КИРБ
КОМПАНИЯ ИННОВАЦИОННЫЕ РЕШЕНИЯ БЕЗОПАСНОСТИ

Общество с ограниченной ответственностью
«Компания «Инновационные решения безопасности»
Российская Федерация, 123112, г. Москва, Тестовская улица, дом 8, помещение XXXIX, этаж 9, К.1-28,31
Тел.: +7 (495) 139 29 11, факс: +7 (495) 139 29 10
e-mail: insesoco@insesoco.ru

**Утвержден**
34075156.425760.006.ЛУ

**Программное обеспечение**
**«Система автоматического анализа состояния сети»**

**(САСС)**

# РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

34075156.425760.006.И3.03

Листов 16

2021

Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата | Инв. № подл.

## СОДЕРЖАНИЕ

# Перечень терминов и сокращений

| Термин/Сокращение | Определение/Расшифровка |
|---|---|
| ИС | Информационная система |
| ЛВС | Локальная вычислительная сеть |
| ОС | Операционная Система |
| ПО | Программное обеспечение |
| САССС | Система автоматического анализа состояния сети |
| СУБД | Система управления базой данных |
| УЗ | Учётная запись |
| AD | Active Directory |

## Аннотация

Программное обеспечение САССС предназначено для обнаружения и анализа поведения в корпоративной сети устройств, подключенных на основе протокола IP, определения их свойств и запущенных на этих устройствах сетевых приложений, а также ведения журнала изменений в сети.

Данное Руководство предназначено для Пользователя системы.

# 1 Получение учётной записи и регистрация в системе

## 1.1 Получение учётной записи пользователя

Для доступа Пользователя к САССС Администратор сперва создаёт ему персональную учётную запись и сообщает любым доступным способом логин. При этом система автоматически высылает на указанную при регистрации почту Пользователя ссылку, пройдя по которой он должен задать пароль (Рисунок 1).

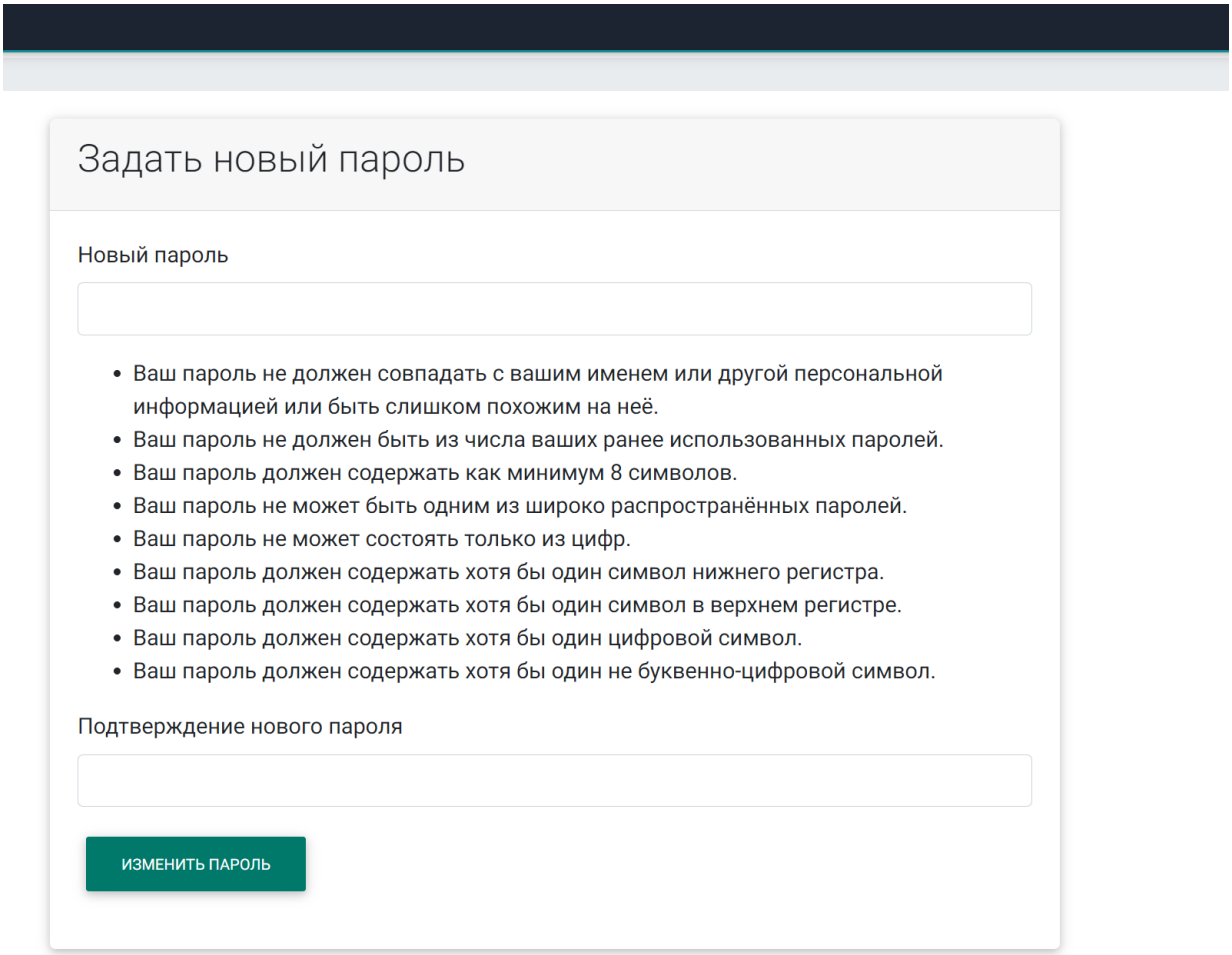


*Рисунок 1. Создание пароля*

## 1.2 Требования к паролю

Согласно требованиям системы, пароль:

- не должен иметь сходство с логином или персональными данными пользователя;
- не должен повторять ранее использованный пароль;

- не должен быть одним из широко распространённых паролей;
- не должен состоять только из цифр;
- должен содержать не менее 8 символов;
- должен содержать одновременно хотя бы один буквенный символ латинского алфавита из нижнего регистра и один из верхнего;
- должен содержать хотя бы один цифровой символ;
- должен содержать хотя бы один не буквенно-цифровой символ.

Пароль действителен в течение 30 дней с момента создания. По окончании срока его действия необходимо создать новый.

### 1.3 Вход в систему

Для входа в панель управления необходимо ввести в браузере web-адрес системы https://<доменное имя>/ и нажать «вход в систему» (Рисунок 2).

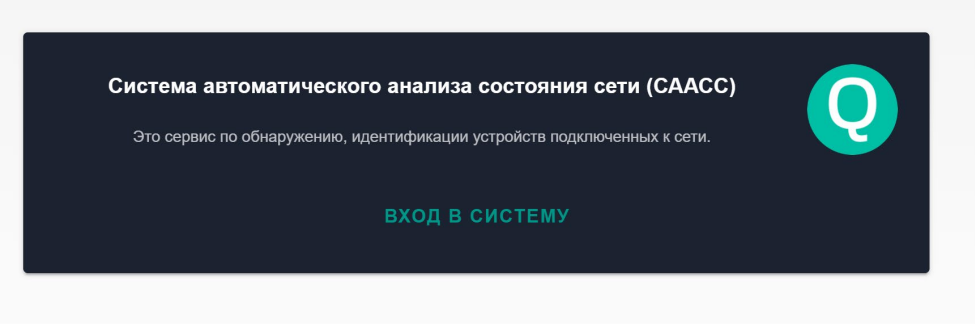


*Рисунок 2. Вход в систему*

В открывшейся странице авторизации ввести «Имя пользователя» (логин) и «Пароль», нажать «Войти» (Рисунок 3).

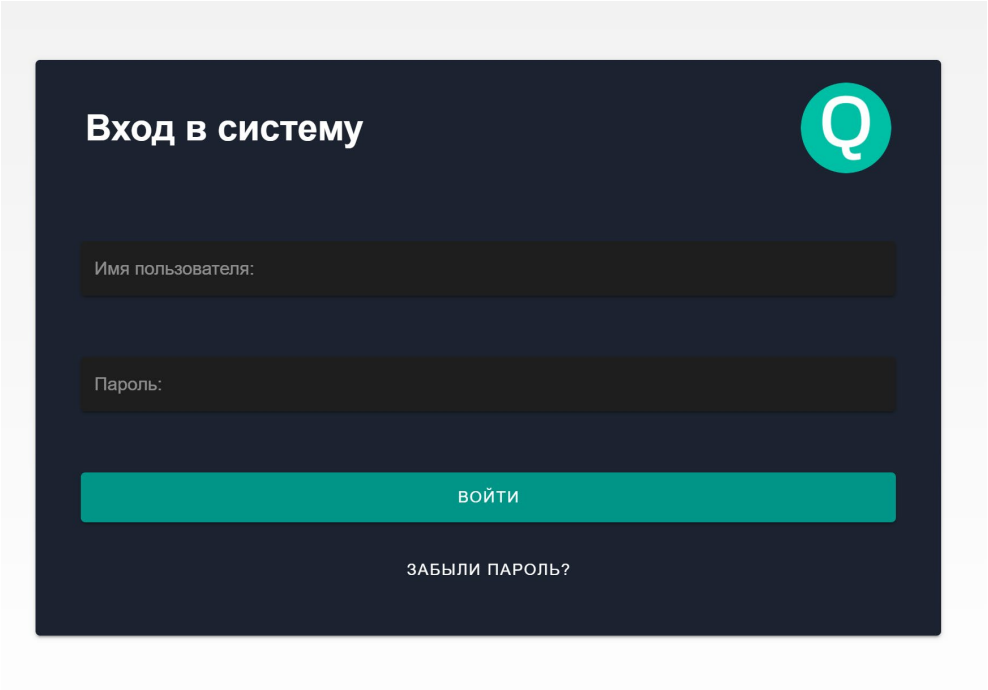


*Рисунок 3. Страница авторизации*

О кнопке «Забыли пароль» подробно описано в пункте 1.4

### 1.4 Процедура изменения (восстановления) пароля

Для восстановления или изменения пароля необходимо нажать «Забыли пароль?» на странице авторизации (Рисунок 3), в открывшейся форме ввести адрес электронной почты, использованной при регистрации в САССС, и нажать «Отправить» (Рисунок 4). После этого на почту придёт письмо со ссылкой для задания нового пароля.

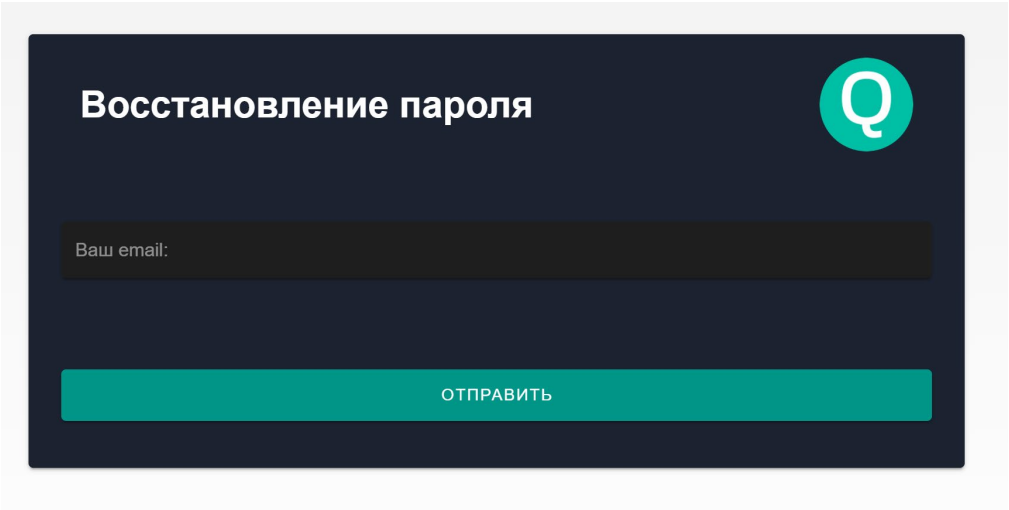


*Рисунок 4. Форма восстановления пароля*

### 1.5 Срок действия учётной записи

Любая неактивная учётная запись, в том числе Учётная запись Администратора системы, блокируется через 60 дней после последнего входа пользователя в систему. Для восстановления учётной записи нужно обратиться к действующему Администратору системы.

### 1.6 Блокировка Учётной записи

В случае неверного ввода пароля более трёх раз учётная запись будет заблокирована. Для разблокировки необходимо обратиться к Администратору системы.

# 2 Общее описание интерфейса

## 2.1 Начальная страница

После успешной авторизации в системе открывается начальная страница, на которой находятся 3 основных раздела: «Активы», «Сканирование», «Отчёты» (Рисунок 5).

Кнопка «Назад» с левой стороны возвращает пользователя на предыдущую страницу.

С правой стороны расположен поиск по базе данных . Поиск осуществляется по всем типам данных (активам, интерфейсам и т.д.).

Для выхода из системы нужно нажать на значок логина в верхнем правом углу, после чего нажать «Выход».

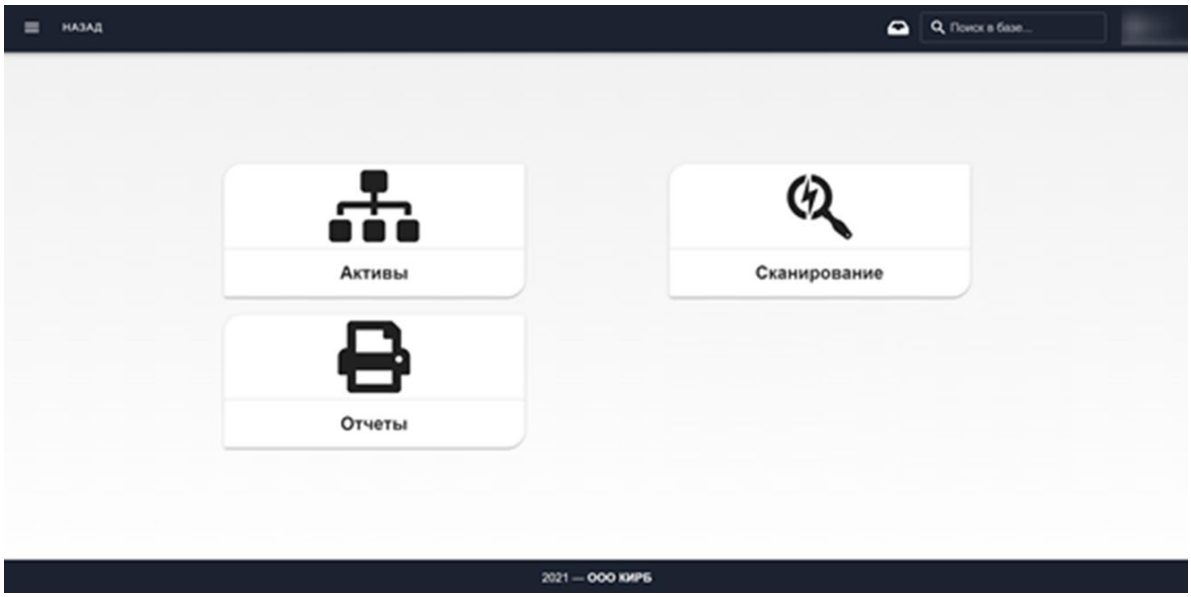


*Рисунок 5. Главная страница*

С левой стороны расположено меню , в котором размещён функциональный список системы доступный пользователю: «Список Активов», «Справочники», «Сканирование», «Отчеты» (Рисунок 6).

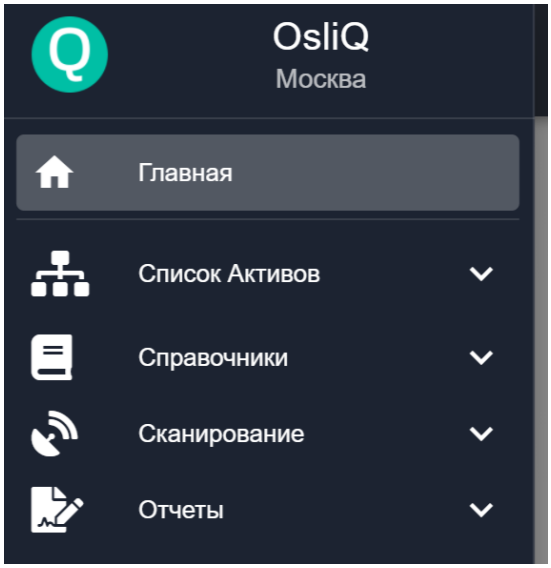


*Рисунок 6. Меню*

## 2.2 Работа с таблицами

Информация в Системе отображается в виде таблиц. В любой таблице данные можно фильтровать при наличии значка «Фильтры». Для этого нажмите «Фильтры» и укажите значение полей для фильтрации (Рисунок 7). Чтобы сохранить группу фильтров, нажмите в разделе «Группы фильтров» , введите название и нажмите «Сохранить». Сохранённые пользовательские группы фильтров доступны в поле «Пользовательские фильтры». Для изменения группы выберите группу фильтров, измените настройки и нажмите , чтобы обновить текущую группу фильтров.

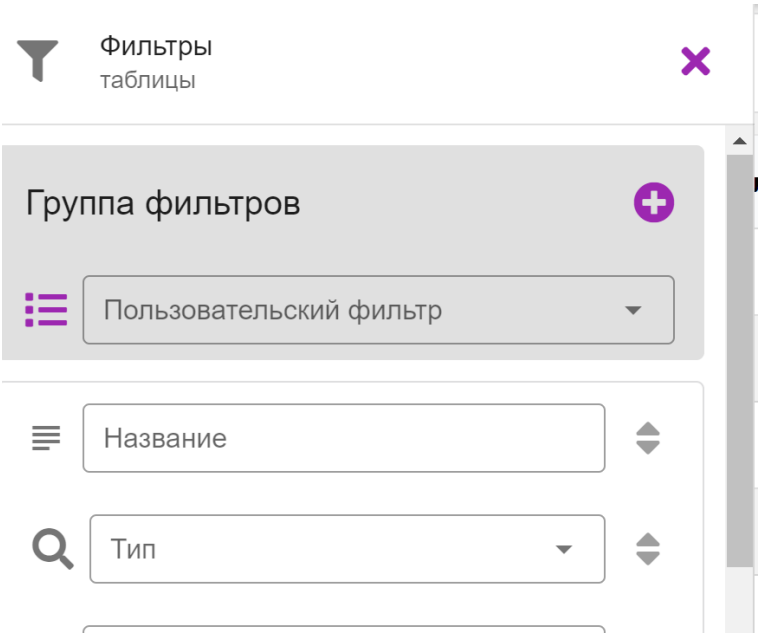


*Рисунок 7. Фильтры*

Чтобы отобразить или скрыть столбцы таблицы, нажмите «Настройка таблицы». Значок означает, что столбец скрыт, значок , что столбец отображён.

Любую таблицу в системе можно экспортировать в формате csv или json, если на странице присутствует значок . Процедура экспорта описана в пункте 2.3.

Чтобы удалить запись в таблице, выберите строку, если в новом окне присутствует значок , строку можно удалить.

Чтобы изменить запись в таблице, выберите строку, если в новом окне присутствует значок , строку можно изменить.

Чтобы изменить количество строк, отображаемых на странице, выберите их количество в левом нижнем углу.

### 2.3 Экспорт данных

Для экспорта данных необходимо нажать на значок и выбрать в выпадающем списке необходимый формат данных (Рисунок 8).

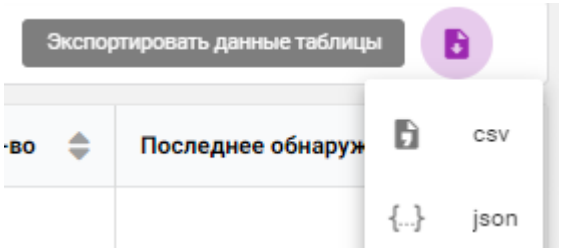


*Рисунок 8. Выбор формата данных*

После выбора формата на несколько секунд отобразится информационное сообщение о запуске задачи (Рисунок 9).

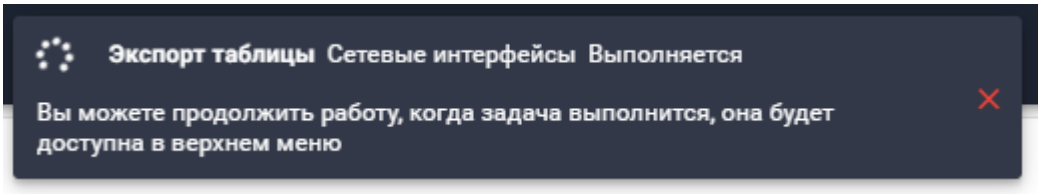


*Рисунок 9. Информационное сообщени о запуке задачи*

В процессе формирования файла экспорта на экране отображается информация о запущенной задаче (Рисунок 10).

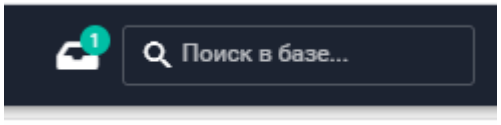


*Рисунок 10. Отображение о запущенной задаче*

При нажатии на задачу открывается детальная информация, где виден прогресс задачи и имеется возможность её отмены (Рисунок 11).

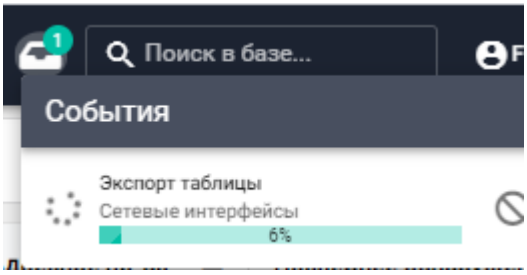


*Рисунок 11. Детальная инфомация о задаче*

После успешного формирования файла экспорта отобразится информационное сообщение (Рисунок 12).


*Рисунок 12. Информационное сообщение о завершении задачи*

Файл готов для выгрузки и может быть скачан, для чего необходимо последовательно нажать на значок задачи и выгрузки (Рисунок 13).

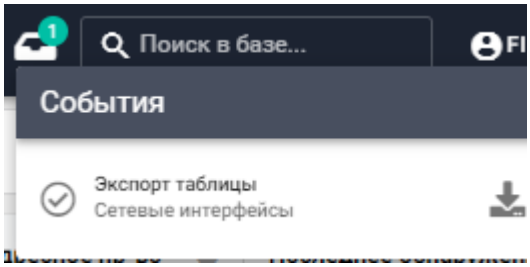


*Рисунок 13. Выгрузка файла*

Файл выгрузки именуется текущей датой (Рисунок 14).


*Рисунок 14. Файл выгрузки*

### 2.4 Список Активов

Активом в системе считается любое сетевое устройство или объект AD

Раздел Активов содержит подразделы:

- активы AD, собранные из доменной структуры;

- активы, обнаруженные при сканировании сети;
- активы, полученные в результате опроса Windows машин.

В Таблице 1 перечислены виды активов по разделам.

Таблица 1. Список Активов

| | |
|---|---|
| **Активы AD** | |
| Домены | Таблица объектов единиц верхней иерархии доменной структуры Active Directory сканируемого пространства |
| Группы | Таблица групп Active Directory, объединяющая различные объекты |
| Компьютеры | Таблица объектов типа «рабочая станция» или «сервер», входящие в домен |
| Пользователи | Таблица пользовательских и технических учётных записей Active Directory |
| **Активы сетевые** | |
| Активы сетевые | Таблица сетевых объектов, полученных в результате сканирования различными методами. |
| Сетевые интерфейсы | Таблица сетевых интерфейсов, обнаруженных при сканировании. Сетевой интерфейс принадлежит сетевому активу |
| Список ОС | Таблица найденных операционных систем |
| Сетевые сервисы | Таблица найденных сетевых сервисов и портов |
| Типы активов | Таблица внутренней типизации найденных сетевых активов |
| **Активы Windows** | |
| Активы Windows | Таблица объектов, найденных в процессе сканирования по протоколу WMI |
| Список ОС | Агрегированная таблица операционных систем найденных путем сканирования по протоколу WMI |
| Список обновлений | Таблица обновлений Windows, полученная в результате сканирования по протоколу WMI |
| Список ПО | Агрегированная таблица установленного на устройства ПО, полученная в результате сканирования по протоколу WMI |

### 2.5 Справочники

Данный раздел содержит доступную только для чтения информацию, необходимую для работы системы. При попытке изменения данных будет выдано

сообщение о недостаточном уровне прав.

Раздел содержит:

| | |
|---|---|
| Адресные пространства | Список адресных пространств, создаваемых для верхнеуровневого объединения сетей. По умолчанию, система содержит одно сетевое адресное пространство «Основное». В случае, если организации используют собственные независимые пространства, или в организации есть пересекаемая адресация, создаются различные адресные пространства. В каждом адресном пространстве размещаются свои Серверы-агенты |
| Сети | Таблица сетей предприятий с привязкой к адресному пространству и организации |
| Адрес | Адреса расположения подразделений организаций, однозначно определяющие физическое расположение |
| Подразделение | Список территориальных подразделений организации |

### 2.6 Сканирование

Сканирование – процесс обнаружения активов в сети. В зависимости от типа выбранного сканирования задаётся список необходимых для заполнения атрибутов. Описание процесса создания задач сканирования содержится в Руководстве Администратора. Список задач сканирования доступен Пользователю только для просмотра.

Раздел «Сканирование» содержит:

| | | |
|---|---|---|
| Задачи | Таблица списка задач сканирования. | |
| Параметры | Агенты | Таблица установленных агентов в системе с указанием адресного пространства, в котором агент производит сканирование |
| | Цели сканирования | Таблица объектов для сканирования. Включает в себя сети, хосты и, при необходимости, их исключения |
| | Учётные данные | Таблица технических Учётных записей для получения привилегированного доступа при сканировании объектов в сети. Если сканирование производиться без Учётных данных, система получит только общедоступные данные об объекте сканирования |

## 2.7 Отчёты

Раздел содержит 2 подраздела, Системные отчёты и Журналы почтовых серверов.

Системные отчёты – предустановленные в системе отчёты, позволяющие получить статистические данные по распределению активов (Рисунок 15).

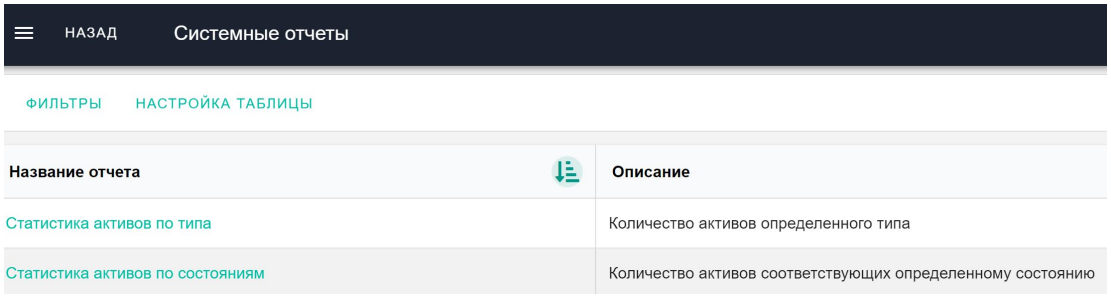


*Рисунок 15. Системные отчеты*

Журналы почтовых серверов – таблица агрегированных данных, полученных из журналов почтовых серверов Exchange для дальнейшего создания отчётов об использовании почтовой системы.

# 3 Технология работы

Пользователь в системе имеет возможность работать с полученной в результате сканирования информацией и выполнять следующие действия:

- просматривать данные;

- экспортировать данные в формат CSV и JSO;

- получать результаты из существующих в системе отчетов.

При необходимости администратор может расшить полномочия пользователя, создав дополнительные роли и предоставив их пользователю.