить устройства, на которых будет стоять агент DiscoveryAgent\_\*\*\*Native для проведения сетевой инвентаризации и прописать его в исключения или в доверительные приложения. На остальных машинах, где нет необходимости проводить сетевую инвентаризацию, SQL и Active directory, можно ставить агент DiscoveryAgentLight\_\*\*\*Native.

Вернемся к заполнению задачи. В открывшемся окне заполняем поле «Наименование задачи», выбираем приоритетность задачи в поле «Приоритетность». Затем в блоке «Цели и расписание инвентаризации» заполняем наши инвентаризационные данные, с помощью которых агент сможет подключиться к сети. Значение в поле «Тип цели» оставляем по умолчанию, в поле подсеть указываем нашу подсеть или диапазон. В блоке пользователи выбираем те учетные данные, которые будут иметь доступ к тому блоку, который хотим собрать. Например, для сетевой инвентаризации – учетные данные сети, для SNMP учетные данные SNMP. В задаче можно сразу добавить несколько сетей со своими учетными данными.

Учетные данные для сетевой инвентаризации хранятся в разделе Администрирование Подразделы Учетные данные и SSH ключи, в зависимости от подключения нужно создать эти данные в этих справочниках. После того как данные будут введены нажимаем кнопку «Добавить» и наши данные появятся в таблице «Цели инвентаризации». И так можно добавлять несколько пользователей к каждой указанной сети.



После того как мы заполнили данные о подсетях необходимо выбрать Агента, который подключен к этой сети.

После того как вы заполните все формы данными нажимаем на кнопку “Далее” и переходим на шаг 3 Нормализация. Далее этот шаг и все остальные шаги настраиваются аналогично задачи «Сбора данных с агента».

### 3.3.2.3 SQL

При использовании SQL базы данных можно настроить импорт данных в систему с помощью SQL запросов. Для этого необходимо знать следующие данные:

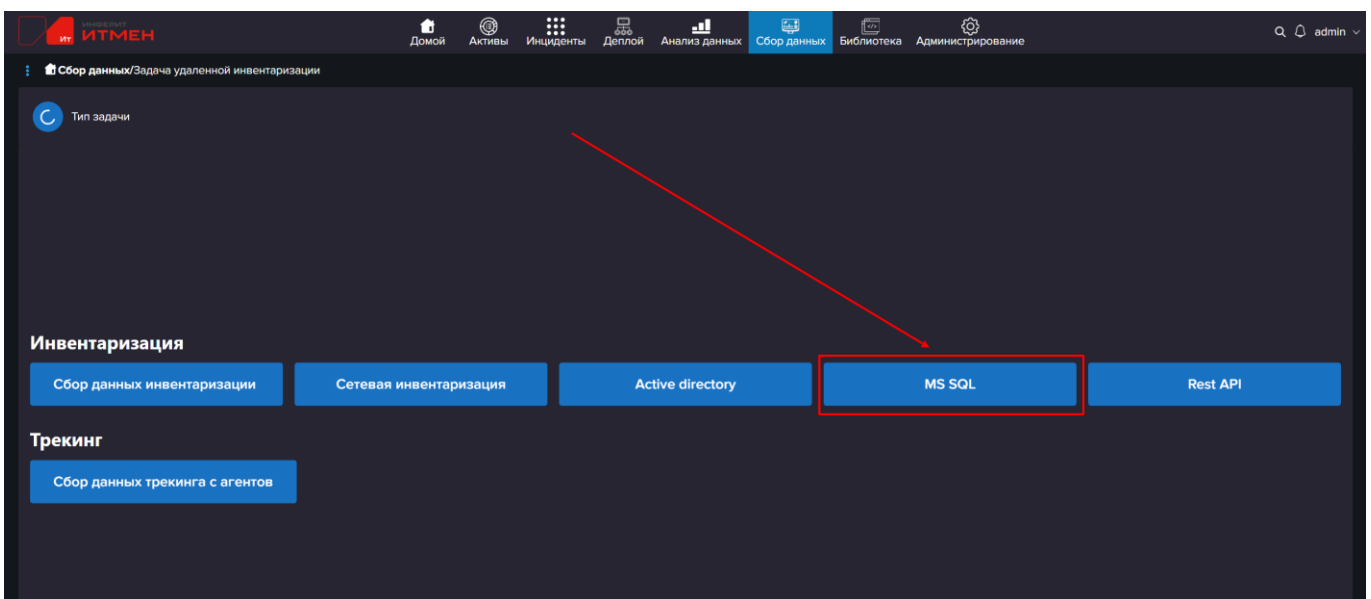
Наименование сервера SQL: это может быть IP-адрес или доменное имя сервера, на котором размещена база данных.

Дата документа: 29.08.2024

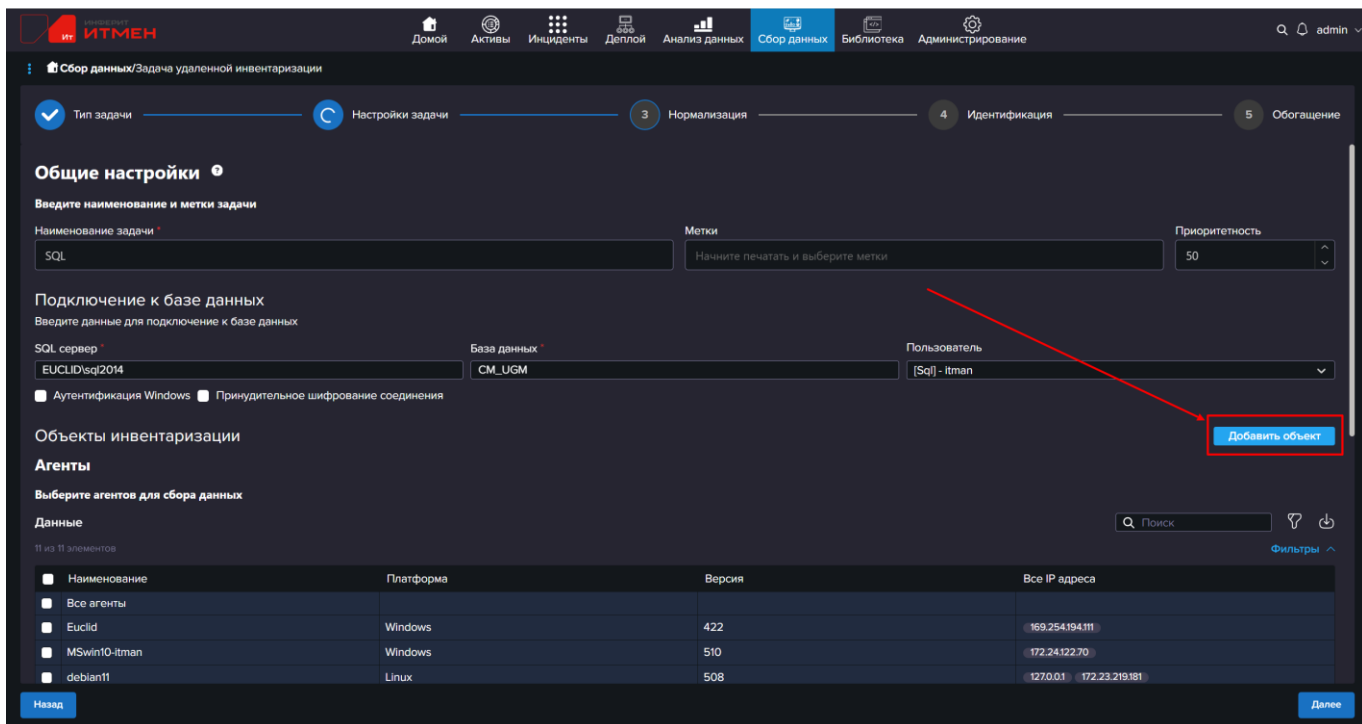
Версия системы: 5.5

1. **Наименование базы данных:** это имя базы данных, из которой вы хотите импортировать данные.
2. **Логин и пароль:** это учетные данные, которые позволяют получить доступ к базе данных.
3. После того как вы получили эти данные, вы можете написать SQL запросы для импорта данных из базы данных в систему. Например, вы можете написать запрос на выборку данных из таблицы и вставку этих данных в таблицу в системе.

Если вы хотите выполнить импорт данных из своей СУБД по устройствам, то вы можете выбрать устройство, на котором расположена база данных, и перейти во вкладку "Удаленная инвентаризация". Затем нажать на кнопку «Создать задачу» и затем выбрать SQL в качестве источника данных и настроить подключение к базе данных, используя вышеуказанные данные. После этого вы можете выполнить импорт данных из базы данных в систему с помощью SQL запросов.



- Затем откроется окно для ввода данных для настройки.
- В открывшемся окне вводим наименование задачи и даны о SQL сервере.
- В блоке Объекты инвентаризации нажимаем на кнопку «Добавить объект» — это необходимо выбрать для того, чтобы задача поняла какие объекты мы будем инвентаризировать.



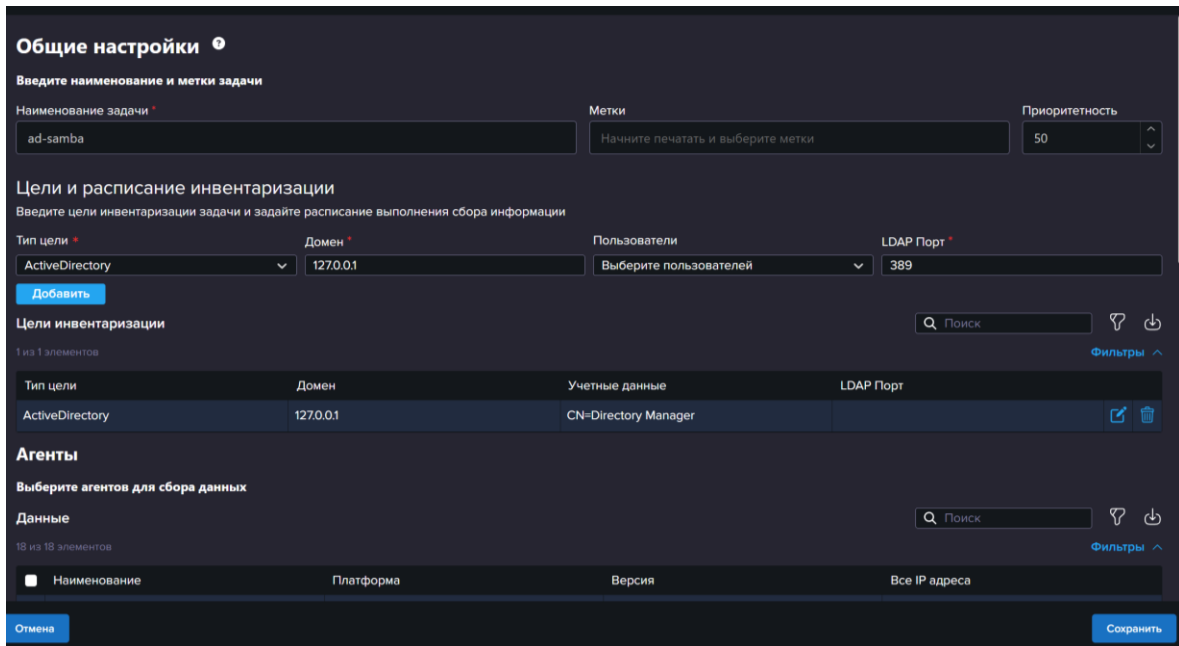
- Затем как появилось поле выбираем из выпадающего списка сам объект инвентаризации и в конце около этого поля нажимаем на кнопку «Добавить».
- Затем как настроили скрипты нажимаем Далее.
- После чего попадаем на важный шаг «Нормализации» для этого типа задач необходимо выбрать SQL сенсоры около каждого объекта. Как это сделать и дальнейшие шаги расписаны в [«сборе данных»](#).

### 3.3.2.4 LDAP

Инвентаризация Active Directory, FreeIPA, Samba AD происходит аналогично Сетевой инвентаризации:

- Переходим в Удаленную инвентаризацию
- Нажимаем Создать задачу
- Выбираем LDAP
- В открывшемся окне вводим Наименование задачи
- Затем вводим Учётный данные
- Потом заполняем Цели:

Для этого выбираем цель ActiveDirectory (название не влияет на платформу, которую будем инвентаризировать, это может быть и FreeIPA, и Samba AD), заполним домен или IP, где хранятся инвентаризируемые данные, после выбираем пользователя (если пользователя нет необходимо добавить) и в конце вводим LDAP порт.

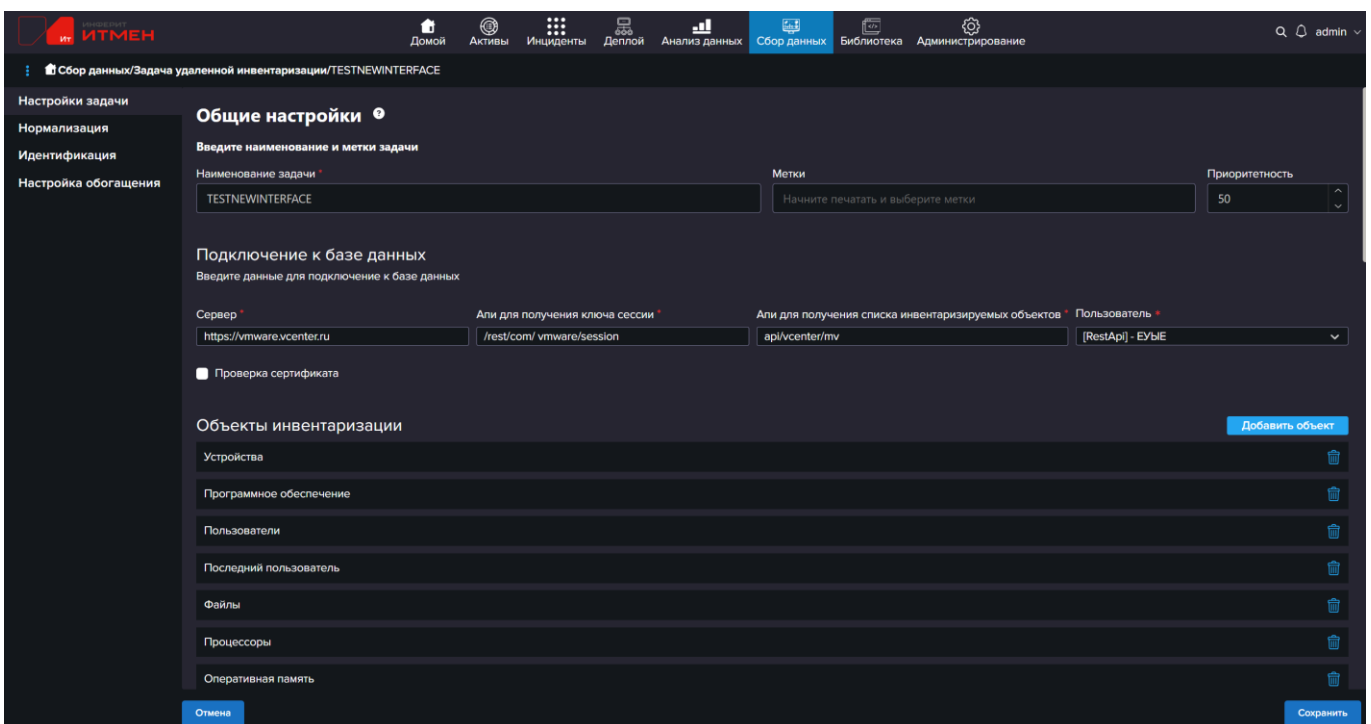


- Проверяем что все заполнено корректно и нажимаем кнопку «Далее»
- Открылся шаг Нормализации
- Заполняем шаги аналогично «Сбору данных с локальных агентов»

Затем нажимаем кнопку «Сохранить».

### 3.3.2.5 REST API

Для сбора данных с VMware vCenter в системе есть тип задач REST API. Чтобы настроить такой тип задачи необходимо перейти в «Сбор данных» - «Управление инвентаризацией». Затем нажать кнопку «Создать задачу» и выбрать значение «REST API».



Для настройки подключения вам понадобятся данные:

Дата документа: 29.08.2024

Версия системы: 5.5



- Адрес сервера – указываем в поле сервер ( Например: <https://vmware.vcenter.ru>)
- Апи для получения ключа – Например: `/rest/com/vmware/session`
- Апи для получения списка инвентаризируемых объектов – Например: `api/vcenter/mv`
- Пользователь – в этом поле выбираем пользователя, который имеет доступ к этим записям. Если пользователя нет, то его можно добавить сразу в поле или перейти в Администрирование-Учетные данные.

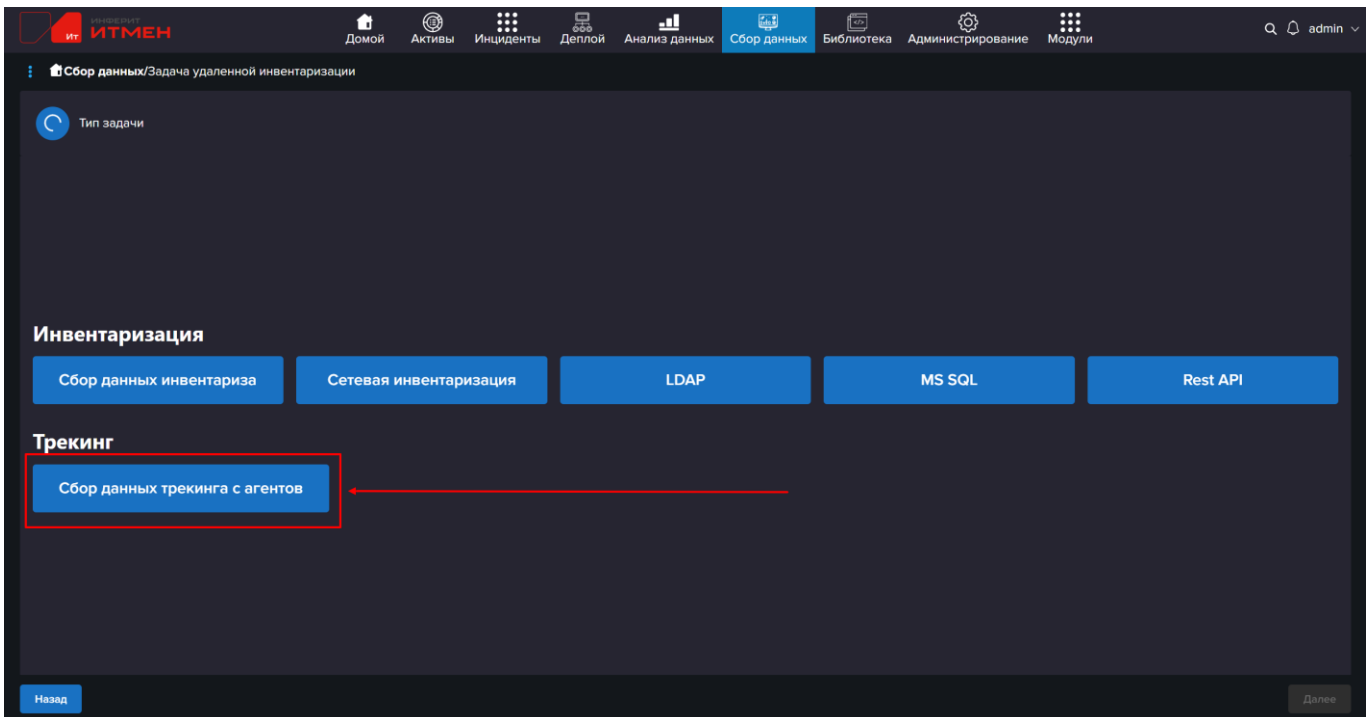
После настройки подключения нажимаем кнопку «Добавить объекты» и выбрать объекты, которые будут участвовать в инвентаризации.

Затем как данные для подключения будут введены и выбраны объектов переходим к выбору агентов. Выбираем необходимый агент и нажимаем кнопку «Далее». В разделе нормализации вам необходимо отключить лишние значения, которые у вас не присутствуют в вашем запросе и около необходимых запросов выбрать Сенсоры с нужными запросами под вашу базу.

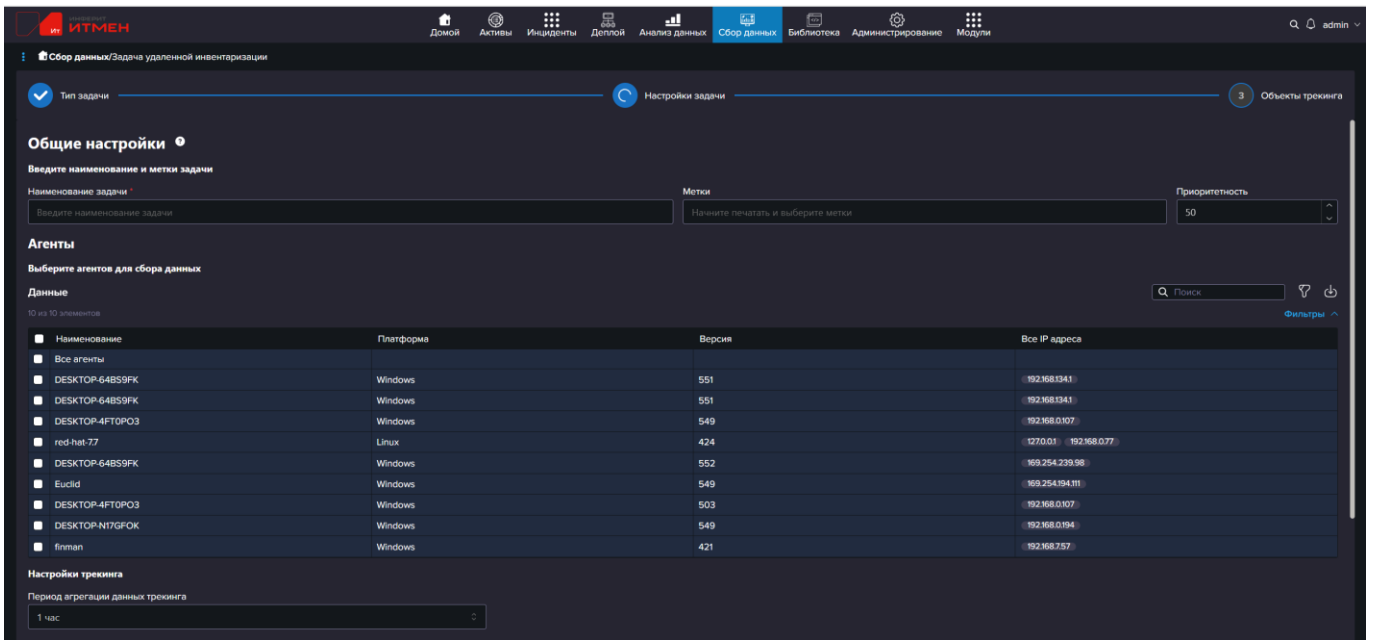
### 3.3.2.6 Сбор данных трекинга с агента

В этом типе задачи будут создаваться задачи для сбора трекинговых данных, например, чтобы отслеживать кто и сколько пользуется той или иной программой.

Для этого нажимаем кнопку «Создать задачу» и выбираем тип «Сбор данных трекинга с агента»

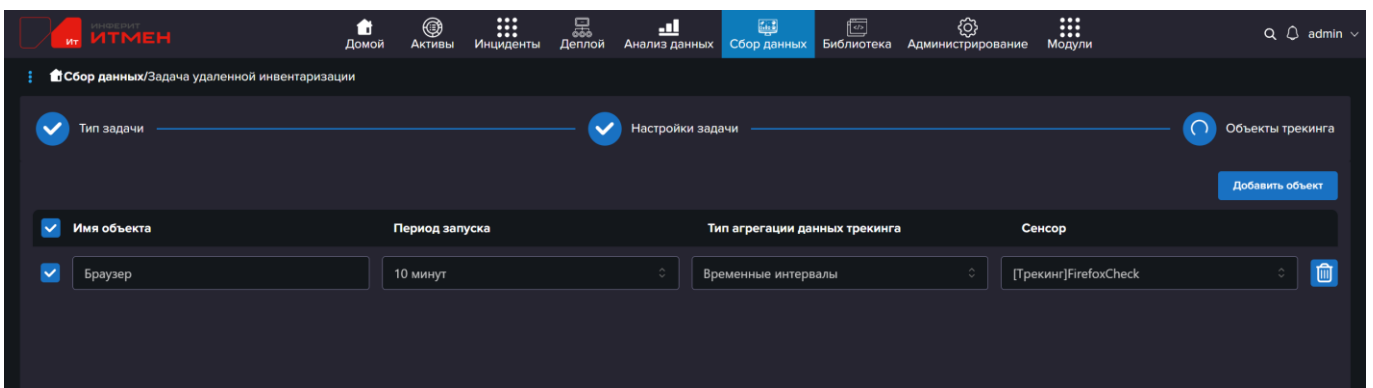


В открывшейся задачи заполняем поле «Наименование». Поле «Метки» и «Приоритетность» заполняем по необходимости. Затем переходим к выбору агента, которое будем проверять. После выбора агента необходимо выбрать период агрегации. Период агрегации означает как часто будут объединяются данные сенсоров в один архив.



Далее заполняем расписание. Желательно чтобы расписание не было меньше периода агрегации. После того как все будет заполнено нажимаем «Далее».

Мы перешли на шаг «Объекты трекинга». На этом шаге мы будем выбирать наши сенсоры для трекинга (требование для написания сенсора описано после описания задачи трекинга). Для этого мы указываем Имя объекта, затем выберем «Период запуска» (это означает как часто будет запускаться на агенте сенсор проверки), затем выбираем «Тип агрегации данных трекинга» (он будет зависеть от того, что будет проверять сенсор), далее выбираем наш сенсор (начните писать в поле имя сенсора чтобы быстрее найти необходимый сенсор).



Заполнили первый объект, если в этой задаче необходимы несколько объектов, то нажимаем кнопку «Добавить объект». После чего у вас появится новая строка добавления объекта, в которой добавляем объект так же, как и первый.

Затем нажимаем кнопку «Сохранить». Карточка создания закрывается и переходим в общий список задач.

Отображение результатов будет в [Отчетах по программному обеспечению](#).

## Требования для написания сенсоров трекинга

Сенсор должен возвращать данные с типом «Справочник формат ключ-значение» или если возврат данных больше одного результата «Список справочников формат ключ-значение».

Обязательные поля результате выполнения скрипта:

- "Value : " результат сбора сенсора (приходит 0 или 1)
- "Owner : " Имя пользователя
- "TrackingName : Уникальное название трекинга";
- "TargetName : ./ описание объекта трекинга ";
- "ValueType : Interval"; или "ValueType : Seconds"; ValueType : Minutes";
- "OwnerType : Users"; оставить по умолчанию

Пример скрипта для сбора данных трекинга:

```
$isChromeStartted = if (Get-Process -Name "chrome" -ErrorAction SilentlyContinue) {1} else {0}; (может быть любое значение на ваше усмотрение)
```

```
Write-Host "Value : " $isChromeStartted; (обязательное поле)
```

```
$UserName = (Get-Process -IncludeUserName -Name "chrome" | Select-Object -First 1).UserName;
```

```
Write-Host "Owner : " $UserName;
```

```
Write-Host "TrackingName : Chrome";
```

```
Write-Host "TargetName : ./Chrome";
```

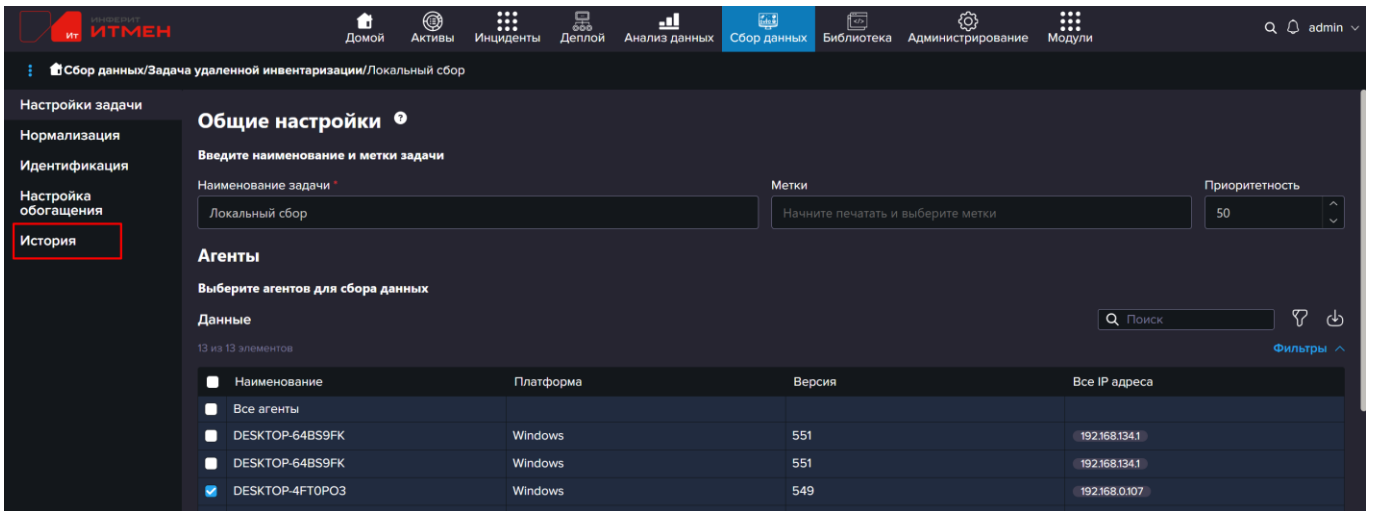
```
Write-Host "ValueType : Interval";
```

```
Write-Host "OwnerType : Users";
```

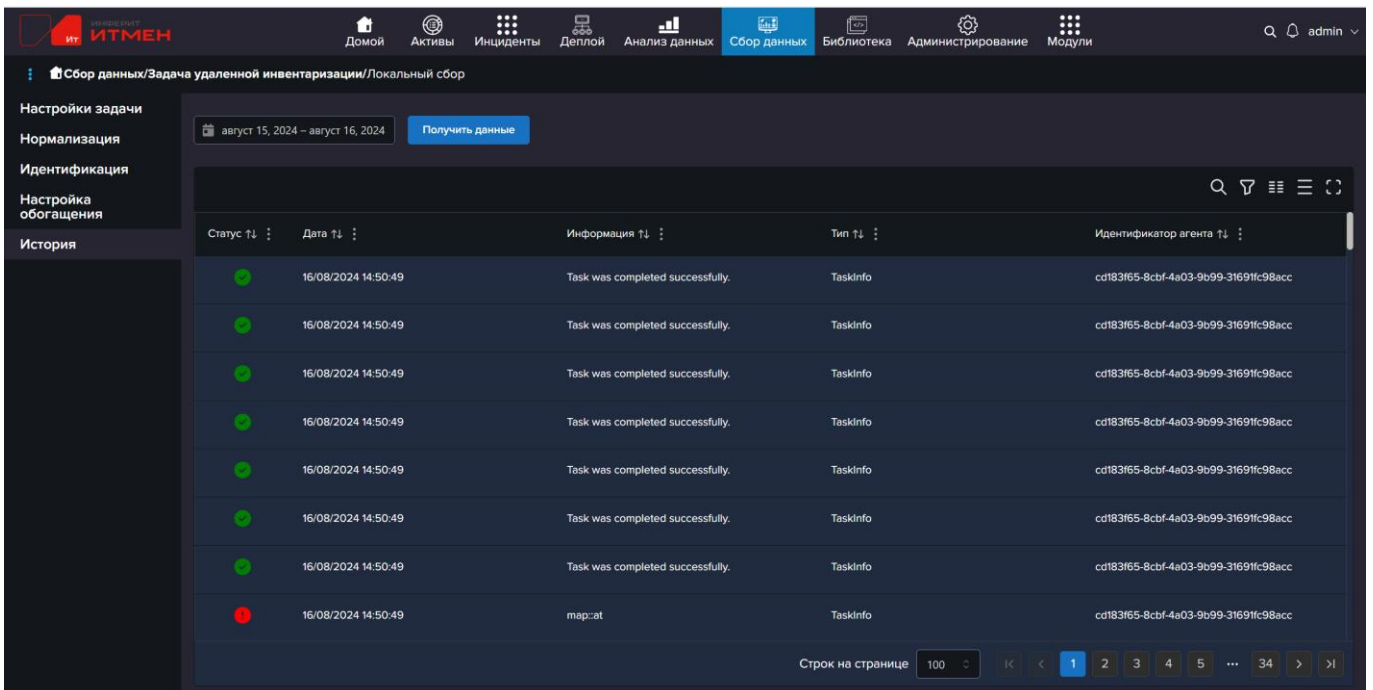
Для написания своего сенсора переходим в раздел [Сенсоры](#)

### 3.3.2.7 История

В каждой задаче в карточке редактирования есть вкладка История, в которой отображены статусы как задача отработала на агенте. Для просмотра истории откроем необходимую задачу в режиме редактирования и выберем вкладку «История».



На открывшейся странице отображены статусы выполнения задачи на агенте.



Зеленый кружок с галочкой – статус что задача отработала успешно.

Красный кружок – задача до агента дошла не корректная (возможно неправильно собран сенсор или указаны данные нормализации или агент старой версии что не смог обработать задачу новой версии).

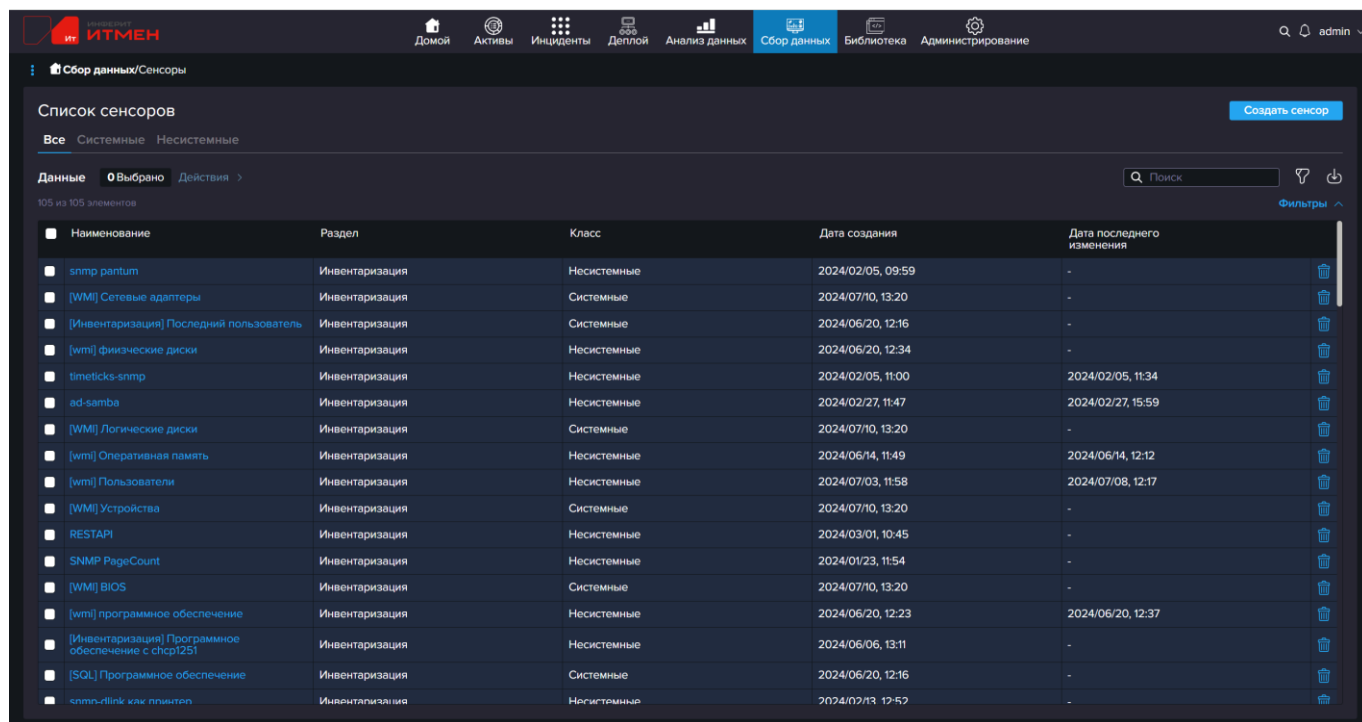
Так можно изменить временной интервал в фильтре и запросить данные с учетом этого интервала нажав на кнопку «Получить данные».

### 3.3.3 Сенсоры

Этот раздел используется для самостоятельной настройки скриптов сенсоров при инвентаризации. Что поможет улучшить и персонализировать отображения данных после нормализации при проведении инвентаризации. Например, вы хотите собирать какие-то данные с

ваших компьютеров, и вы знаете где они находятся и у вас есть скрипт для отображения этих данных, то вы можете создать свой сенсор.

### Раздел редактора сенсоров.

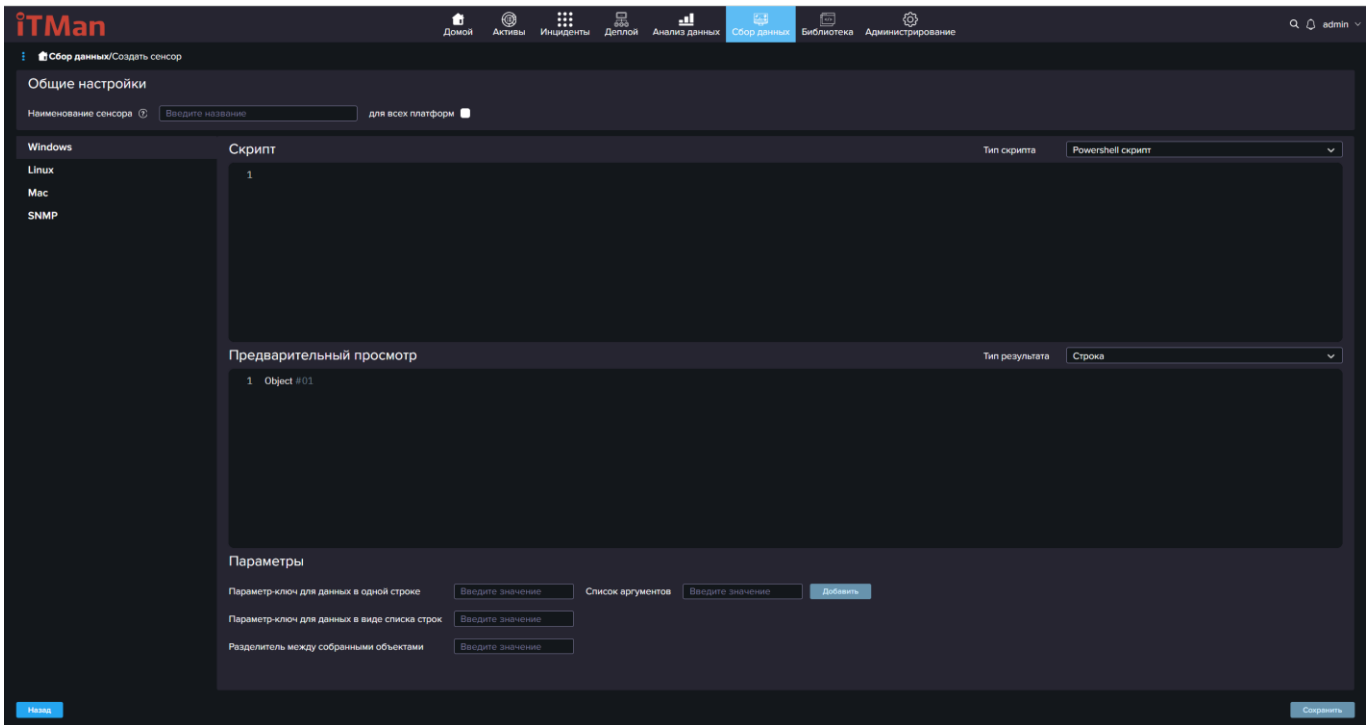


В системе представлены два типа сенсоров системные и несистемные:

- Системные — это сенсоры, которые созданы по умолчанию в сборе данных, для сбора информации с устройств. Так же системные сенсоры можно отредактировать с учетом каких то персональных настроек вашей системы, но если вы допустите ошибку, то у вас будет возможность откатится до стандартное сенсора, который создан по умолчанию.
- Несистемные сенсоры – это полностью персонализированные сенсоры, которые вы создаете самостоятельно. Чтобы создать персональный сенсор, необходимо будет нажать на кнопку «Создать сенсор». После чего у вас откроется окно создания сенсора. Где необходимо будет ввести «Наименование» и сам код сенсора в зависимости от платформы, которую вы выберете: Windows, Linux.

### Как создать сенсор.

Для это вам необходимо перейти в раздел Сбор данных – Сенсоры. В открывшемся окне нажимаем на кнопку «Создать сенсор». После система откроет редактор сенсоров.



В редакторе сенсоров есть две области:

2. Область Общих настроек
3. Область Редактора скриптов

В общих настройках мы только указываем наименование и будет ли этот скрипт использоваться для всех платформ. Функция для всех платформ необходима тогда, когда скрипт будет аналогичный на всех платформах и не зависеть от синтаксиса. Если же у нас будут разные скрипты для каждой платформы, то мы уже переходим в область «Редактора скриптов».

В редакторе скриптов представлены 4 платформы:

1. Windows
2. Linux
3. Mac (в разработке)
4. SNMP

Рассмотрим на примере Windows скрипта. Для этого нажимаем на значение Windows. Далее в поле скрипт мы выбираем Тип скрипта в зависимости что мы будем собирать.

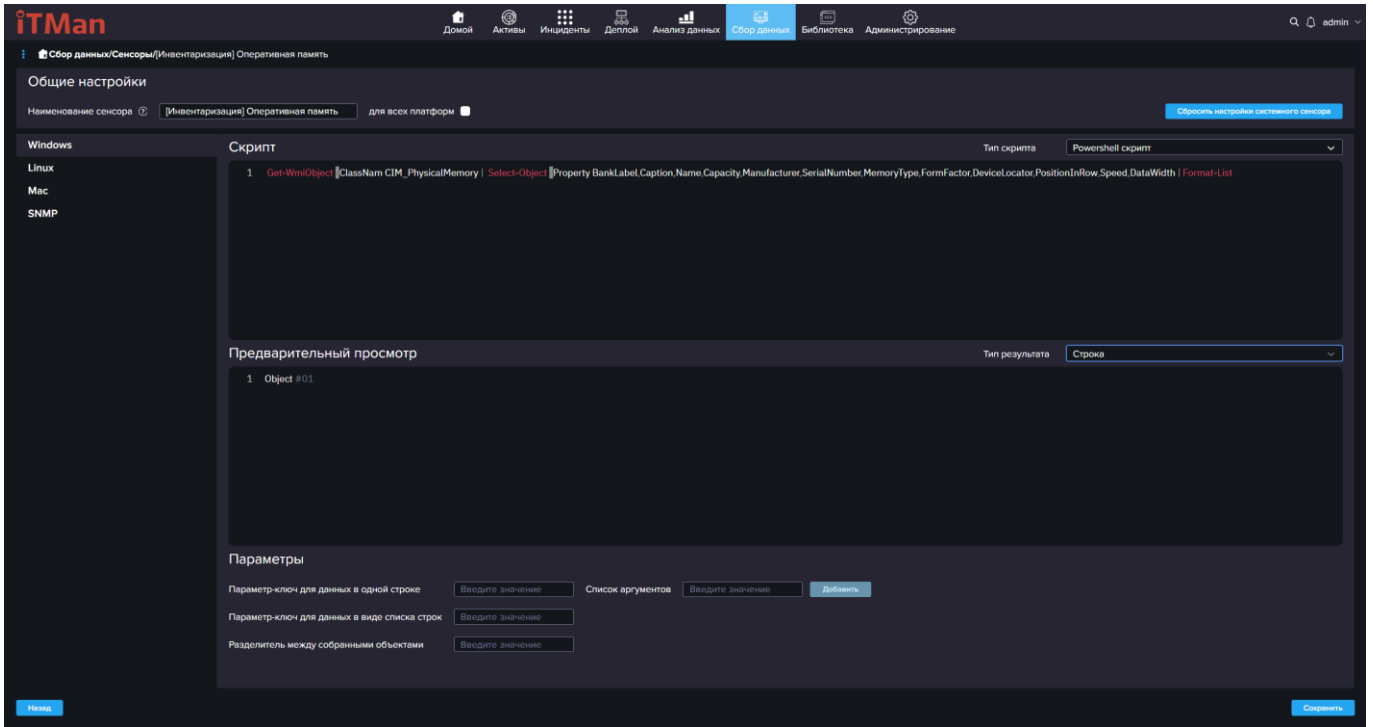
Типы скрипта:

1. Powershell скрипт
2. Shell скрипт
3. Внутренний скрипт
4. SQL скрипт

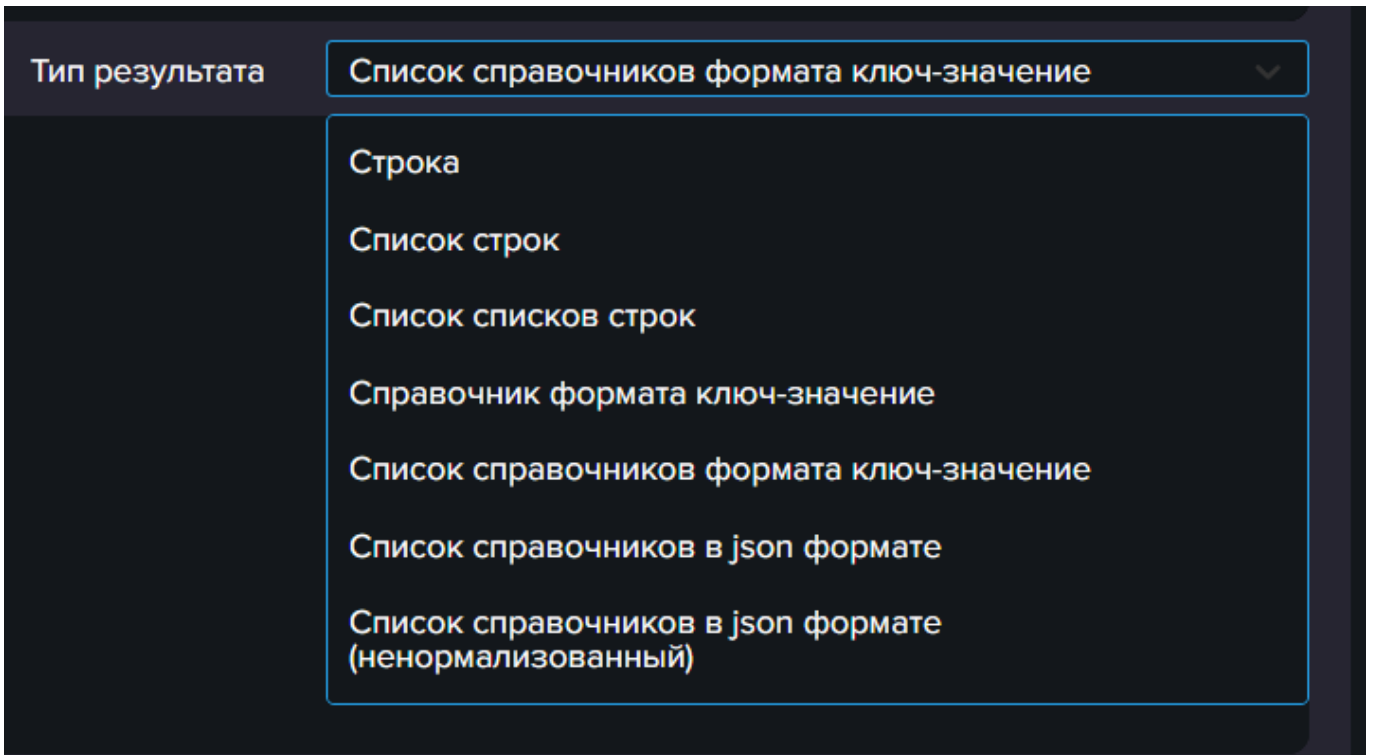
После того как мы выбрали тип переходим к написанию скрипта. Сам скрипт мы пишем в редакторе поля «Скрипт».

Дата документа: 29.08.2024

Версия системы: 5.5



Затем, чтобы наши данные сформировались и были отправлены в систему необходимо выбрать значение «Тип результата».



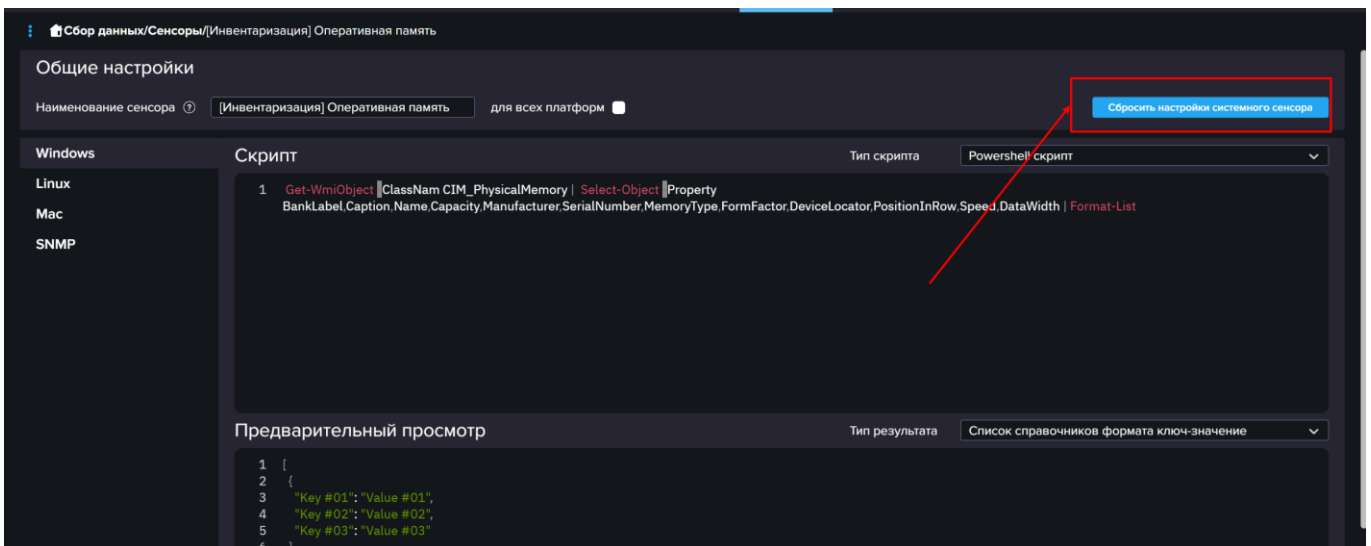
В нашем скрипте из примера мы выбираем «тип результата»: «Список справочников формата ключ-значение», чтобы данные в обрести «Предварительный просмотр» выглядели следующим образом:

## Предварительный просмотр

```
1  [  
2  {  
3    "Key #01": "Value #01",  
4    "Key #02": "Value #02",  
5    "Key #03": "Value #03"  
6  },  
7  {  
8    "Key #01": "Value #04",  
9    "Key #02": "Value #05",  
10   "Key #03": "Value #06"  
11  }  
12 ]
```

После того как все данные будут введены в разделе для Windows мы нажимаем кнопку «Сохранить».

Важно! Если мы переключите платформу и не сохраните ваши внесенные данные, то они не будут сохранены. Также важно у системных сенсоров есть возможность откатиться к первоначальному виду сенсора с помощью кнопки «Сбросить настройки системного сенсора»

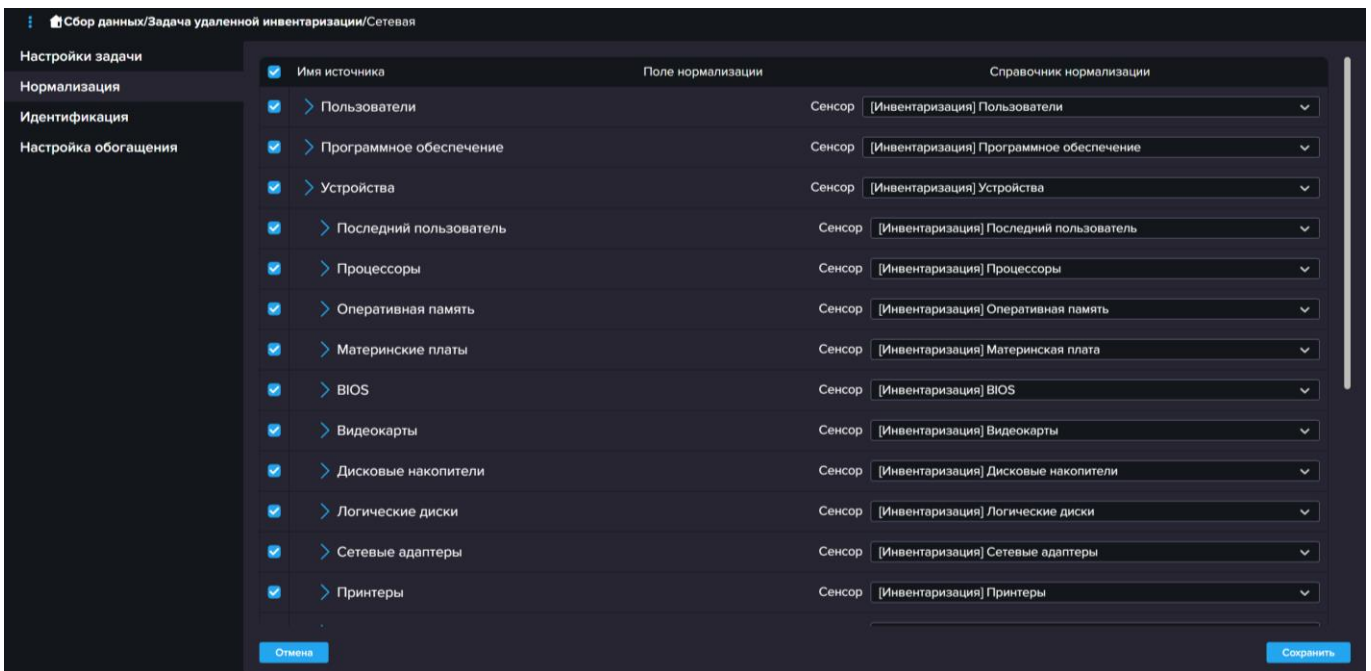


Где же выбрать наш новый сенсор в приложении.

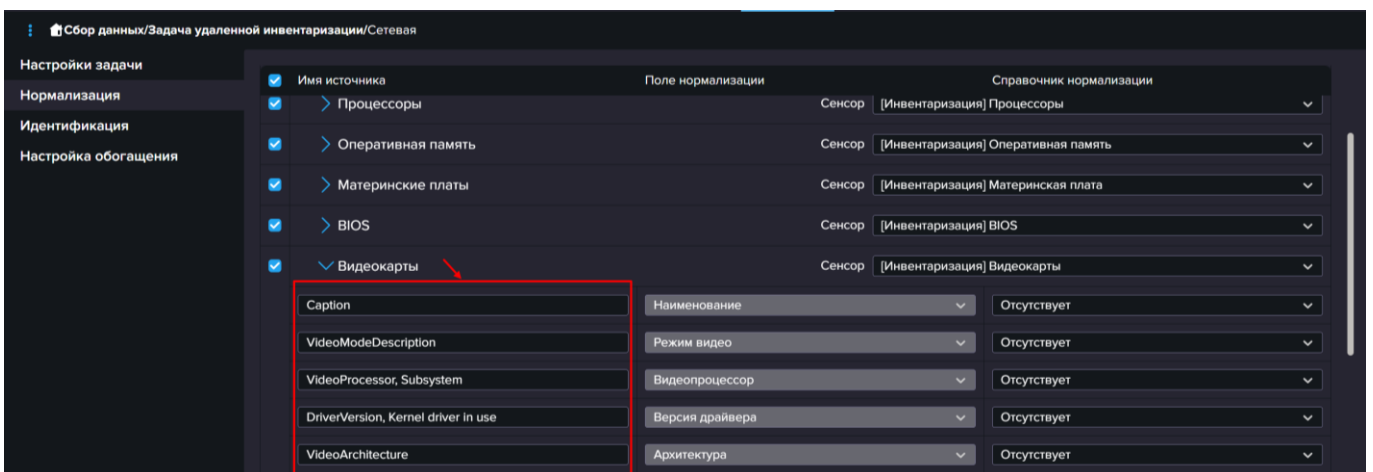
Для использования нового сенсора вам необходимо перейти в раздел Сбор данных – Управление инвентаризацией. Затем открыть существующую задачу Сетевой инвентаризации или создать новую (в случае создания новой вам необходимо дойти до шага Нормализации).



Например, рассмотрим уже существующую задачу. Для этого открываем задачу и переходим на вкладку Нормализации.



Как мы видим из скриншота около каждой области выбран свой сенсор. Если вы отредактировали название параметров в своем сенсоре, то вам также необходимо прописать эти параметры. Рассмотрим на примере Видеокарты, раскрываем область Видеокарты и в первом столбце вводим необходимые параметры из сенсора.



Название Полей нормализации, пока не изменяются. Поэтому вы также можете в своем скрипте оставлять стандартные названия из Нормализации задачи.

### 3.3.4 Модель данных

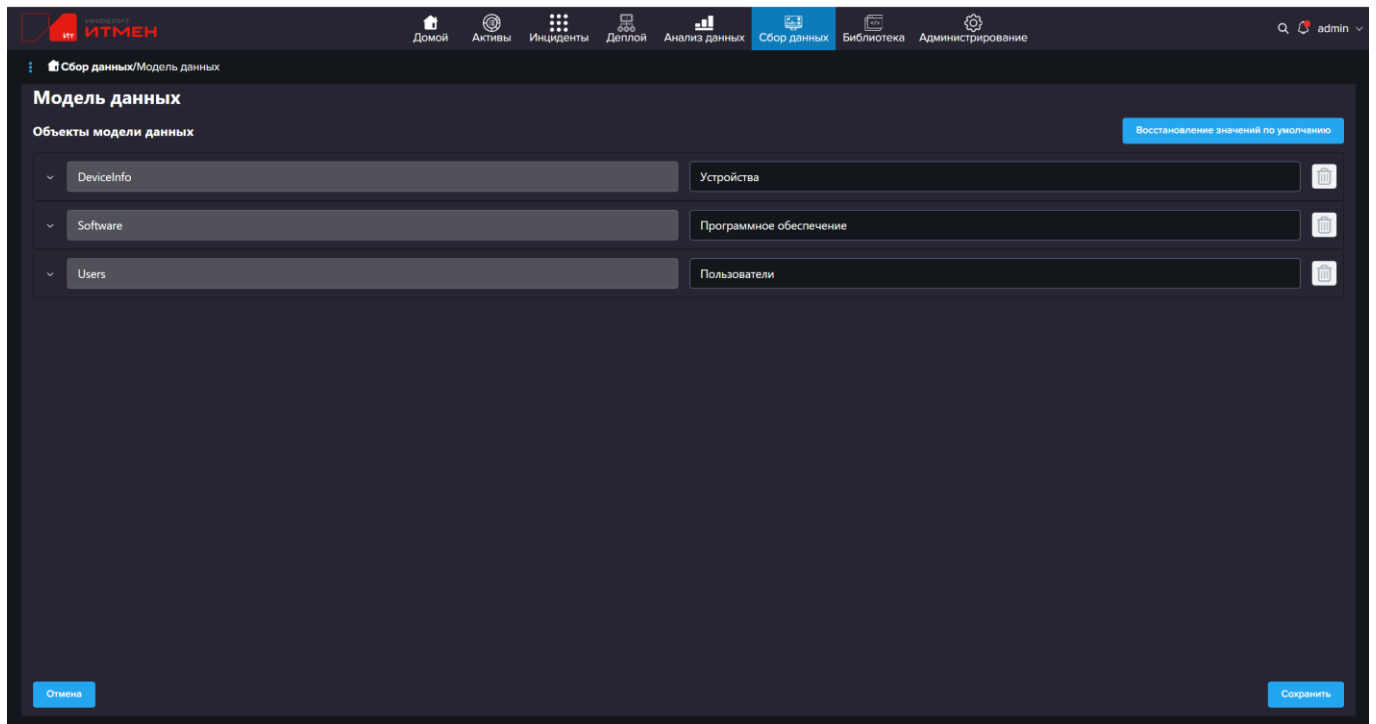
В разделе модель данных отображены все поля устройств, которые участвуют в инвентаризации. В этом разделе представлены «Объекты» и «Поля». С помощью них можно добавить дополнительные данные в инвентаризацию.

**Важно!** После добавления или редактирования объекта или поля, необходимо сначала проверить уже готовые сенсоры или добавить новый сенсор, а после отредактировать задачи.

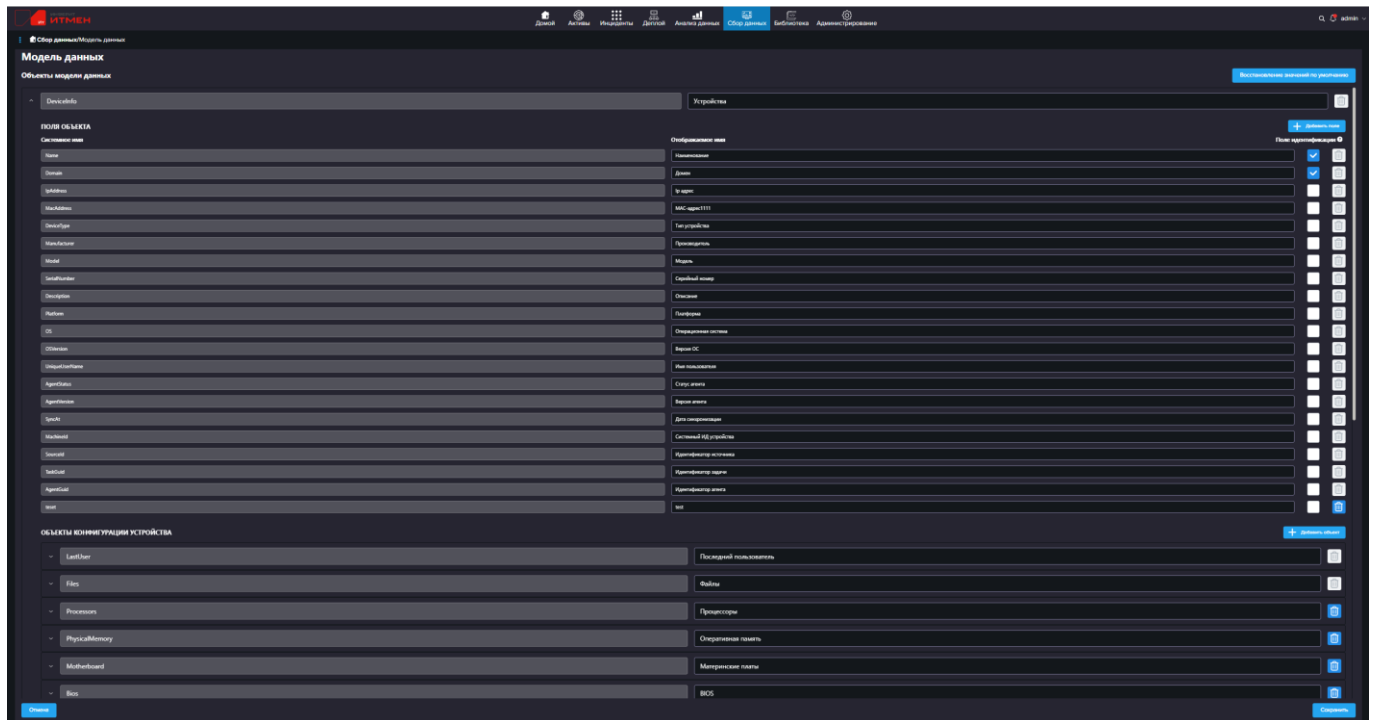
А пока рассмотрим подраздел «Модель данных».

В нем представлены три главных раздела это:

- Устройства
- Программное обеспечение
- Пользователи



Раскроем один из объектов и видим, что внутри каждого объекта представлены: «Поля объектов» и «Объекты конфигурации устройства».



В системе отображаются системные поля и поля, которые вы можете добавить самостоятельно. Системные поля удалять или редактировать нельзя, чтобы не нарушить работу инвентаризации. Поля, которые добавлены самостоятельно можно редактировать и удалять, но если вы настроили эти поля в задачах, то при изменении не забудьте отредактировать сенсор и задачи, где эти поля были использованы. Так как при изменении задача может отработать не корректно, поэтому после изменения задача не будет перезапущена.

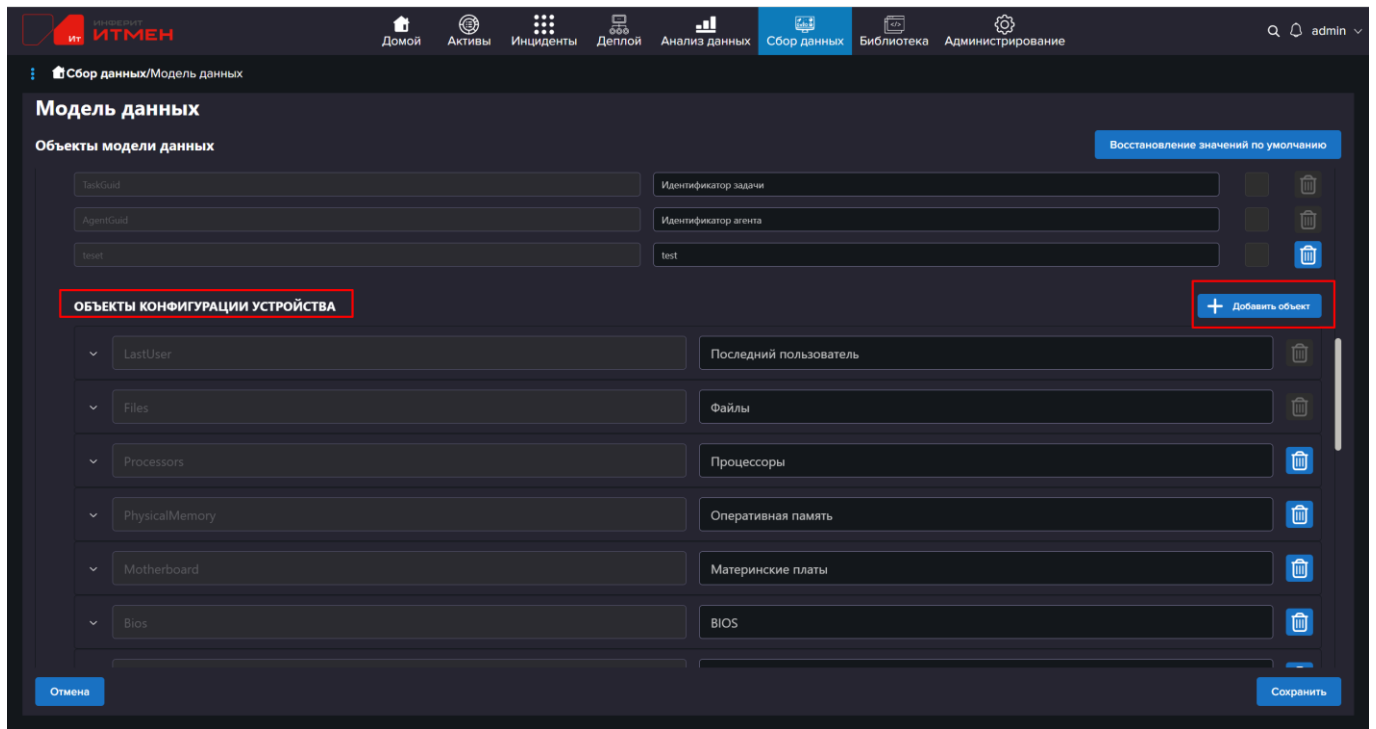
Где же можно посмотреть добавились ли наши поля или нет?

Поля можно посмотреть:

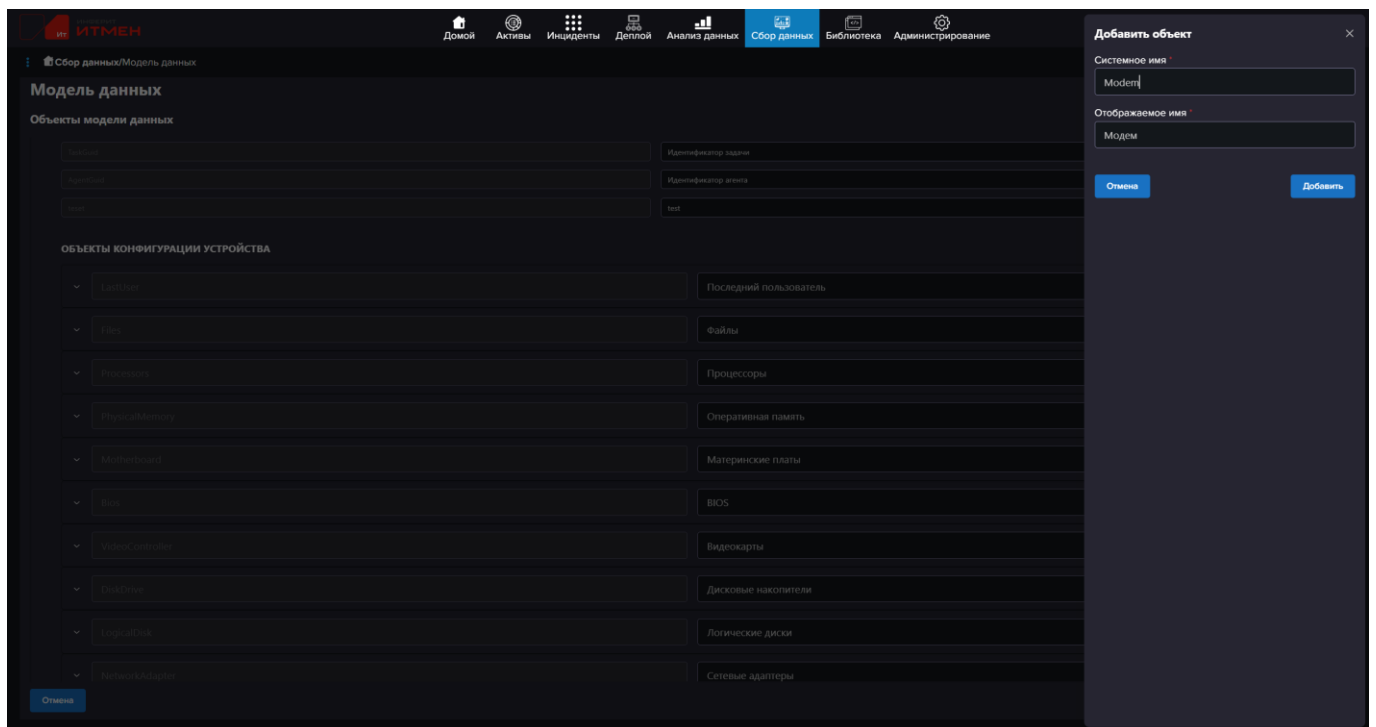
1. В блоке Нормализации при настройке задачи в разделе Сбор данных – Управление инвентаризацией.
2. В разделе Анализ данных
3. После инвентаризации это поле так же появится в карточке устройства в Основном разделе, разделе Конфигураций или Пользователи

Ну а пока рассмотрим добавления «Объекта конфигурации».

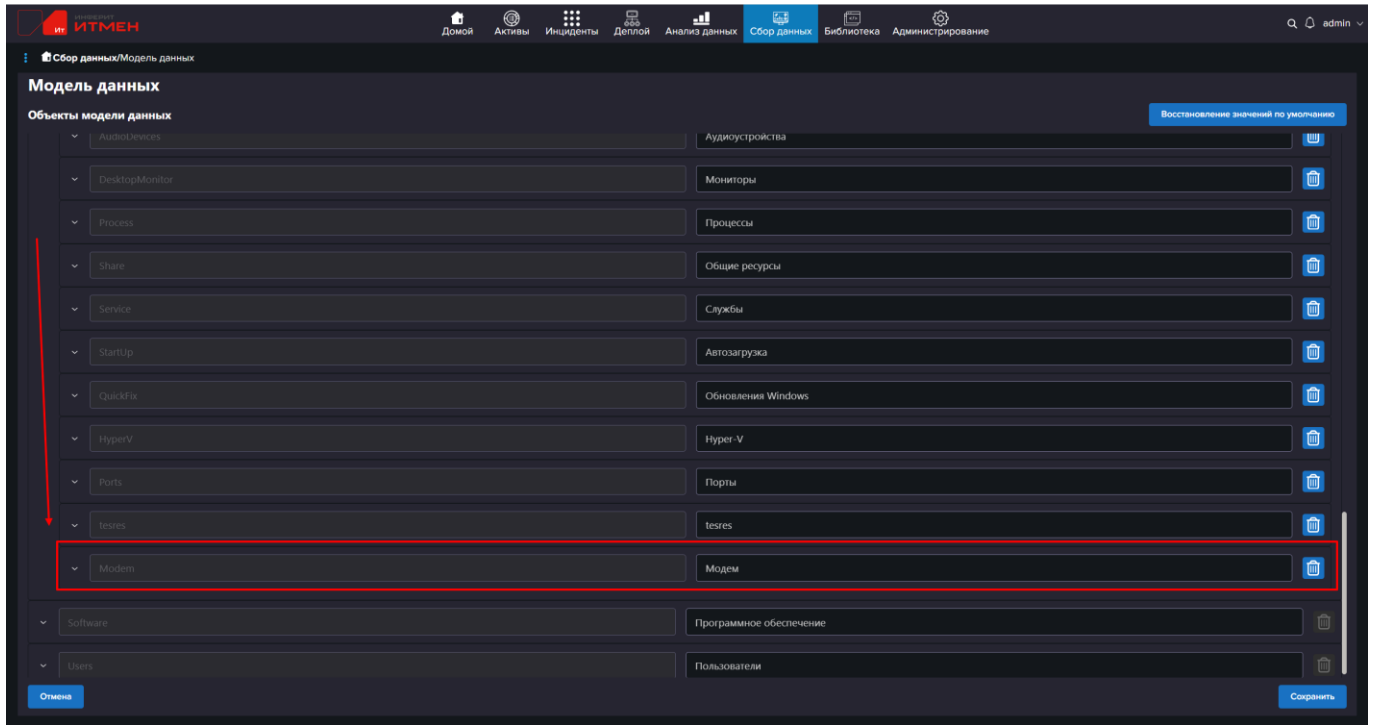
Для этого открываем любой блок, например: Устройства. Прокручиваем до блока «Объекты конфигурации устройства».



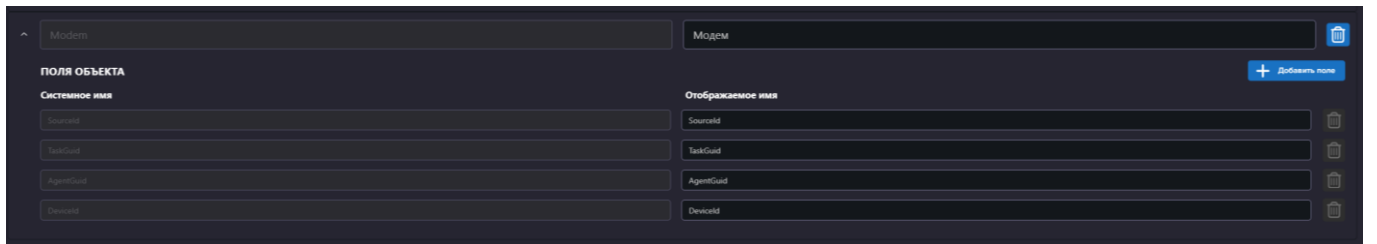
В этом блоке нажимаем кнопку «Добавить объект», после чего у нас появляется боковая панель добавления. В которой мы вводим системное имя объекта и отображаемое имя. Системное имя должно быть написано латинскими буквами и не иметь: пробелов и спец символов.



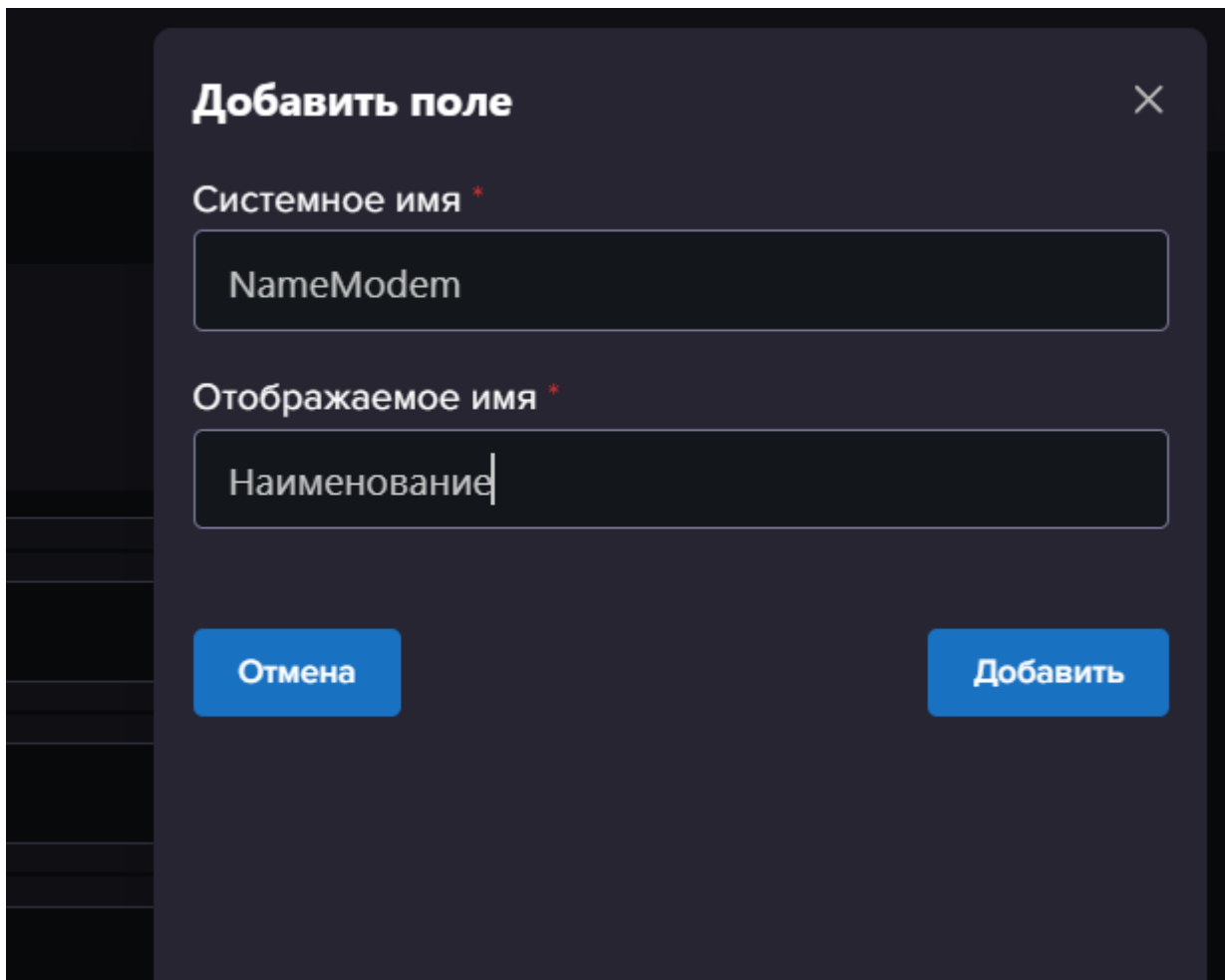
После того как данные будут введены нажимаем кнопку «Добавить». И смотрим как наш новый объект добавился в список.



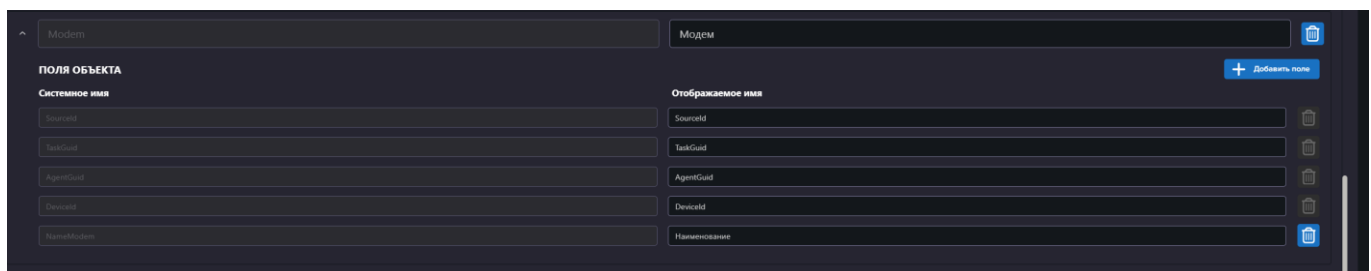
Но пустой объект еще не может участвовать в инвентаризации так как ему нужны поля. Для этого открываем наш созданный объект, смотрим что все системные поля для связи добавлены и нажимаем кнопку «Добавить поле» в этом блоке.



После нажатия кнопки у нас отрылась боковая панель. Где мы так же вводим Системное имя и Отображаемое имя. И нажимаем кнопку добавить.



Поле появилось в общем списке и теперь его можно будет использовать при создании сенсора для сбора данных.

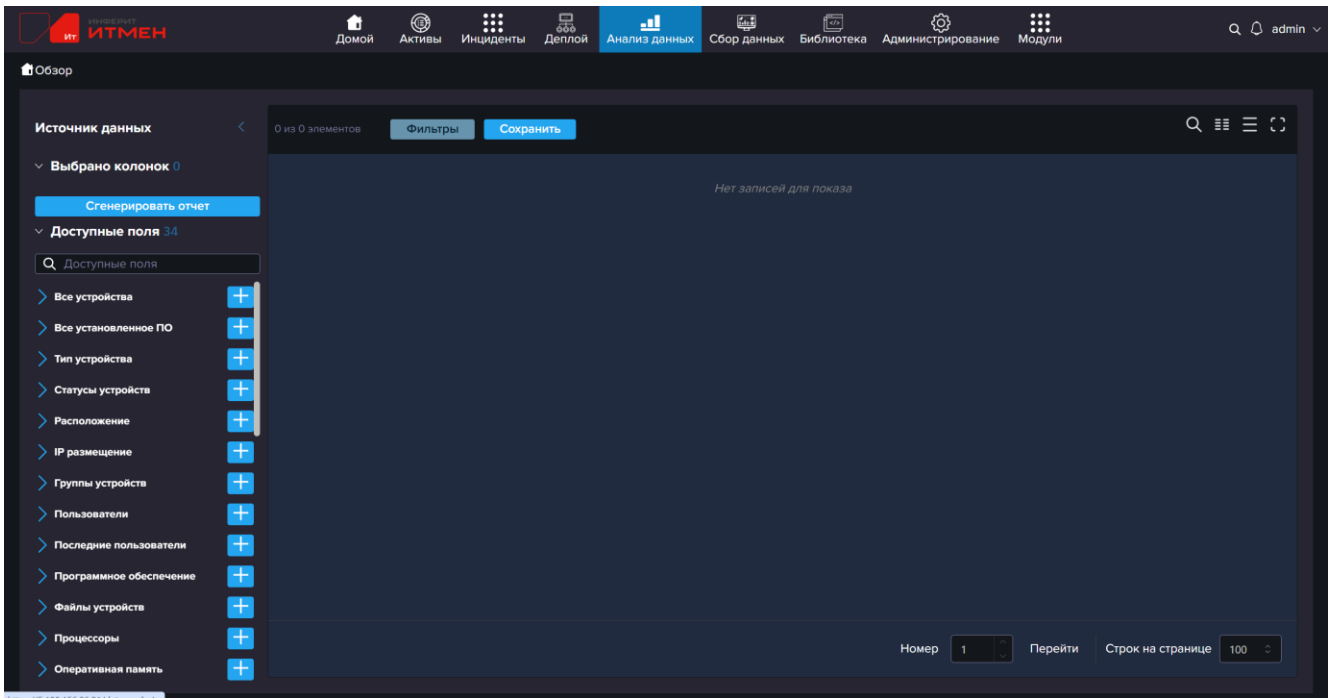


### 3.4 Анализ данных






Работа с запросами данных агентской сети. Сохраненные запросы можно использовать для дальнейшей отчётности.

Для создания отчета необходимо перейти в раздел Анализ данных. Анализ данных строится на основании существующих полей, которые были собраны в инвентаризации.

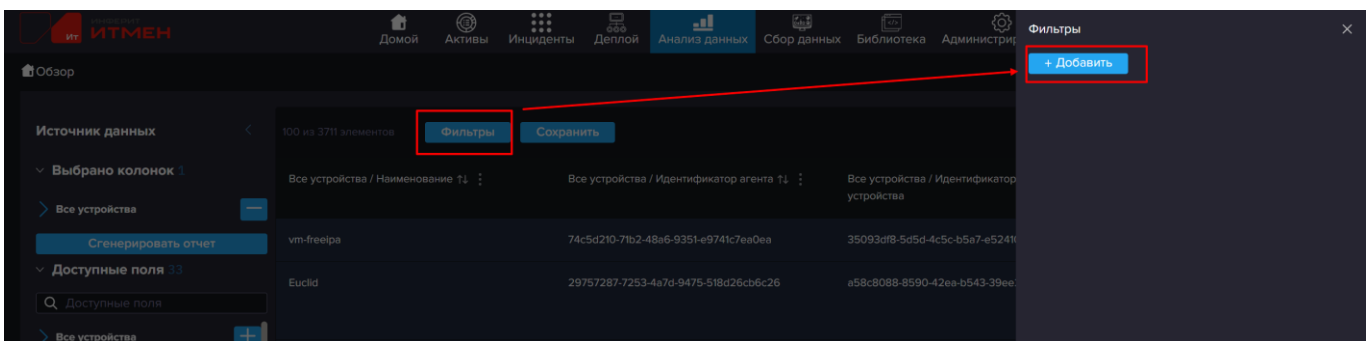
После того как мы перешли в Анализ данных необходимо выбрать колонки, которые будут включены в отчет и нажать на кнопку «Сгенерировать отчет».



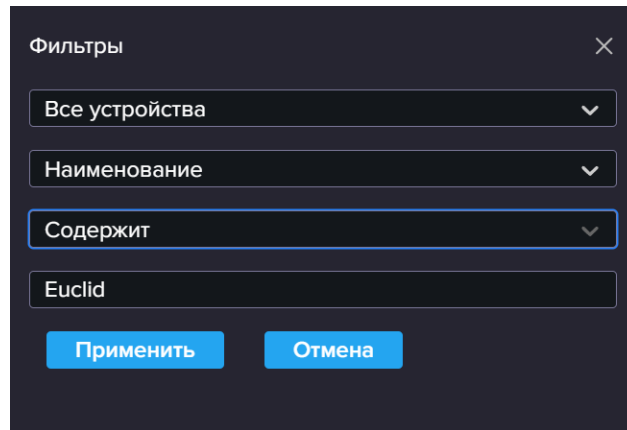
Если раскрыть выбранный справочник, то около каждой колонки можно встретить следующие кнопки:

	Добавить элемент в отчет
	Убрать элемент
	Добавить внутренний элемент
	Убрать внутренний элемент
	Объединить все в одну строку (данная кнопка заблокирована в данном релизе)

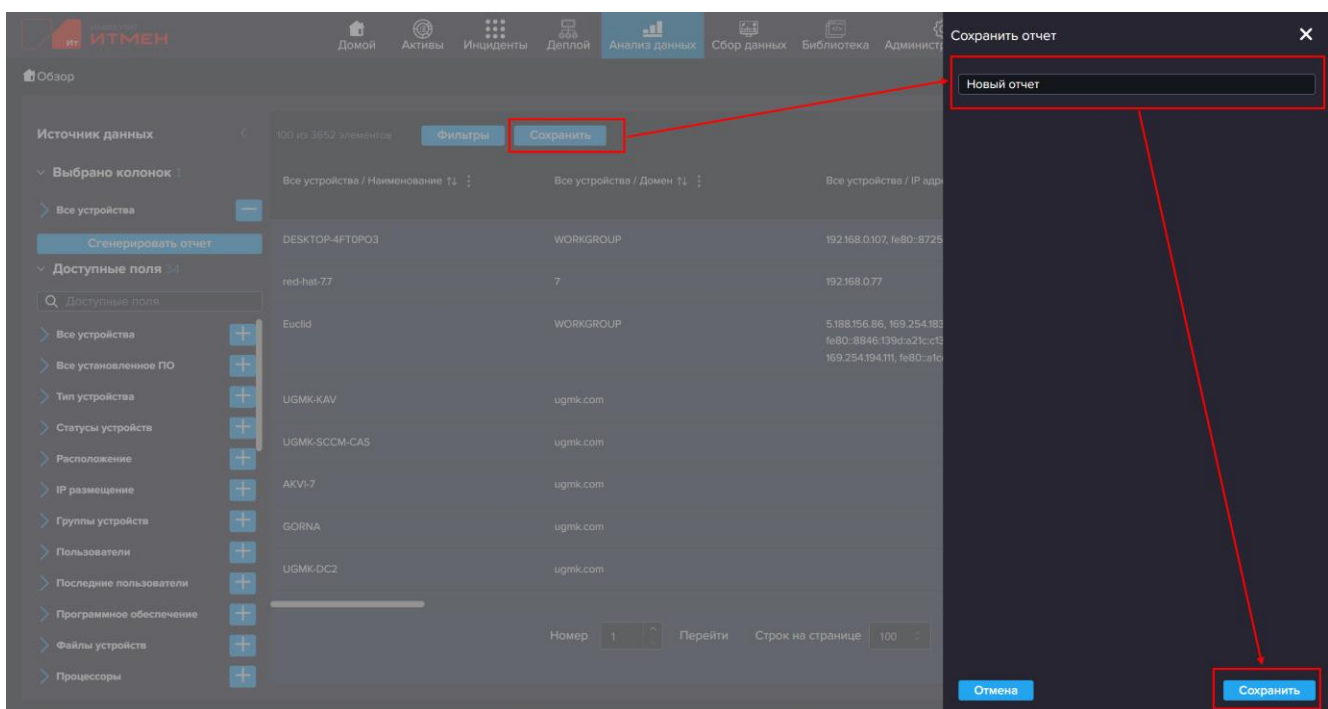
Так же для удобства пользования можно выставить дополнительные Фильтры. Для этого над таблицей необходимо развернуть блок фильтров и нажать кнопку “Добавить”.



После этого выбираем необходимые нам параметры и нажимаем “Применить”



Когда все параметры введены и вы захотите сохранить этот отчет, нажмите кнопку “Сохранить”. Откроется правая панель, где необходимо будет ввести название отчета.



После того как введете название отчета, нажмите кнопку “Сохранить”. Сохраненный отчет можно открыть в разделе [Администрирование – Отчеты– Отчетность](#).

### 3.5 Библиотека

Библиотека данных ПО может быть создана двумя способами: Импорт или при инвентаризации системы через задачи. Импорт рассмотрим чуть ниже, а пока рассмотрим автоматическое создание Библиотека ПО при инвентаризации и её настройки.

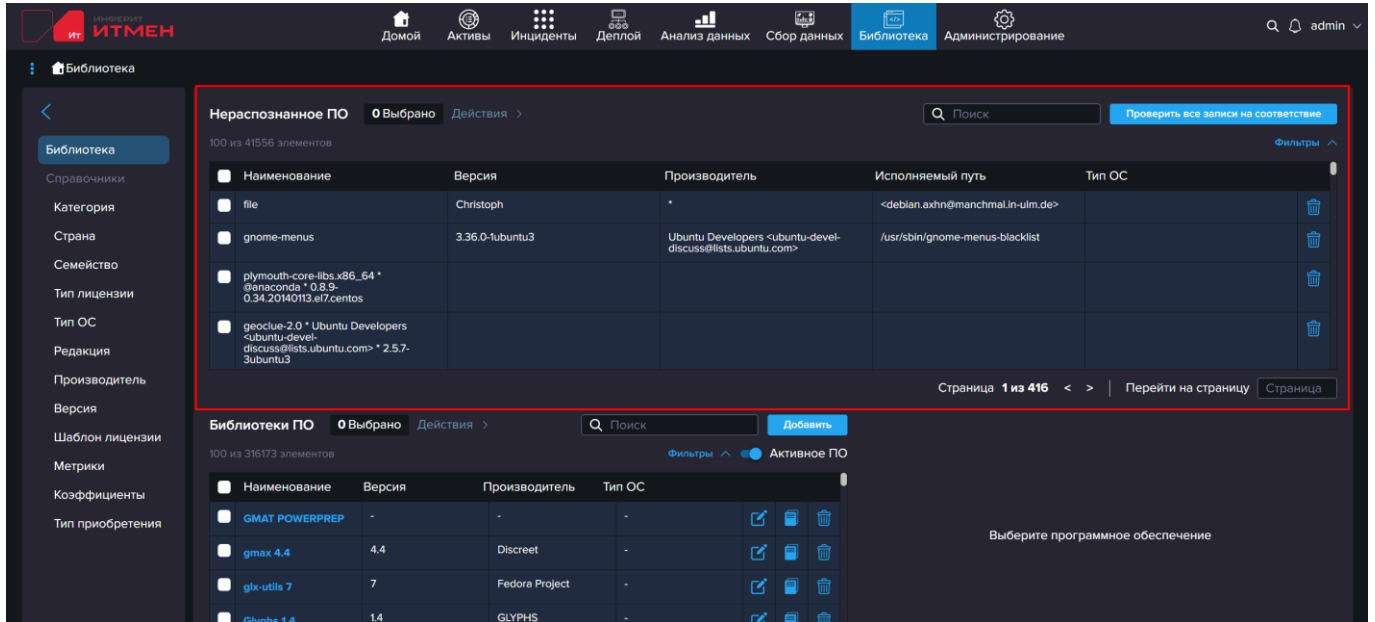
После того как у вас создались данные в Активах, у вас также появятся данные в разделе Библиотека.

В разделе "Библиотека" можно работать не только с программным обеспечением, установленным на компьютерах пользователей, но и отслеживать программное обеспечение, которое было недавно установлено или не соответствует правилам, установленным в компании.



Как это работает? При проведении инвентаризации и импортировании данных система сравнивает все установленные программы с правилами, установленными в системе. Если появляются программы, которые не соответствуют этим правилам, они будут отображаться в области "Нераспознанное ПО".

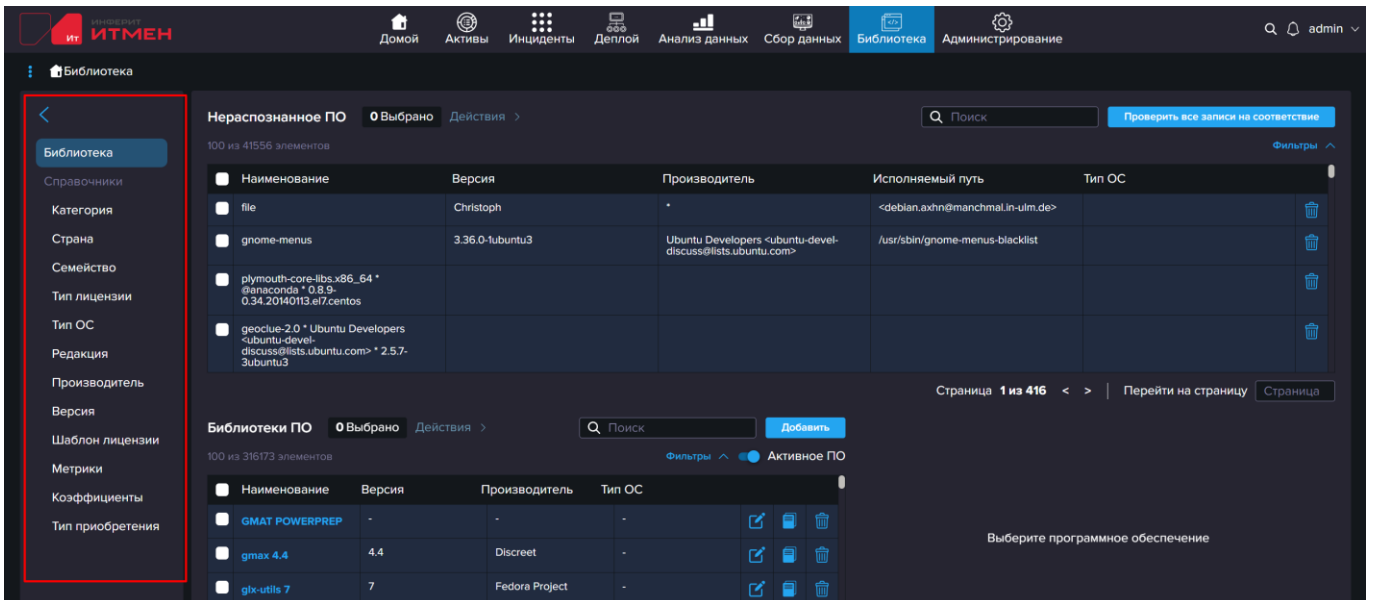
Таким образом, система помогает контролировать установленное программное обеспечение и определять программы, которые могут представлять угрозу для безопасности или не соответствовать правилам использования в компании.



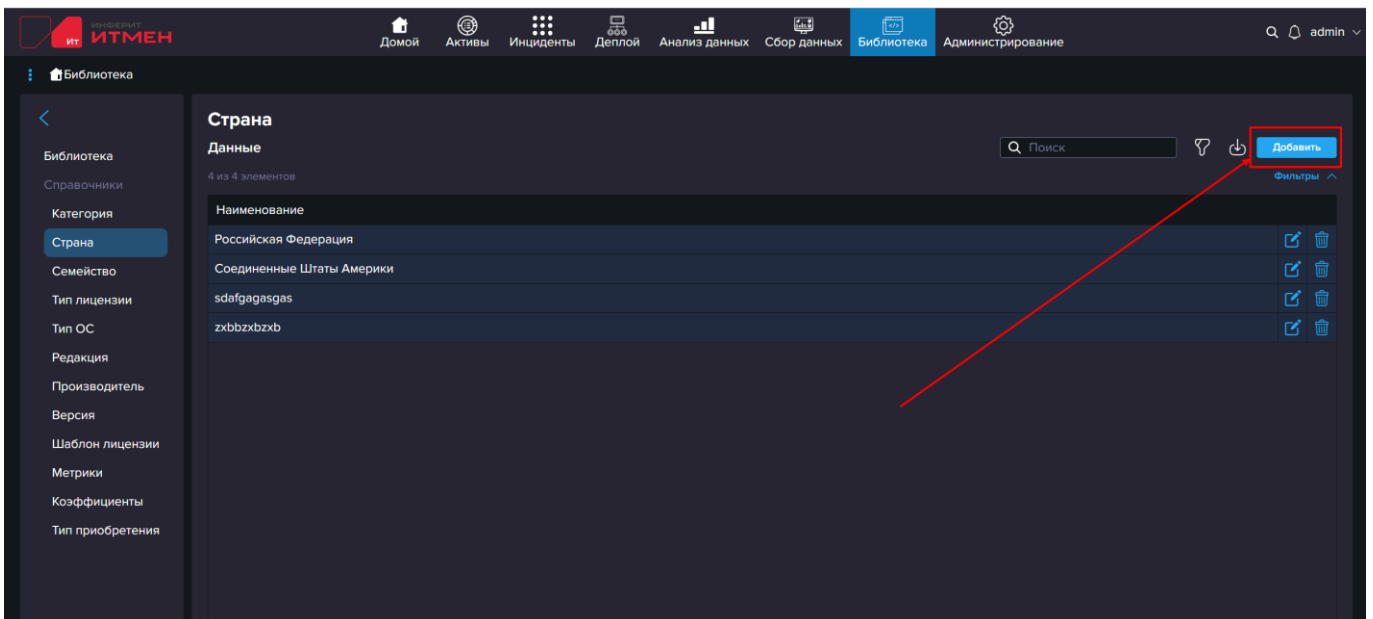
Сам раздел состоит из самой Библиотеки - рабочей области и справочников. Справочники заполняются в соответствии с вашими требованиями и потом отображаются в детальной информации ПО.

Список справочников:

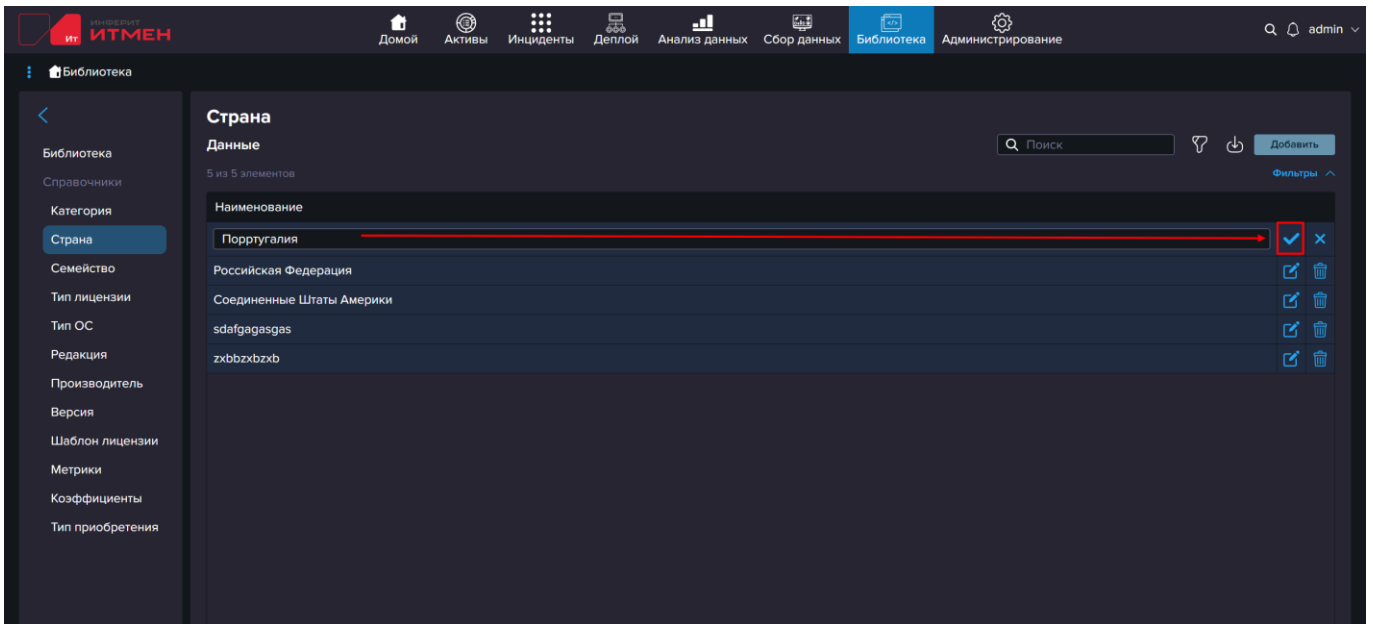
- Категории
- Страна
- Семейство
- Тип лицензии
- Тип ОС
- Редакция
- Производитель
- Версия
- Шаблон лицензий
- Метрики
- Коэффициенты
- Тип Приобретения



Рассмотрим добавление одного из справочников (остальные справочники добавляются аналогично), например, Страна. Для этого в боковом меню выбираем справочник Страна. В открывшемся справочники нажимаем кнопку «Добавить».

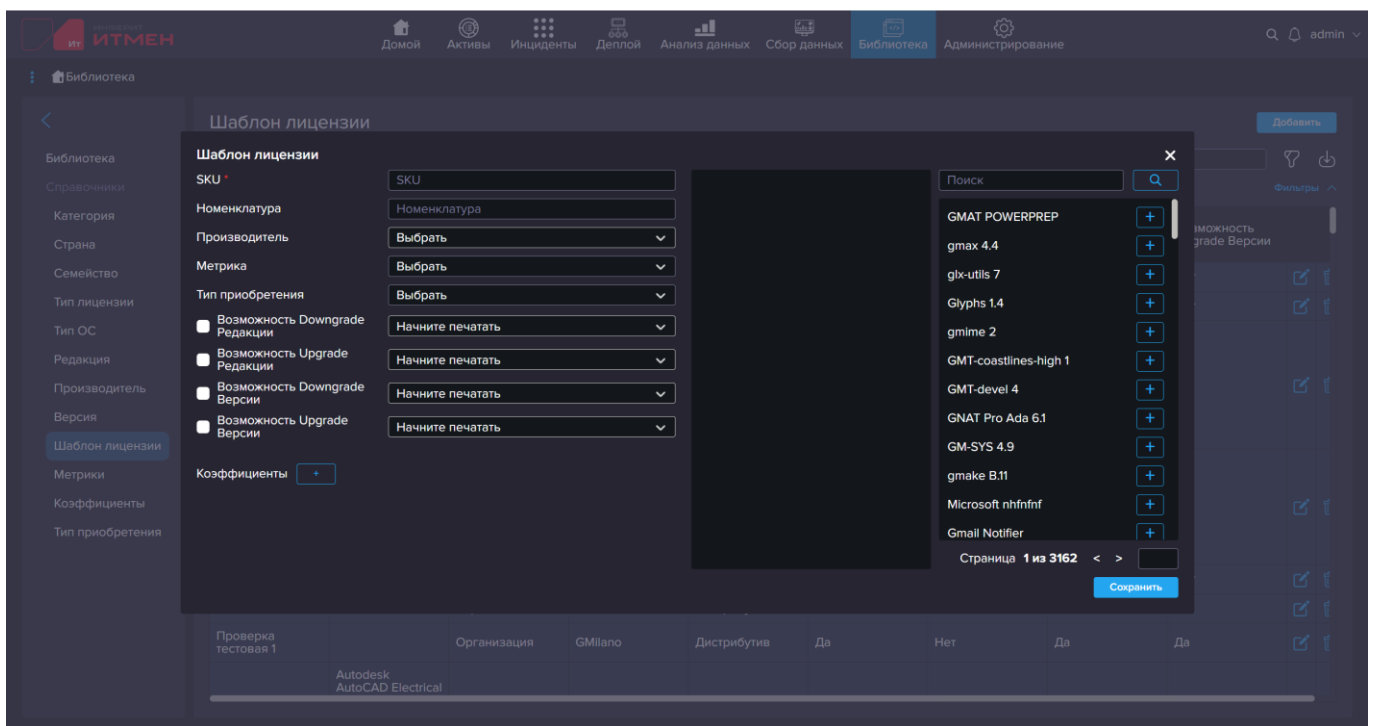


В появившейся области можно ввести обозначение и нажать на кнопки в виде галочки, которая сохранит наше наименование. Так же справочник можно будет отредактировать, удалить или отменить изменения.



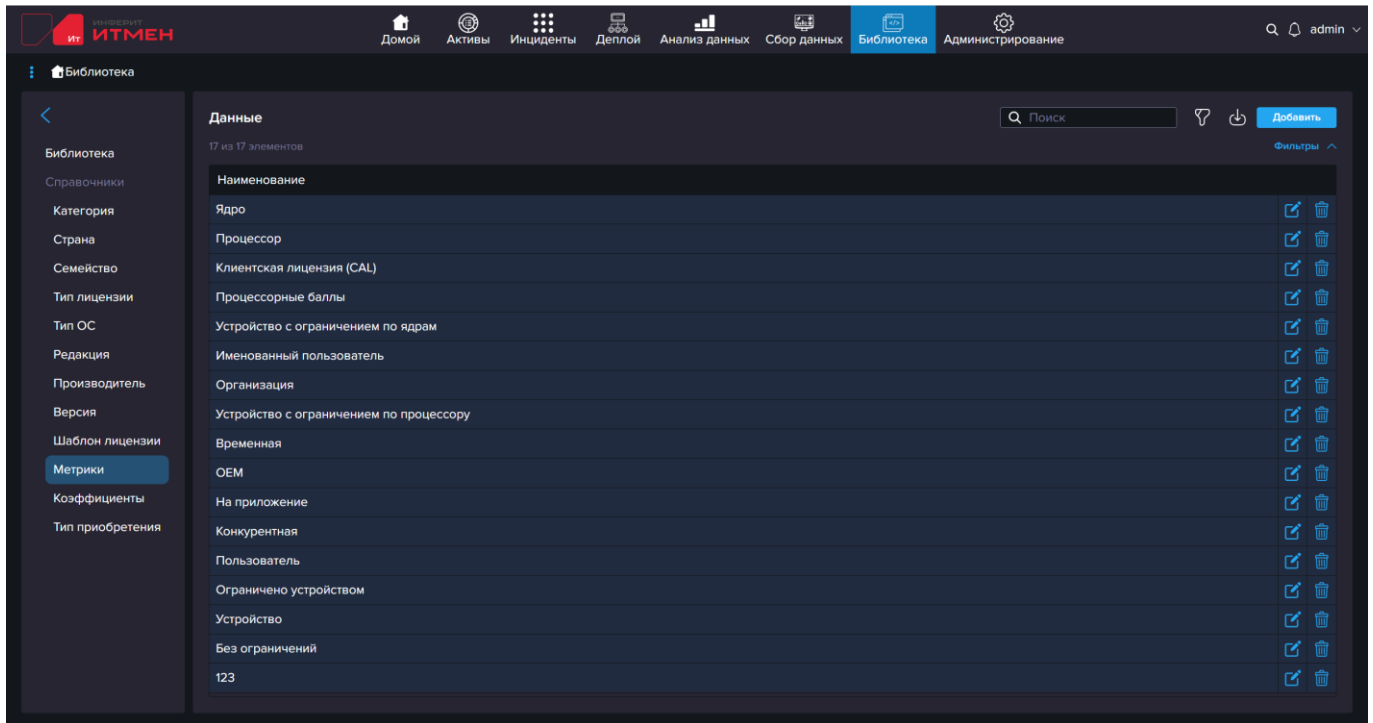
После того как наши справочники будут добавлены, можно приступать к созданию ПО. Для этого нажимаем на раздел Библиотека в левом меню. И в открывшемся окне в области Библиотека ПО нажимаем кнопку «Добавить». С права появится окно детальной информации, где мы введем описания ПО и нажмем «Сохранить».

Так же если необходим свой шаблон, то в открывшейся боковой панели «Справочников» выбираем «Шаблоны лицензий». После чего вам откроется страница со списком «Шаблонов лицензий». Для добавления своего шаблона необходимо нажать кнопку «Добавить». После чего откроется модальное окно добавления



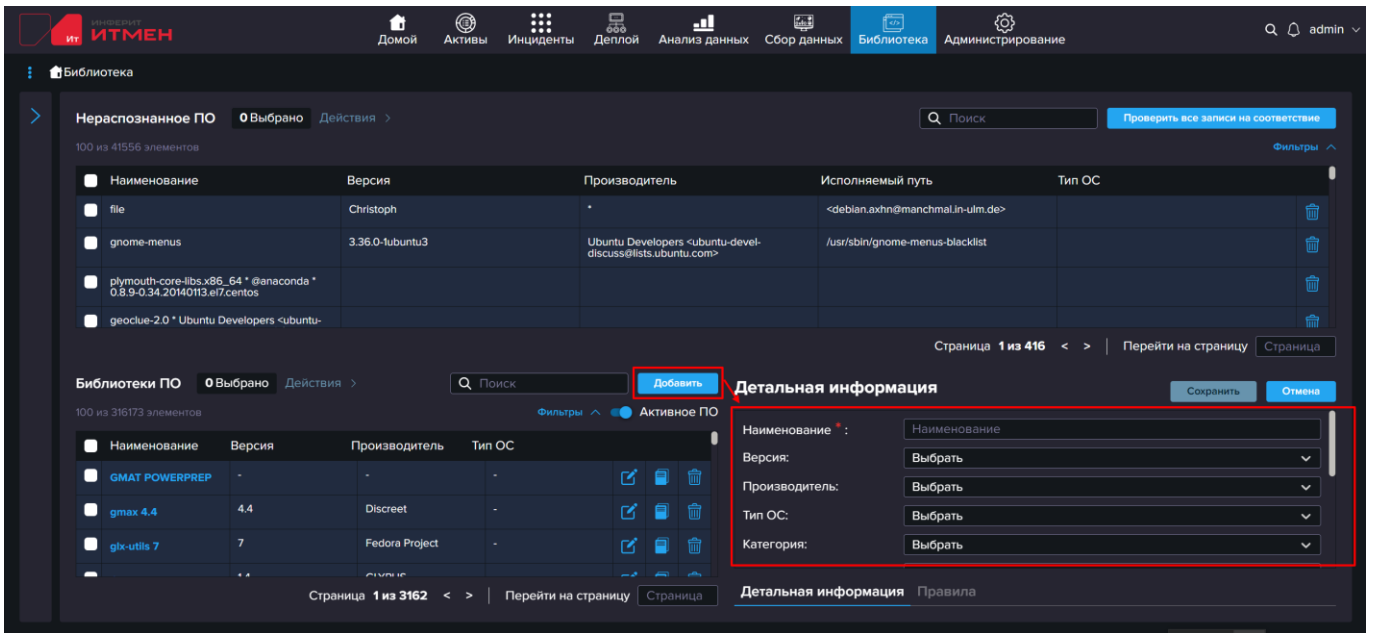
В поле SKU вводим наименование шаблона. Затем в выпадающем списке выбираем Производителя. Для того чтобы выбрать значение в поле Метрики и Тип Приобретения. Так как  
 Дата документа: 29.08.2024  
 Версия системы: 5.5

эти справочники обычно имеют большое количество данных, в выпадающем списке можно воспользоваться поиском. Для этого отрываем выпадающий список и начинаем вводить интересующие нас данные. После чего выбираем нужно из списка. Чтобы добавить необходимые данные которых не хватает, вам необходимо перейти в одноименный справочник. Например: Метрики

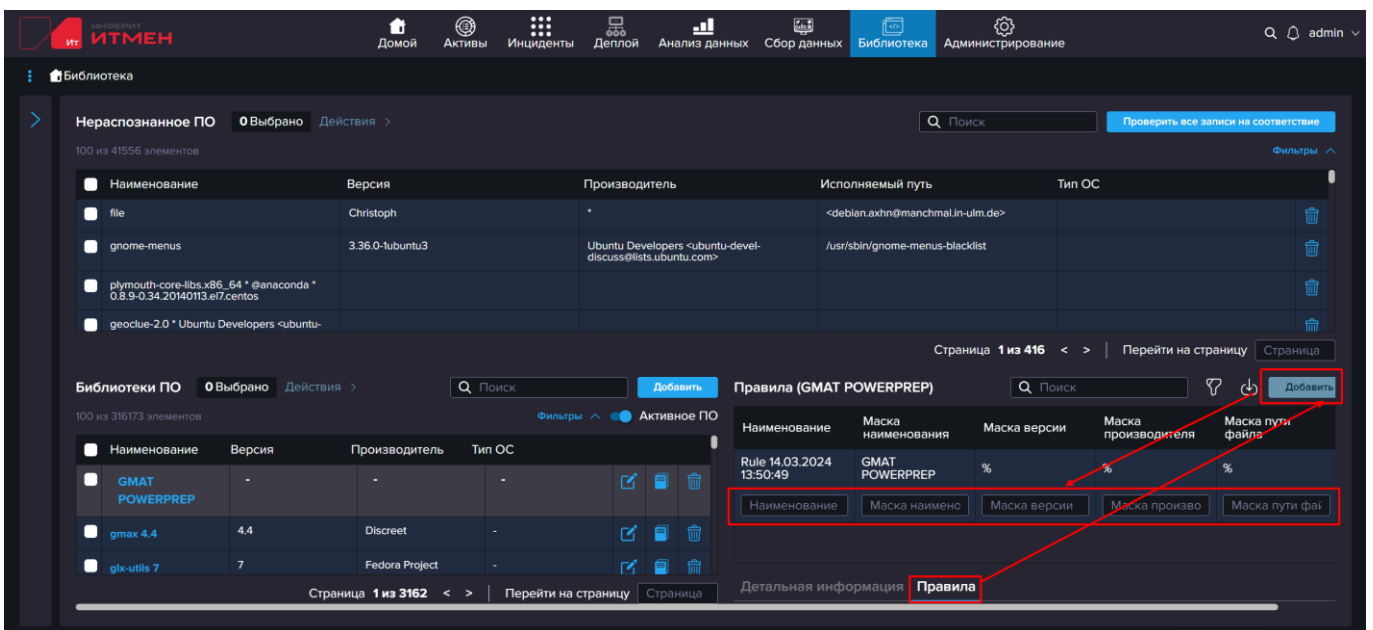


Так же необходимо будет заполнить Тип приобретения и Производители. Эти справочники так же будут использоваться при создании Шаблона лицензий.

Далее рассмотрим, как добавить «Программное обеспечение» в Библиотеку. Для этого необходимо в блоке списка справочников нажать на значение «Библиотека». Откроется рабочая область «Библиотеки». В блоке «Библиотека ПО» нажимаем «Добавить», после чего с права появится карточка «Программного обеспечения». Далее заполняем карточку и нажимаем «Сохранить».



После того как карточка ПО сохранится она появится в левой области и будет открыта его детальная информация. Затем, чтобы это ПО не попадало в список нераспознанных необходимо создать правило. Для этого в окне детальной информации необходимо нажать на вкладку правила, затем нажать на кнопку «Добавить» и ввести правило.

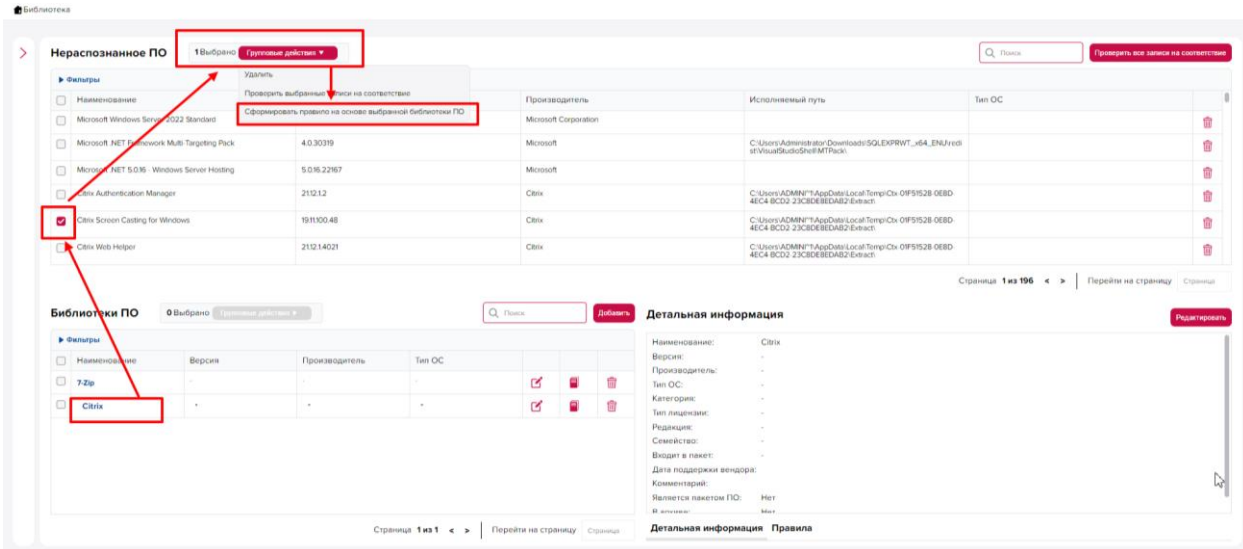


Теперь все приложения, соответствующие этому правилу, не будут попадать в список нераспознанного. Так же если вы не точно уверены в названии ПО на каждом компьютере можно обозначение выделить знаком «%». Например, рассмотрим поле наименование:

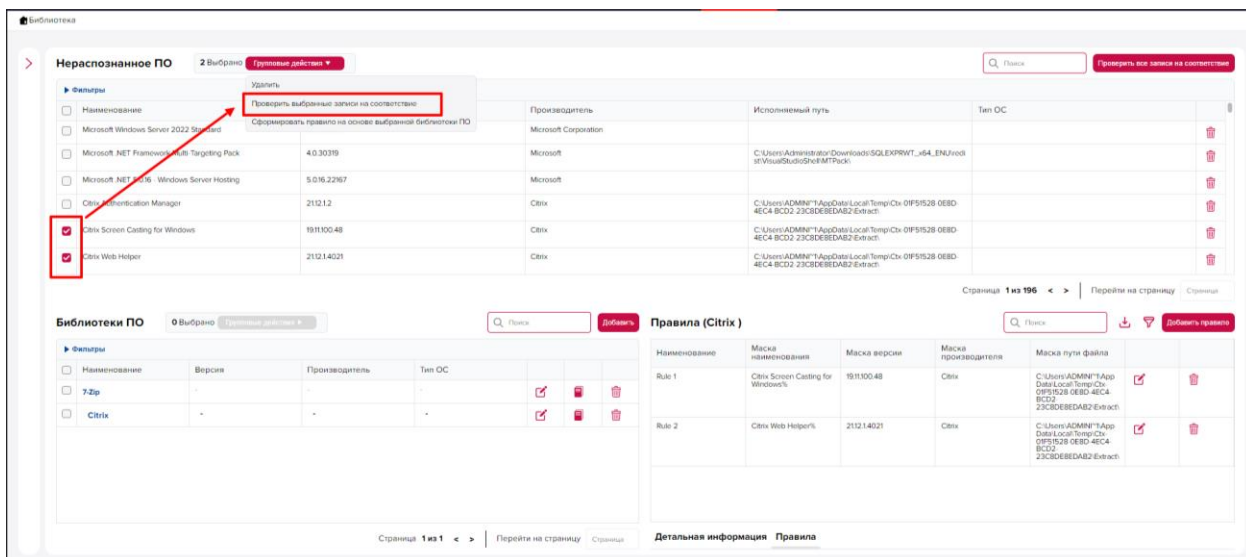
- Если мы введем «Viber%», то сюда попадут все значение такие как Viber MC
- Если введем «%Viber», то попадут все значение MC Viber, а значения Viber CU не попадут и отобразятся в нераспознанном.

Так же если вы хотите создать правила на основе уже найденных нераспознанных ПО можно сделать следующие действия:

1. Необходимо создать новый объект в библиотеке ПО или выбрать объект в Библиотеке ПО нажав на Наименование
2. Если создаете Объект ПО, не забудьте проверить, что он выбран в Библиотеке.
3. Затем перейти в область Нераспознанное ПО и выбрать чек-боксами те объекты, которые должны подходить под правила
4. После того как все объекты будет выбраны в Групповых действиях нажимаем “Сформировать правило на основе выбранной Библиотеки ПО”



Затем если хотите, чтобы нераспознанные объекты ушли из списка, необходимо активировать чек-боксы около тех элементов, которые должны уйти. Затем в Групповых действиях выбрать значение “Проверить необходимые записи на соответствие”. Если все правильно создается они пропадут из области Нераспознанное ПО.



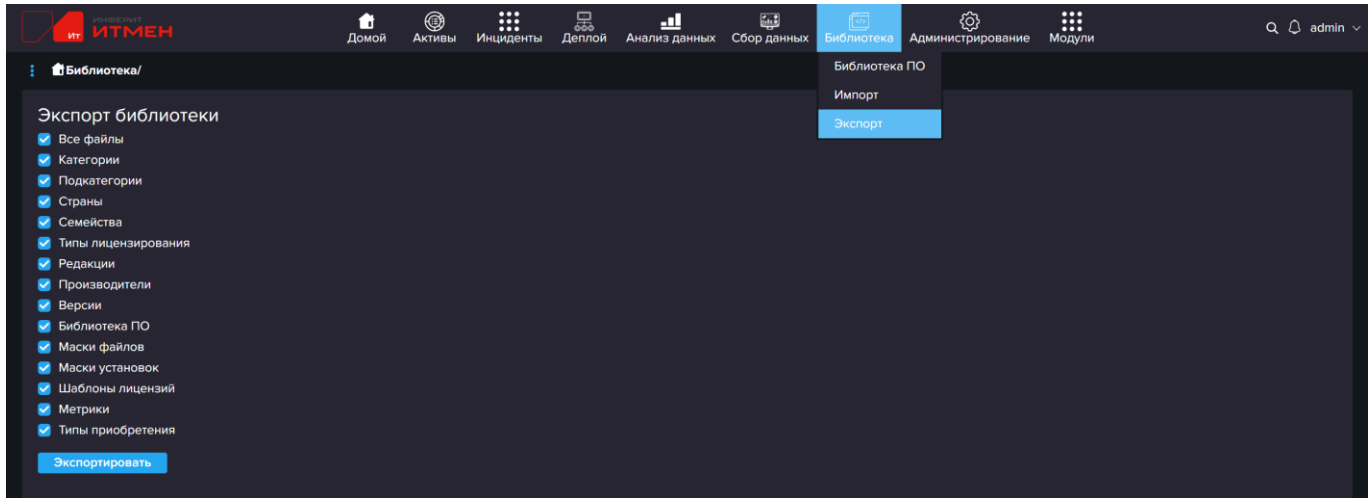
## Импорт и Экспорт Библиотеки ПО

Если у вас уже есть Библиотека программного обеспечения, которая одобрена руководством её можно импортировать и не вносить руками по отдельности, но для этого

Дата документа: 29.08.2024

Версия системы: 5.5

необходимо привести её к правильному шаблону. То для этого можно скачать файлы и заполнить их своими данными. Для этого необходимо перейти в раздел Библиотека ПО и выбрать подраздел Экспорта.



В открывшемся подразделе скачиваем файлы, если библиотека пустая у вас скажутся пустые файлы, если данные уже есть, то удалить данные и внести свои изменения не меняя заголовки столбцов. Маска файлов каждого справочника:

1. Справочник Версии: имя файла Versiya\_\_01.csv

ID	Версия программного обеспечения
В этом столбце указываем нумерацию. Например: 1	В этом столбце указываем версию программного обеспечения

2. Справочник Вендор: имя файла Vendor\_\_01.csv

ID	Наименование	Страна
В этом столбце указываем нумерацию. Например: 1	В этом столбце указываем наименование вендора	Наименование страны

3. Справочник Тип лицензии: имя файла Tip\_litsenzirovaniya\_\_01.csv.

ID	Тип лицензирования
В этом столбце указываем нумерацию. Например: 1	В этом столбце указываем тип лицензии

4. Справочник Страна: имя файла Strana\_proizvoditel\_\_01.csv

ID	Страна
В этом столбце указываем нумерацию. Например: 1	В этом столбце указываем страну программного обеспечения

5. Справочник Семейство: имя файла Semeystvo\_prilozheniy\_\_01.csv

ID	Семейство приложений
----	----------------------

В этом столбце указываем нумерацию. Например: 1	В этом столбце указываем семейство программного обеспечения. Например: Яндекс или Google
--	--

6. Справочник Редакция: имя файла Redaktsiya\_\_01.csv

ID	Редакция программного обеспечения
В этом столбце указываем нумерацию. Например: 1	В этом столбце указываем редакция программного обеспечения.

7. Справочник Категории: имя файла Kategoriya\_programmnogo\_obespecheniya\_\_01.csv

ID	Категории	Подкатегории
В этом столбце указываем нумерацию. Например: 1	В этом столбце указываем наименование категории	В этом столбце можно указываем подкатеорию. Если подкатегорий много, то указываем строку в этом столбце в соответствии со следующим примером в следующей строке
1	Финансы	Бухгалтерия***ERP***Финансы*** Налоги***Управление рабочим временем

8. Справочник Подкатегория Podkategoriya\_programmnogo\_obespecheniya\_\_01.csv

ID	Подкатегории
В этом столбце указываем нумерацию. Например: 1	В этом столбце подкатегории.

9. Таблица Библиотека ПО, наименование файла Prilozhenie\_\_01.csv, столбцы

- ID – обязательное поле
- Полное наименование приложение обязательное поле
- GUID
- Семейство приложений – Необязательное поле
- Вендор -Необязательное поле
- Тип лицензирования – Необязательное поле
- Редакция -Необязательное поле
- Версия – Необязательное поле
- Дата окончания поддержки вендора – Необязательное поле
- Категория- Необязательное поле
- Подкатегория- Необязательное поле

10. Так же есть возможность сразу загрузить правила, только наименование приложения должно совпадать с наименованием из таблицы библиотека ПО. Правила можно загрузить с помощью одного из двух файлов: Маска инсталляции (Maska\_installyatsii\_\_01.csv) и Маска файла (Maska\_fayla\_\_01.csv). Они отличаются тем, что в файле «Маска инсталляции» нет пути файла, поэтому если хотите загрузить с правилом, где указан путь к файлу, то лучше воспользоваться

Дата документа: 29.08.2024

Версия системы: 5.5



шаблоном Маска файла. Если же вы не будете указывать путь, то правила можно загрузить с помощью файла «Маска инсталляции».

Маска инсталляции (Maska\_installyatsii\_\_01.csv):

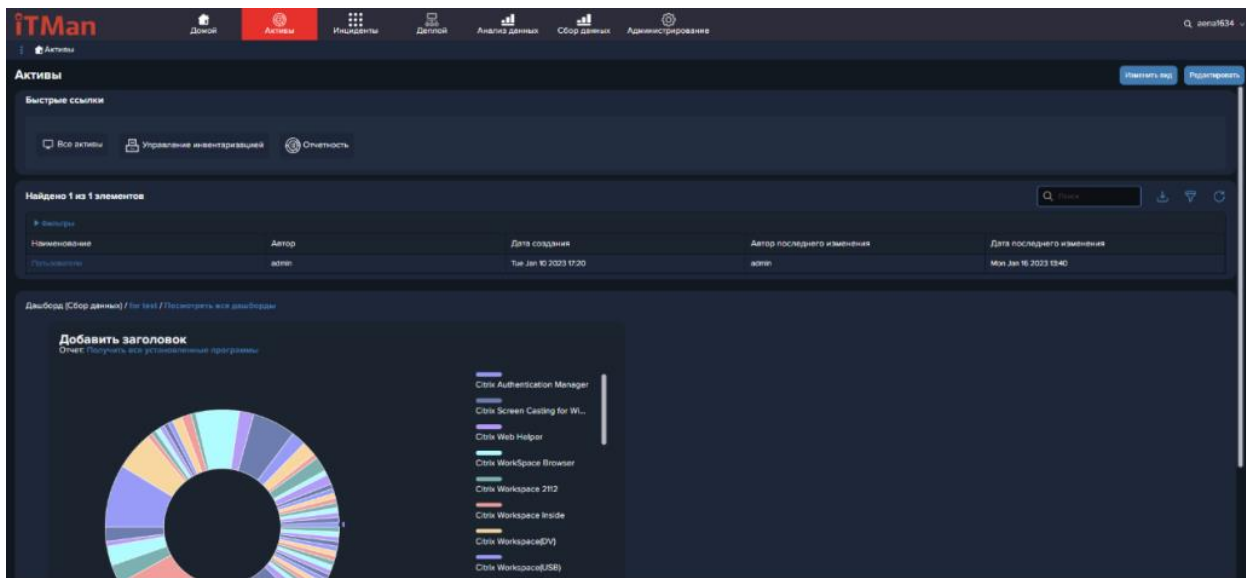
ID	Маска наименования инсталляции	Маска версии инсталляции	Маска вендора инсталляции	Приложение
Пример: 411685	Пример: MacDrive 8	Пример: 8.%	Пример: Mediafour%	Пример: MacDrive 8

### 3.6 Разделы в доработке

В этом разделе представлены разделы, которые по техническим причинам находятся в доработке или в стадии разработки.

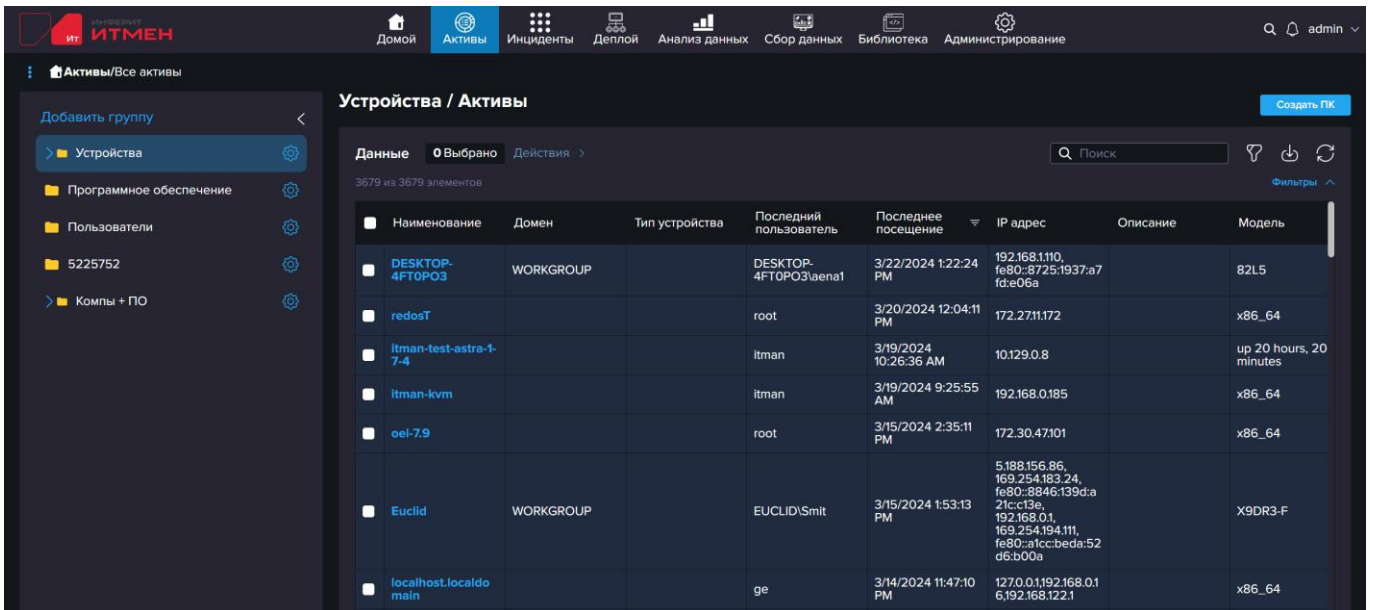
#### 3.6.1 Активы

Активы - раздел в котором можно работать со всеми активами: программное обеспечение, пользователи и т.д.



#### 3.6.2. Все активы

В этом подразделе представлены все активы в виде таблиц и детальных карточек. Для удобства работы данные отображены в виде таблиц: все пользователи, устройства, ПО, ПК и Историю изменения ПК.



Наименование	Домен	Тип устройства	Последний пользователь	Последнее посещение	IP адрес	Описание	Модель
DESKTOP-4FTOPO3	WORKGROUP		DESKTOP-4FTOPO3\aela1	3/22/2024 1:22:24 PM	192.168.1.110, fe80::8725.1937:a7fd:e06a		82L5
redost			root	3/20/2024 12:04:11 PM	172.27.11.172		x86_64
itman-test-astra-1-7-4			itman	3/19/2024 10:26:36 AM	10.129.0.8		up 20 hours, 20 minutes
itman-kvm			itman	3/19/2024 9:25:55 AM	192.168.0.185		x86_64
oei-7.9			root	3/15/2024 2:35:11 PM	172.30.47.101		x86_64
Euclid	WORKGROUP		EUCLID\Smit	3/15/2024 1:53:13 PM	5.188.156.86, 169.254.183.24, fe80::8846.139d:a21c:c13e, 192.168.0.1, 169.254.194.111, fe80::a1cc:beda:52d6:b00a		X9DR3-F
localhost.localdomain			ge	3/14/2024 11:47:10 PM	127.0.0.1, 192.168.0.1, 6.192.168.122.1		x86_64

Как мы видим на экране у нас есть две рабочие области.

- Группы
- Отображения таблицы данных

### Таблица данных

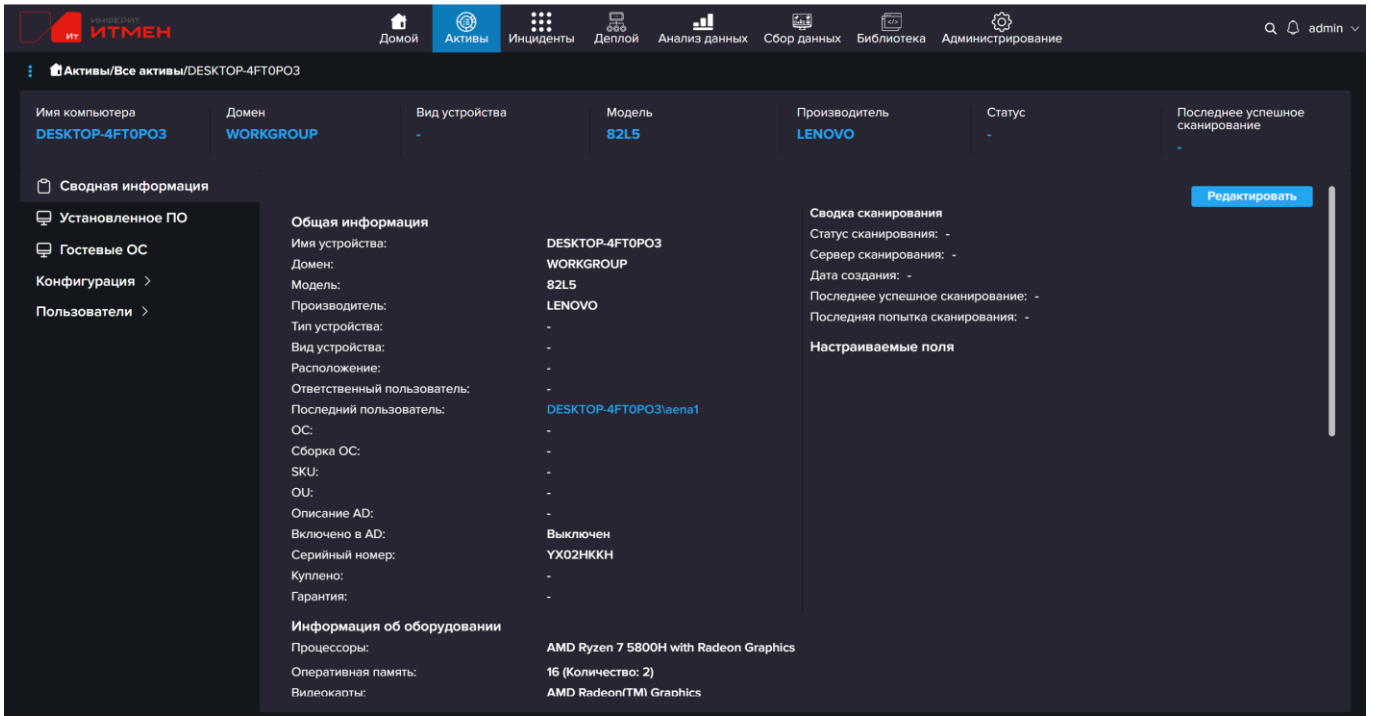
По умолчанию в системе созданы три основные группы, в которых отображаются все наши активы, пользователи и программное обеспечение.

Выберем, например "Активы". Отобразится список наших ПК. В этом разделе отображены как созданные при инвентаризации, так и созданные вручную через кнопку "Создать ПК"

Если нажать на наименование актива можно просмотреть всю информацию касающуюся этого актива, а также всех пользователей. Если появились дополнительные данные или изменения, данный актив всегда можно отредактировать.

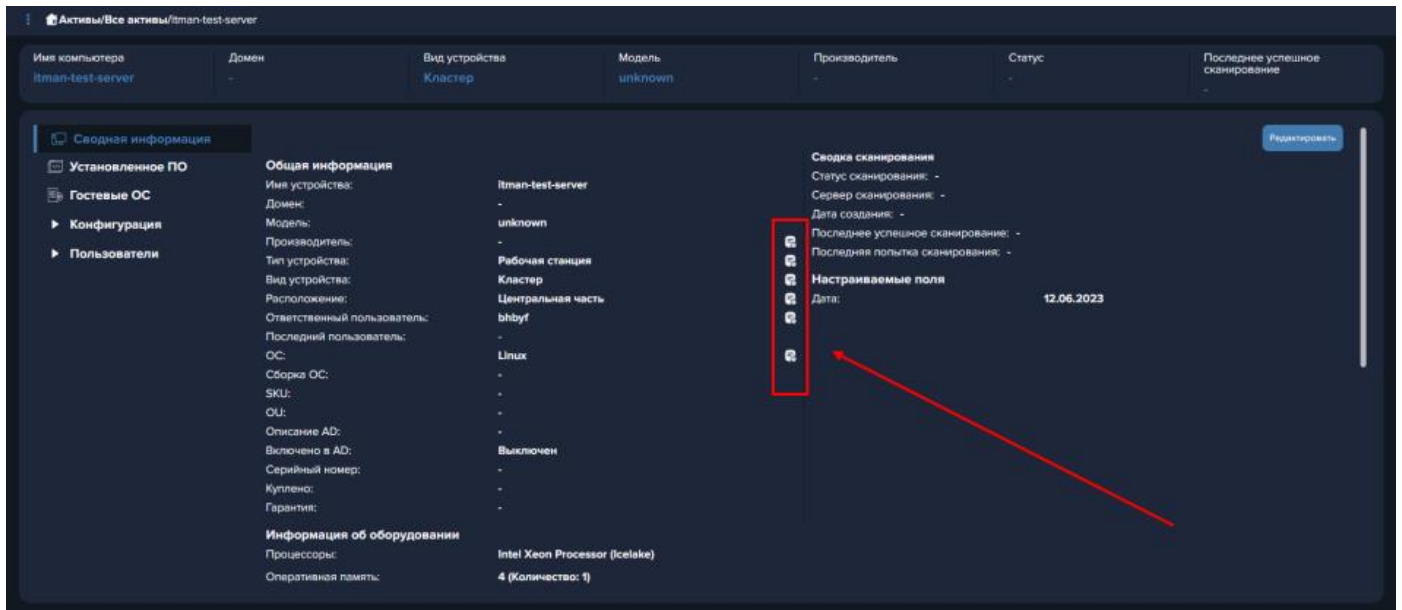
Описание делится на:

- Сводная информация
- Установленное ПО
- Конфигурации
- Пользователи

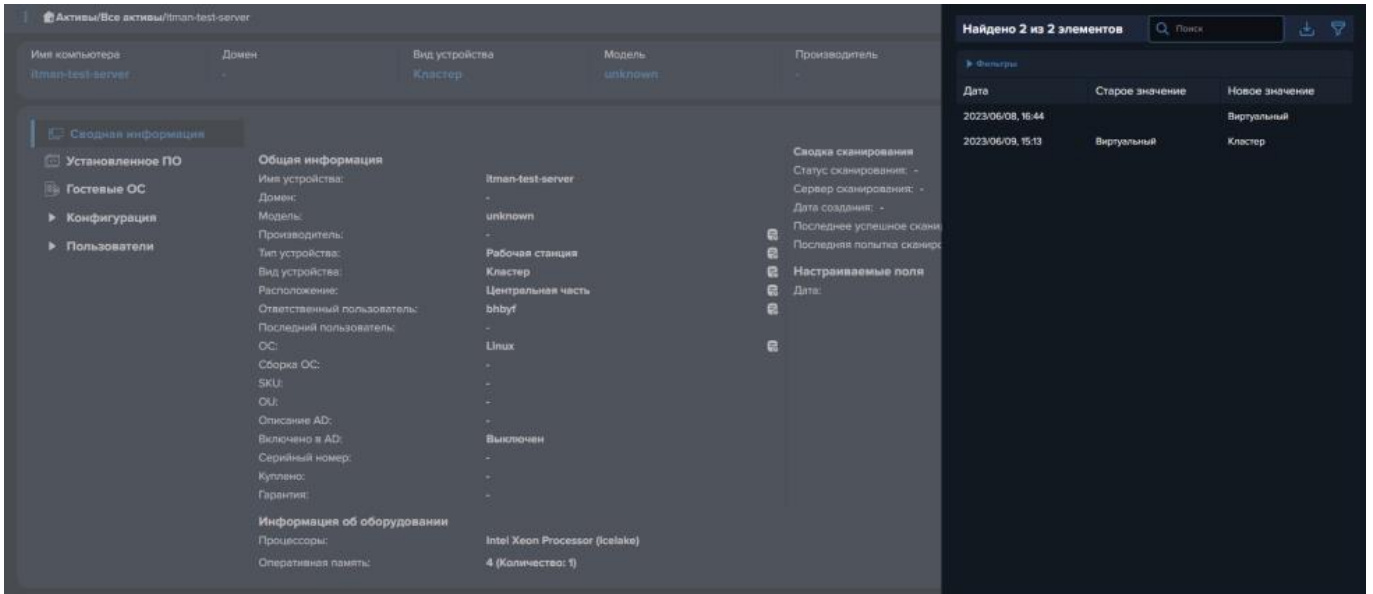


Как же нам увидеть нашу Историю изменения?

После того как будут введены изменения в какое-то значение устройства у вас около поля появится значок истории.

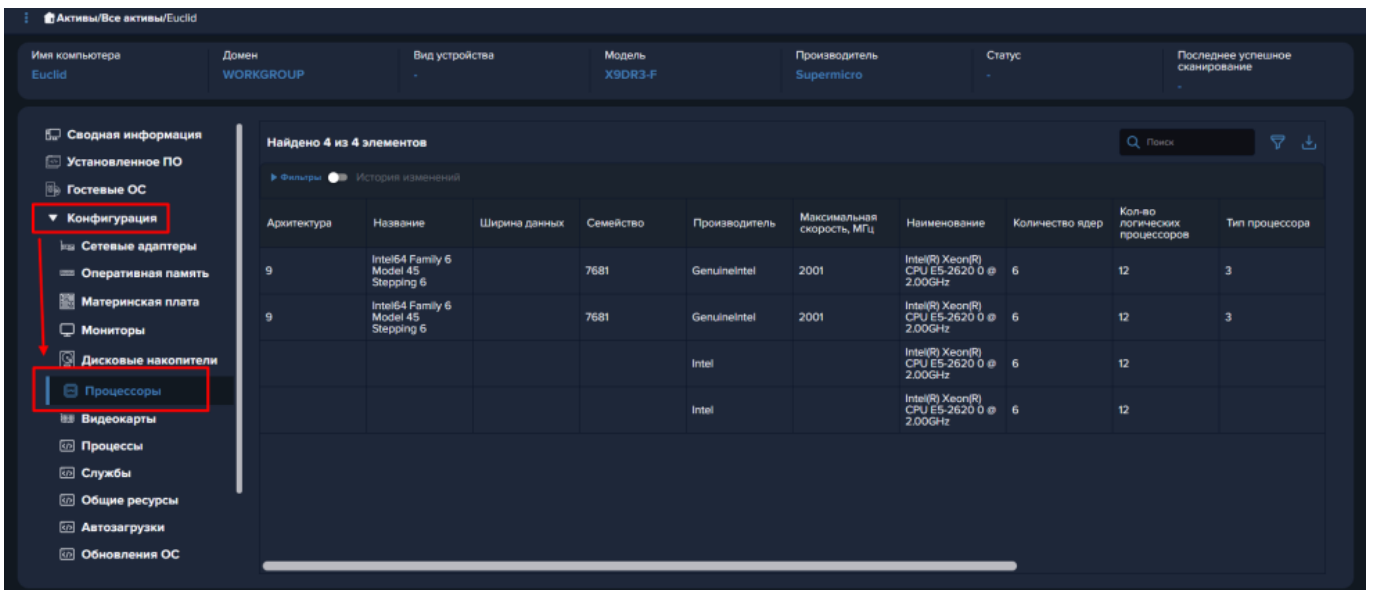


При нажатии на этот значок у вас откроется боковая панель с информацией об изменении, закрыть её можно с помощью кнопки крестика в правом верхнем углу панели.

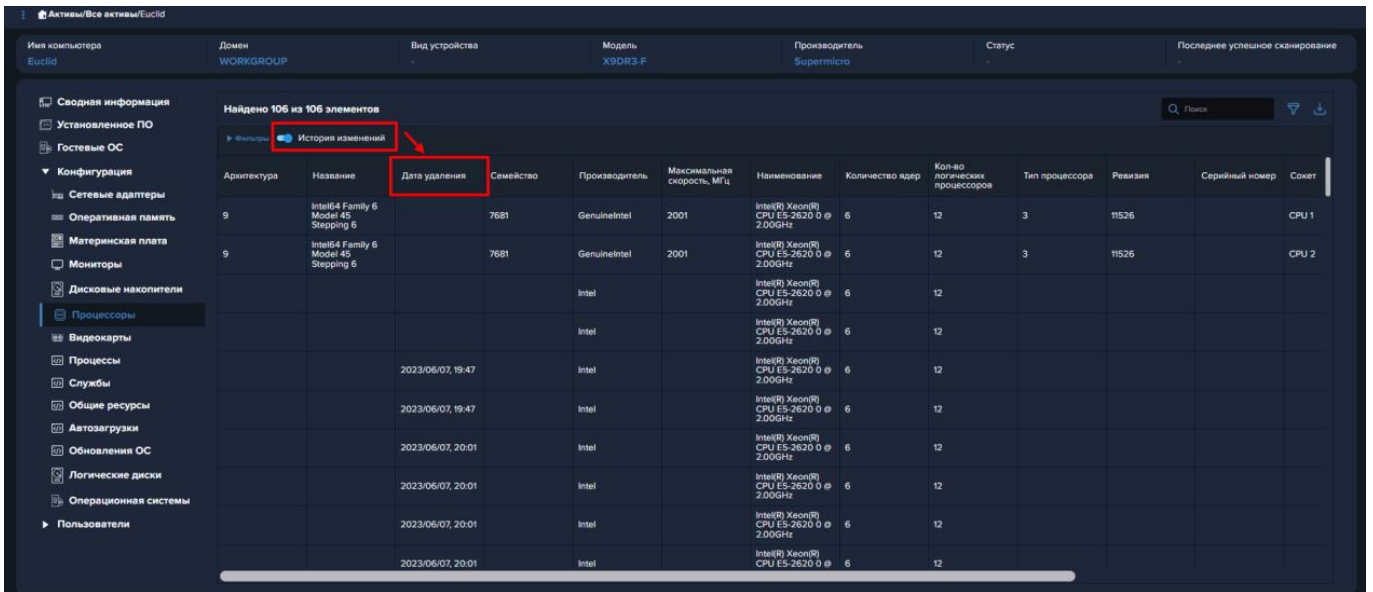


Также в блоке Конфигураций отображена история с помощью таблицы. Как её посмотреть?

Открываем блок Конфигураций и выбираем, например, блок Процессоры.

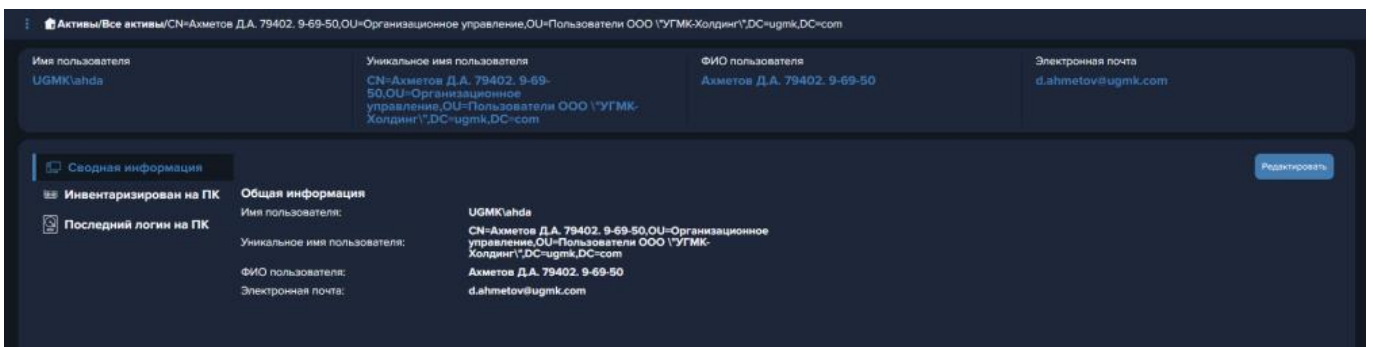


Затем около фильтра включаем значение "История изменения". И у вас отобразятся в таблице данные с учетом даты изменения (столбец Дата удаления расположен в конце таблицы, переносить его можно с помощью инструмента редактирование таблицы).



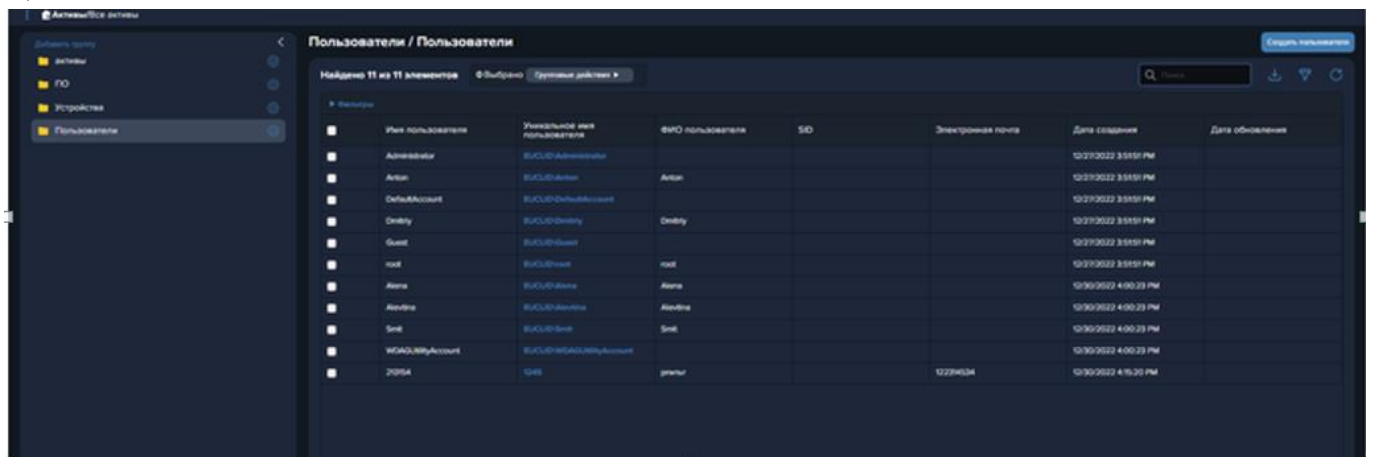
Перейдем в группу Пользователи.

Здесь отображены все пользователи с информацией о нем. Для того чтобы узнать к какому ПК относится пользователь необходимо перейти в карточку пользователя.



Для создания пользователя актива необходимо перейти во “Все активы” и выбрать папку “Пользователи” и нажать на кнопку “Создать пользователя”

Щ



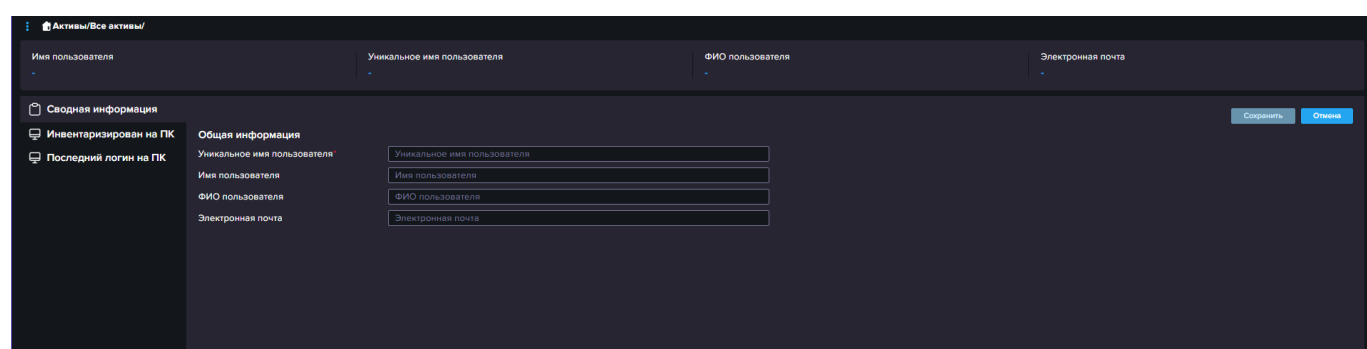
Для создания пользователя необходимо будет заполнить следующие поля:

Дата документа: 29.08.2024

Версия системы: 5.5

- Уникальное имя пользователя
- Имя пользователя
- ФИО пользователя
- Электронная почта

Где “Уникальное имя пользователя” его персональный идентификатор, который не должен совпадать с другими пользователями. Так же это поле является обязательным и в дальнейшем его нельзя будет отредактировать.



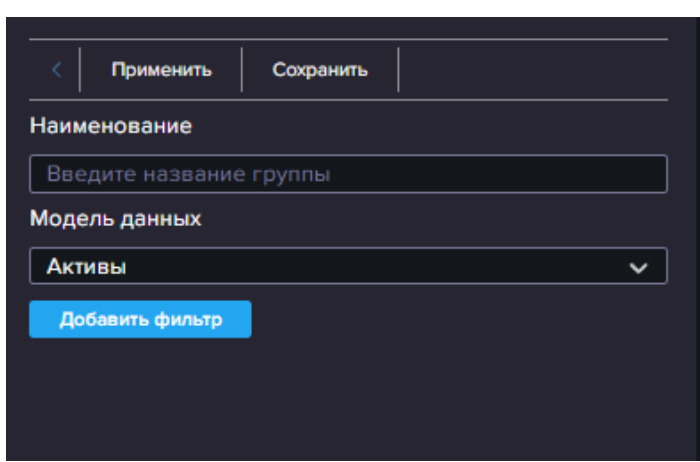
## Группы

С лева это группы, а с права отображаются данные, соответствующие этим группам.

Группы можно создать свои и настроить их с помощью фильтра отображения.

Как это сделать?

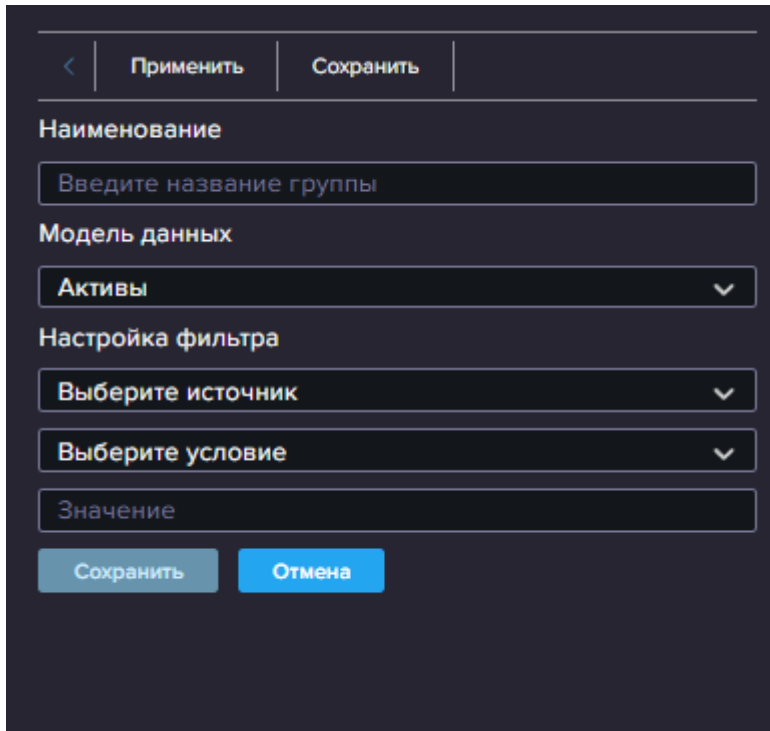
Для этого необходимо нажать на кнопку "Добавить группу". После чего вам откроется раздел добавления и редактирования группы, в котором можно ввести "Наименование", "Модель данных" - откуда будут браться данные. Чтобы более персонализировать группу, можно нажать на кнопку "Добавить фильтр".



В фильтре указываем:

- Источник - какие данные будут выводиться

- Условие - что будет содержать
- Значение - само обозначение по чему будет искать фильтр



The screenshot shows a dark-themed dialog box for configuring a filter. At the top, there are two buttons: "Применить" (Apply) and "Сохранить" (Save). Below these are several input fields and dropdown menus:

- Наименование**: A text input field with the placeholder "Введите название группы".
- Модель данных**: A dropdown menu currently showing "Активы".
- Настройка фильтра**: A section containing two dropdown menus: "Выберите источник" and "Выберите условие".
- Значение**: A text input field.

At the bottom of the dialog, there are two buttons: "Сохранить" (Save) and "Отмена" (Cancel).

После того как ввели все данные можно нажать кнопку "Сохранить", для предварительного просмотра что будет выводиться можно нажать кнопку "Применить".

Далее создается папка, при нажатии на которую будет открываться таблица данных.

