«Инфомаксимум»
(Общество с ограниченной ответственностью)

Proceset

Руководство прикладного администратора

2019 г.

Содержание

1. Общие положения

1.1 Основные термины

Термин	Описание
GPO	набор правил или настроек, в соответствии с которыми производится настройка рабочей среды приёма/передачи (Windows, X-unix и другие операционные системы с поддержкой сети).
GraphQL	стандарт декларирования структуры данных и способов получения данных, который выступает дополнительным слоем между клиентом и сервером
Https	расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов SSL или TLS
RocksDB	высокопроизводительная встраиваемая СУБД на основе LSM-tree с открытым исходным кодом (лицензия Apache 2.0) от компании Facebook
Unix	система описания моментов во времени, принятая в Unix и других POSIX-совместимых операционных системах. Определяется как количество секунд, прошедших с полуночи (00:00:00 UTC)
UTC	всемирное координированное время, стандарт времени, принятый на Земле
Агент мониторинга	приложение proceset.agent, которое устанавливается на компьютер сотрудника и собирает статистику об его активности
Активность сотрудника	сведения о работе сотрудника за компьютером
Карта процесса	схема последовательности событий (операций, которые осуществляют сотрудники в ходе выполнения процесса), и связей между ними
Профиль сотрудника	информация о сотруднике компании, включающая общие сведения, настройки доступа и список источников сбора информации
Репозиторий	место, где хранится и поддерживается исходный код системы
Удаленный установщик	приложение, с помощью которого администратор Системы может удалённо установить на ПК агенты мониторинга, а также частично осуществлять мониторинг состояния агента

1.2 Основные сокращения

Сокращение	Описание
АС	Автоматизированная система
ЖА	Журнал аудита
ИБ	Информационная безопасность
ИС	Информационная система
ММАП	Модуль мониторинга активности пользователя
МНА	Модуль настройки и аналитики
ОС	Операционная система
ПК	Персональный компьютер
РД	Роли доступа
GPO	Group Policy Object

2. Инструкции по установке Системы

2.1 Установка Системы

Для установки Системы необходимо чтобы были соблюдены регламенты работы Системы. (см. Общее описание системы п.3.2). Установка Системы должна производится пользователем с правами локальной группы безопасности – Administrators.

В состав дистрибутива входит:

- jre-8u191-windows-x64;
- jar-файлы;
- Исполняемый exe-файл;
- js-скрипты;
- Исполняемые файлы агентов;

Установка Системы: запустить файл setup_proceset.exe (Рисунок 1) Согласиться с условиями пользовательского соглашения.

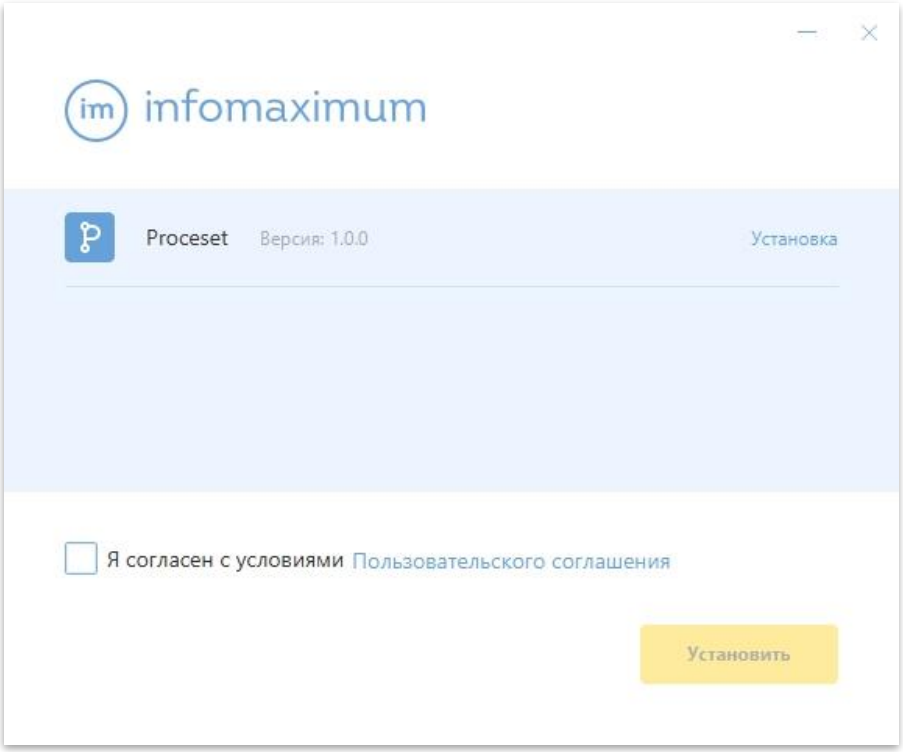

Рисунок 1- Установка системы

Нажать «Установить», далее осуществляется установка системы (Рисунок 2)

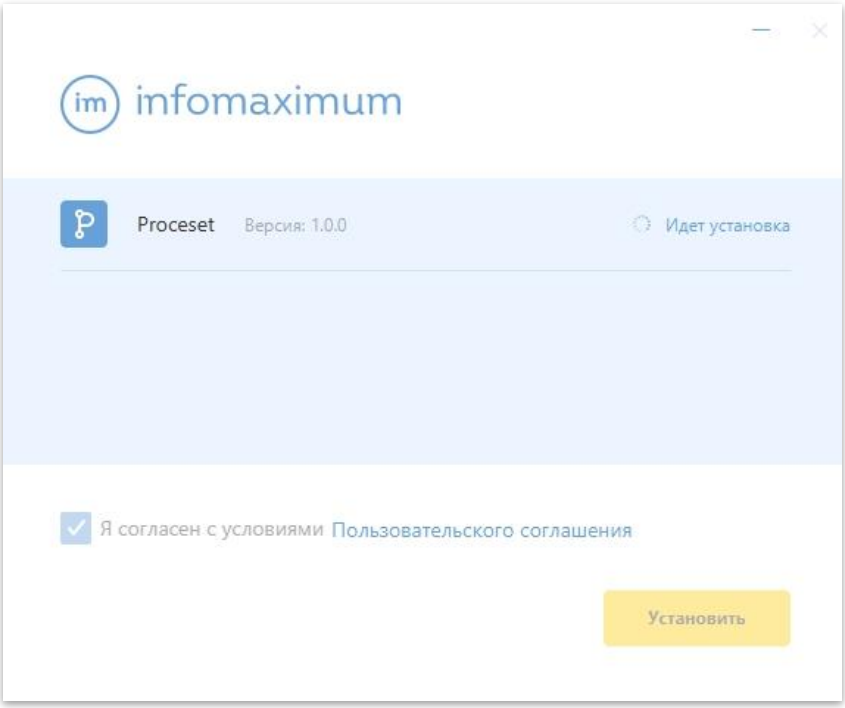

Рисунок 2 - Установка Системы

После установки Системы, в браузере автоматически откроется веб-страница Системы, на которой необходимо задать учётные данные администратора Системы (Рисунок 3).

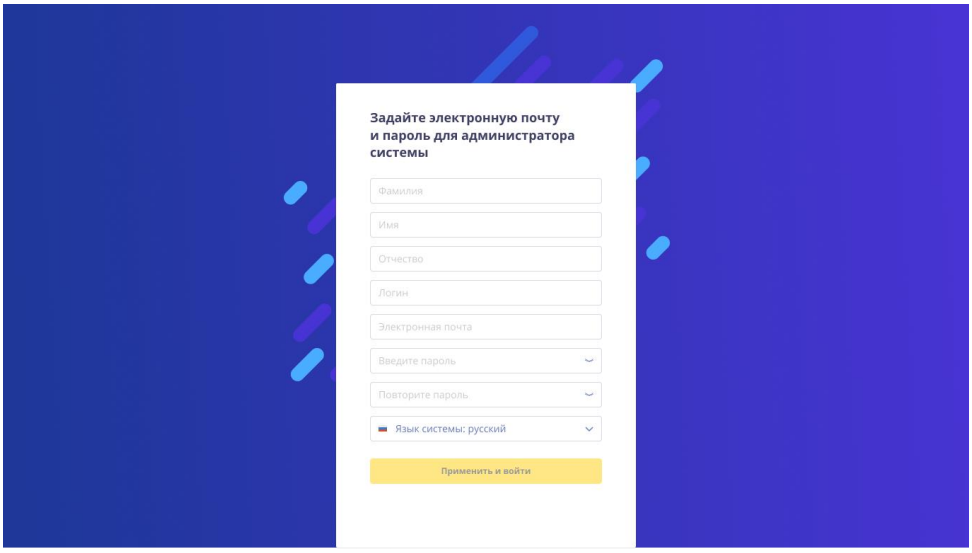

Рисунок 3- Создание учётной записи администратора Системы

Необходимо указать:

- Фамилия;
- Имя;
- Отчество;
- Логин;
- Электронная почта;
- Пароль;
- Язык системы.

Система устанавливается в: C:\Program Files\Infomaximum. Изменение пути установки Системы невозможно.

Файлы АС располагаются:

- C:\Program Files\Infomaximum
- C:\ProgramData\Infomaximum

Агент мониторинга находится в отдельной папке (см. п. 2.3)

База данных Системы располагается по адресу: C:/ProgramData/Infomaximum/database. Для работы с базой данной необходимо использоваться специальный инструмент. (см. Руководство администратора информационной безопасности). Конфигурационные файлы Системы располагаются по адресу: C:\ProgramData\Infomaximum\config.

Запуск Системы осуществляется автоматически после установки Системы и при каждом запуске ПК. Остановить/перезапустить Систему возможно посредством отключения Службы. Название службы «Infomaximum». Также посредством Служб можно отключить автоматический запуск Системы.

2.2 Скачивание агентов мониторинга

При первом входе в Систему открывается окно выбора и скачивания агента для сбора информации с компьютеров сотрудников, участвующих в исследуемых процессах (Рисунок 4).

Страница скачивания агента находится в Системе по адресу: Меню/Настройки/ Скачать агент.

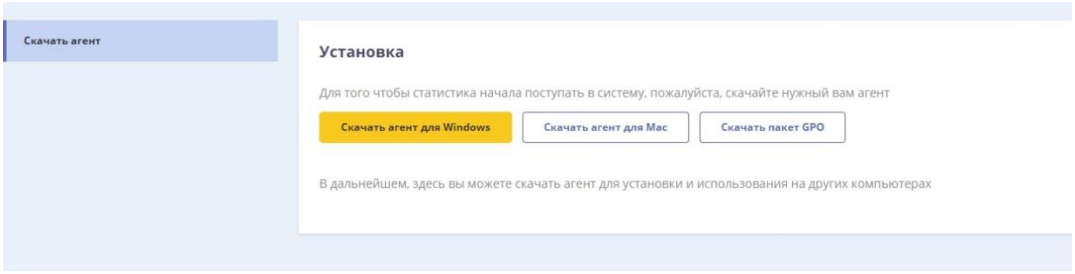

Рисунок 4 - Скачивание агентов системы

2.2.1 Настройка Ключа API для агента мониторинга

Перед началом скачивания агента следует предварительно создать безопасный ключ API для агента мониторинга. Для создания Ключа API с клиентской авторизацией (взаимной аутентификацией) необходимо выбрать создание безопасного ключа API. (Рисунок 5)

Для создания безопасного ключа необходимо:

- Ввести название ключа API;
- Загрузить клиентский сертификат безопасности;

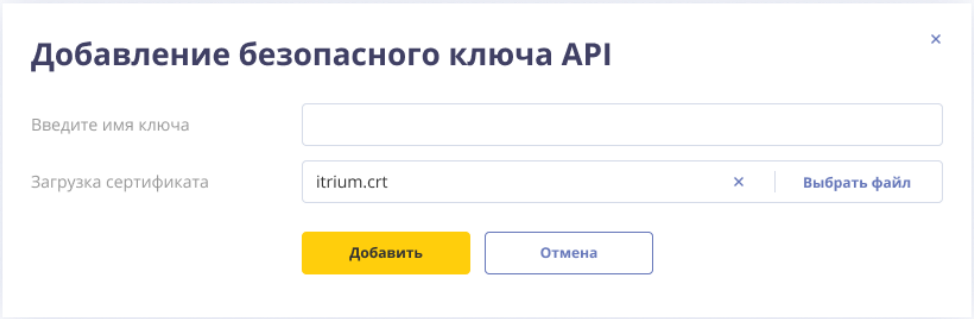

Рисунок 5- Добавление безопасного ключа

Для безопасного ключа API необходимо загрузить SSL сертификат, который в последствии будет использован для авторизации агента мониторинга с сервером.

Далее в привилегиях Ключа API устанавливаем привилегию ключа «Агент мониторинга» на «Чтение». (Рисунок 6)

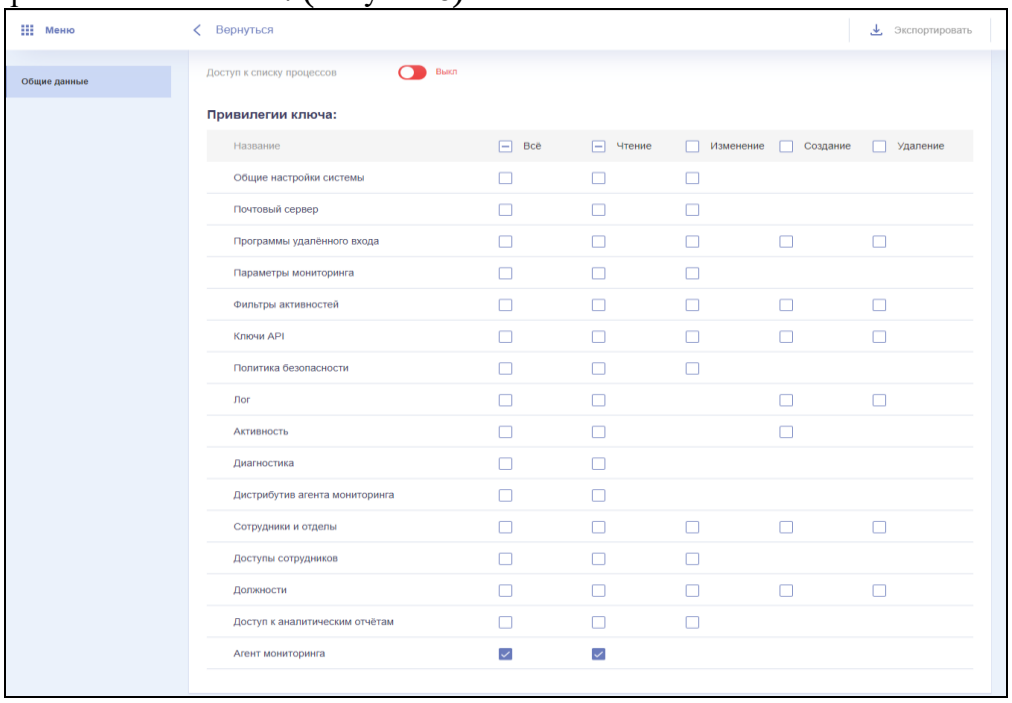

Рисунок 6 - Привилегии для Ключа API

- Сохранить Ключ API и перейти к скачиванию агента мониторинга.

2.2.2 Скачивание агента для Windows

- Указать адрес сервера
- Указать безопасный Ключ API с клиентским сертификатом (который планируется использовать для агента мониторинга)
- Выбрать тип авторизации сотрудника (см. 2.2.3);
- Произвести выбор параметра использовать / не использовать «Прокси» (в случае использования, заполнить все сопутствующие параметры);
- Скачать агент исходя из настроенных параметров (Рисунок 7).

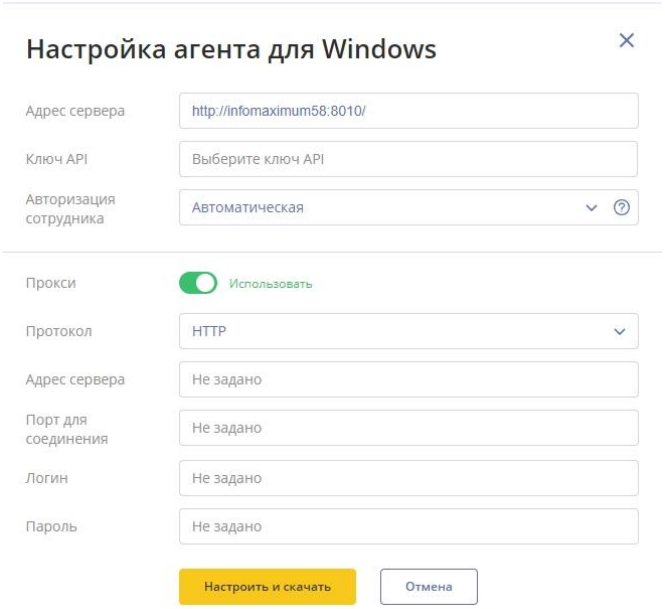

Рисунок 7 - Настройка агента

2.2.3 Тип авторизации сотрудника

Автоматическая авторизация предполагает, что авторизация сотрудника в агенте происходит автоматически. Данный вариант подходит в случае, когда у каждого сотрудника отдельная учётная запись на компьютере.

Полуавтоматическая авторизация предполагает, что каждый раз при входе в Систему будет запрашиваться авторизация в агенте. Данный вариант подходит, когда одной учётной записью на компьютере пользуется несколько сотрудников.

Ручная авторизация предполагает, что сотрудник может включать и выключать сбор статистики по мере необходимости. Вариант подходит, когда сотрудник удалённо работает со своего личного компьютера.

2.2.4 Скачивание агента GPO

Скачать пакет GPO можно из интерфейса Системы по адресу: Меню/Настройки/Скачать агент/Скачать пакет GPO. (см. 2.2.4) Перед скачиванием необходимо произвести настройку (Рисунок 8).

- Указать адрес сервера (проставляется автоматически, при необходимости возможно поменять);
- Указать Ключ API для агента мониторинга (см. 2.2.1)
- Настроить автообновление (включает или выключает автообновления агента мониторинга);
- Указать тип авторизации сотрудника (см. 2.2.3)
- Прокси сервер (использовать/не использовать);
- Нажать «настроить и скачать».

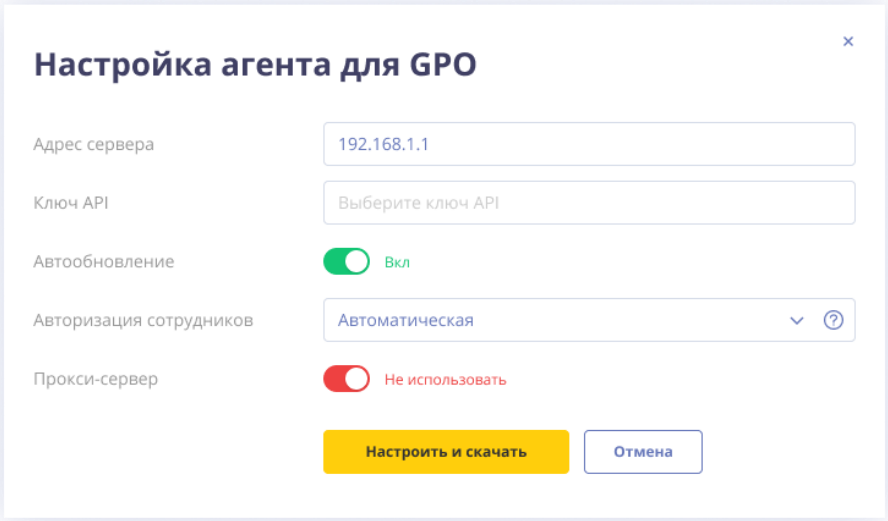

Рисунок 8 - Настройка агента для GPO

Происходит скачивание архива, в котором находится два файла:

1. agent_setup (файл для установки);
2. setting_mst (файл конфигурации).

2.3 Установка агентов мониторинга

Существует 3 способа установки агента мониторинга.

- С помощью установщика агента (см. 2.3.2). Осуществляется скачивание файла и его установка на конкретный ПК. Установка одновременно на несколько ПК невозможна.
- С помощью удаленного установщика (см. 2.3.3). Возможна установка одновременно на несколько ПК.
- С помощью пакета GPO (см. 2.3.3.8). Данный способ подходит для опытных администраторов. Возможна одновременная установка на несколько машин в рамках домена.

2.3.1 Настройка клиентского сертификата

Прежде чем устанавливать агент мониторинга по безопасному соединению необходимо выполнить п.2.2.1, п.2.2.2, п.4.1. После того как инсталлятор агента мониторинга загружен необходимо выполнить следующие действия:

- Запустить в windows утилиту «mmc»;
- Нажать Файл/ «Добавить или удалить оснастку»;
- Выбрать пункт «Управление сертификатами для учётной записи компьютера»;
- Добавить корневой сертификат в «Доверенные корневые центры сертификации»;
- Добавить тот же клиентский сертификат, который был указан в Ключе API, который в свою очередь используется для скаченного инсталлятора агента мониторинга в «Личное»;
- Открыть свойства клиентского сертификата, найти поле «Отпечаток» - это есть идентификатор сертификата. (Рисунок 9)

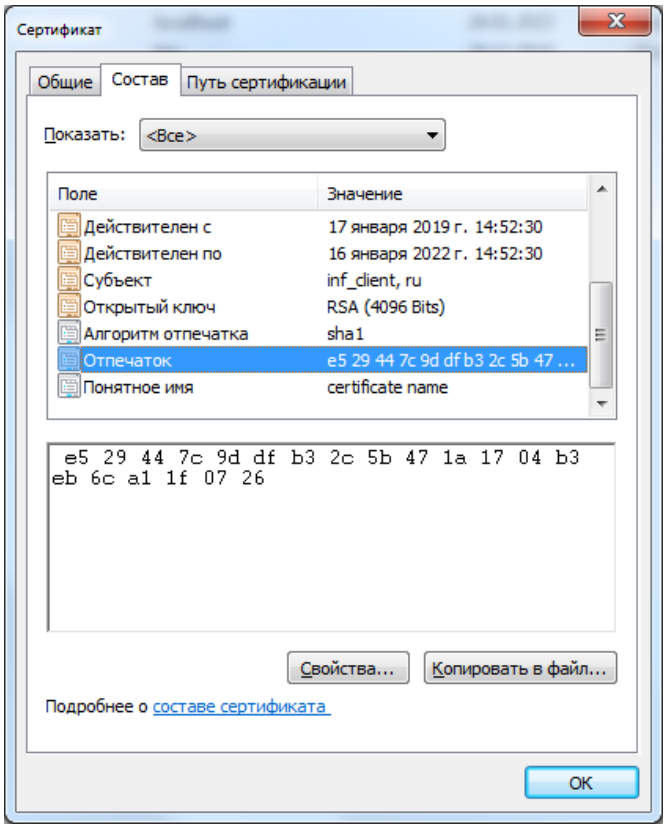

Рисунок 9 - Свойства клиентского сертификата

- Необязательно, для проверки: открыть редактор реестра, открыть раздел HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\MY\Certificats Тут должен появиться клиентский сертификат с этим же значением отпечатка. (Рисунок 10)

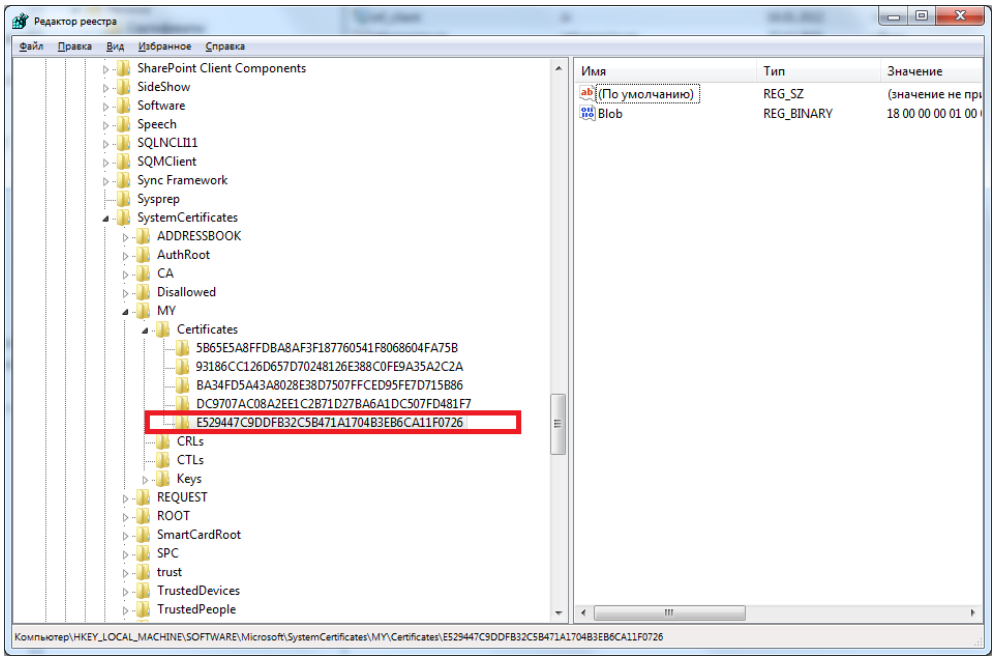

Рисунок 10 - Отпечаток клиентского сертификата

Если настройка клиентского сертификата не будет осуществлена, то соединение агента мониторинга и сервера не будет осуществлено.

2.3.2 Установщик агента

После настройки клиентского сертификата (см. п. 2.3.1) можно перейти к установке агента мониторинга. Если скачивание агента происходит из интерфейса Системы, то в установщике поля принимают значения, указанные при скачивании. (см. 2.2) (Рисунок 11)

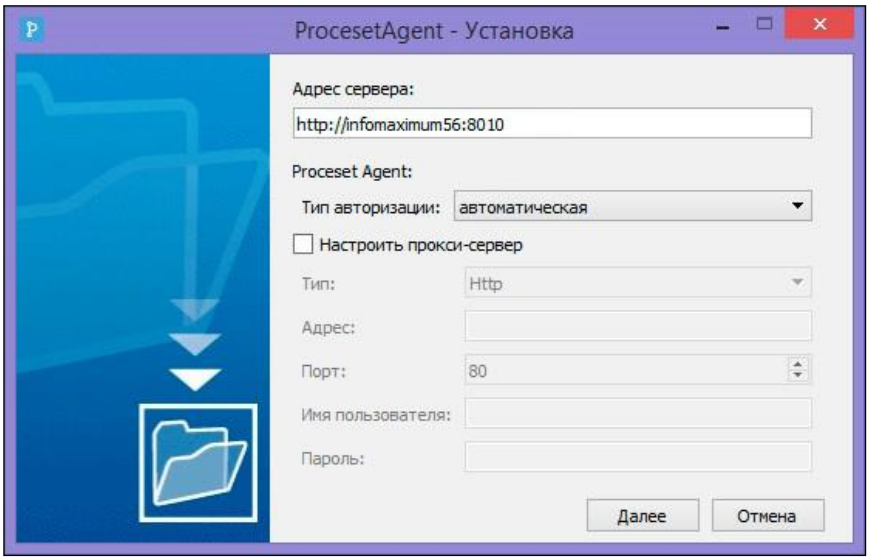

Рисунок 11 - Установка агента

Если настройка не осуществлялась в web-интерфейсе, то при установке агента необходимо вручную настроить параметры (Рисунок 12)

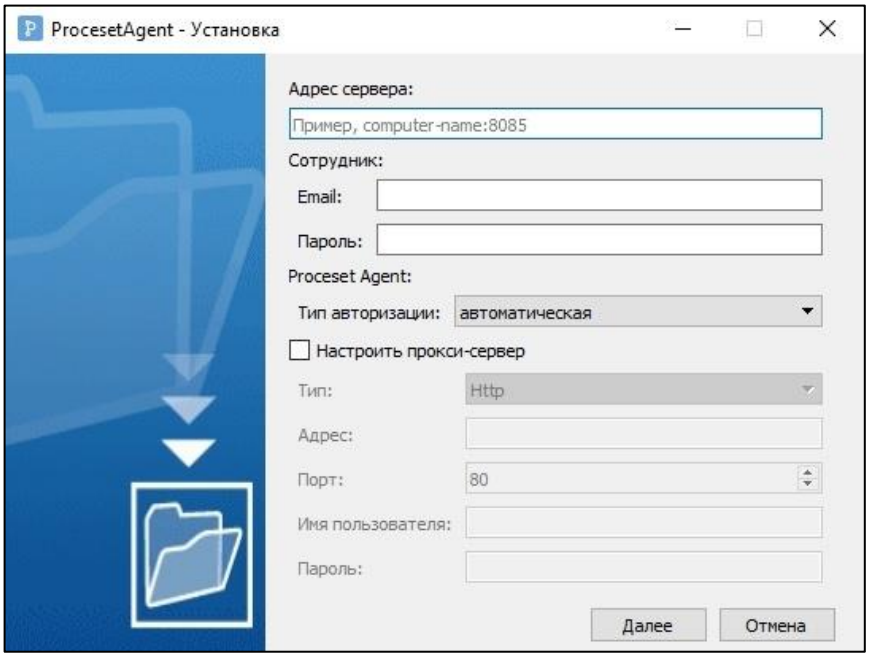

Рисунок 12 - Установка агента без заданных ранее настроек

Необходимо указать следующие настройки:

- Адрес сервера (указывается адрес сервера, на который агент будет отправлять статистику);
- E-mail (логин сотрудника);
- Пароль;

- Необходимо указать учетные данные пользователя, который имеет доступ в Систему (это не обязательно должен быть сотрудник с администраторскими правами)
- Выбрать тип авторизации (см. п. 2.2.2);
- Произвести настройку прокси-сервера (при необходимости).

2.3.3 Удаленный установщик

Приложение «Удаленный установщик» устанавливается вместе с сервером. Местоположение приложения: C:\Program Files\Infomaximum\agent. Название приложения удаленного установщика: remote_installer.exe (Рисунок 13) Над таблицей указывается адрес сервера, на который отправляется статистика.

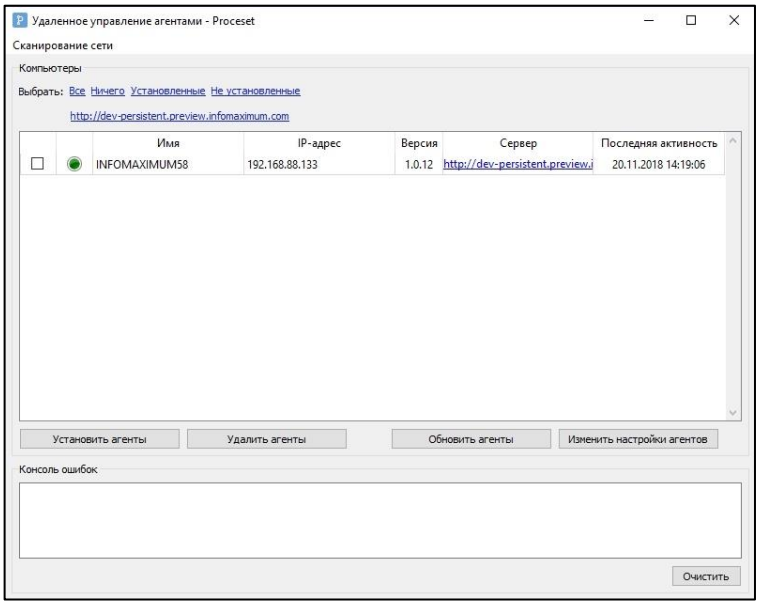

Рисунок 13 - Основное окно «Удаленного установщика»

2.3.3.1 Сканирование сети

Сканирование необходимо,чтобы найти ПК, на которые требуется установить агенты мониторинга.

Сканировании сети бывает следующих видов:

- Простое сканирование (происходит поиск ПК в домене);
- Настраиваемое сканирование.

При настраиваемом сканировании возможно указать сетевой адрес, в котором будет осуществлён поиск, или же указать диапазон IP-адресов (Рисунок 14).

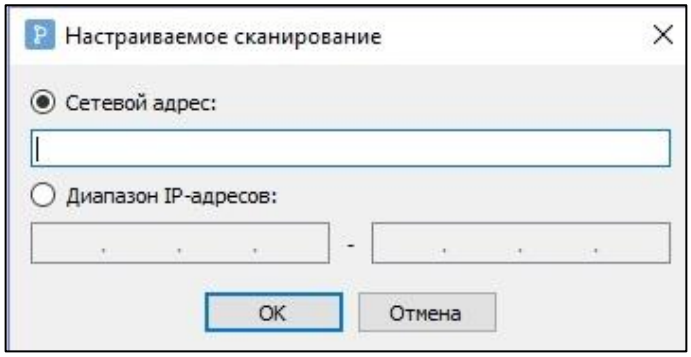

Рисунок 14 - Настраиваемое сканирование

2.3.3.2 Индикатор состояния агента

В таблице существует индикатор состояния агента (иконка цветного круга):

- Зелёный индикатор (агент мониторинга установлен на ПК);
- Красный индикатор (проблемы с соединением агента мониторинга и сервера);
- Серый индикатор (агент мониторинга не установлен на ПК).

2.3.3.3 Данные таблицы

В таблице указываются следующие сведения о всех ПК, которые были найдены при сканировании сети:

- Имя (имя ПК);
- IP-адрес (адрес ПК);
- Версия (версия агента мониторинга; указывается в случае, если агент установлен);
- Сервер (адрес сервера, с которым соединяется агент мониторинга);
- Последняя активность (дата и время, когда последний раз агент мониторинга присылал активность сотрудника).

Для обновления данных в таблице необходимо заново провести сканирование сети.

2.3.3.4 Консоль ошибок

В окне «Консоль ошибок» указываются ошибки, которые происходят при установке агентов и другие ошибки удаленной установки, которые происходят на удаленных ПК.

2.3.3.5 Сортировка данных

В Системе возможно осуществлять сортировку данных в строке «Выбрать» по следующим значениям:

- «Все» (выбираются все агенты мониторинга в таблице);
- «Ничего» (снимаются «галочки» выбора со всех агентов мониторинга в таблице);
- «Установленные» (выбираются все агенты, которые установлены на ПК);
- «Не установленные» (выбираются все агенты, которые НЕ установлены на ПК).

2.3.3.6 Установка агентов

Для установки агентов необходимо (Рисунок 15):

1. Осуществить сканирование сети (см. п. 2.3.3.1);
2. Выбрать ПК, на которые требуется установить агенты мониторинга;
3. Нажать «Установить агенты»;
4. Указать нужные настройки агента мониторинга (аналогично п. 2.3).

После установки агентов начинается сбор данных для более точного анализа процессов. Для более корректного анализа требуется некоторое время для накопления статистики – от двух недель и более (в зависимости от анализируемого процесса).

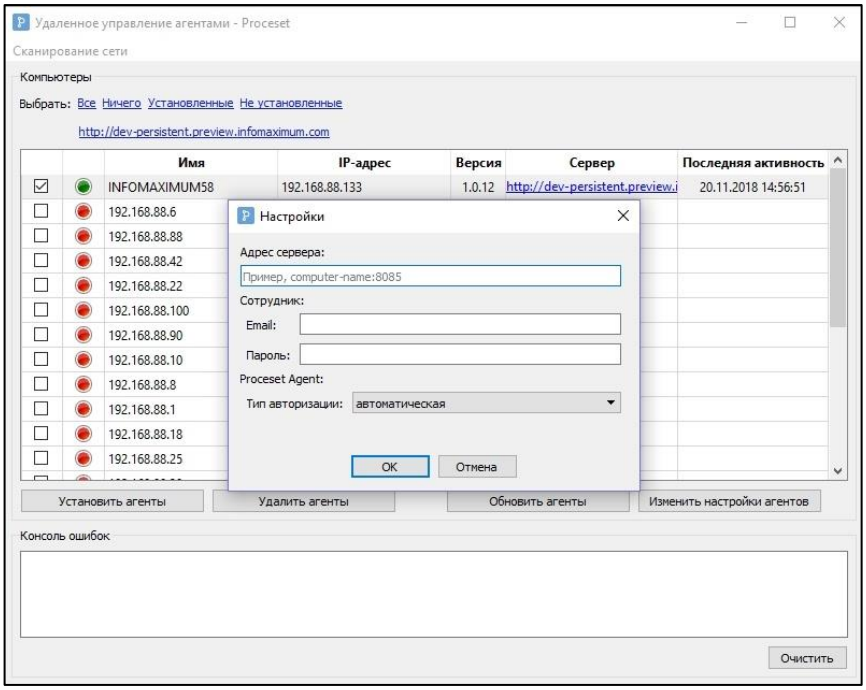

Рисунок 15 - Установка агентов в удалённом установщике

2.3.3.7 Восстановление соединения агента и сервера

Если в таблице агент отмечен красным индикатором, то существуют проблемы с соединением агента и сервера. (см. 2.3.3.2) Для восстановления соединения необходимо (Рисунок 16):

- Нажать на индикатор;
- Нажать «Исправить»;
- Указать имя пользователя (логин от учётной записи Windows/MacOS; учётная запись должна иметь права администратора);
- Указать пароль от учётной записи;
- Выбрать ОС. Если выбрана операционная система MacOS, то необходимо указать дополнительный параметр – SSH-порт (по умолчанию на MacOS – 22);
- Выбрать действие: «Применить для всех» (применяет настройки для всех выбранных ПК в таблице) или «Применить для текущего» (применяется для текущего ПК).

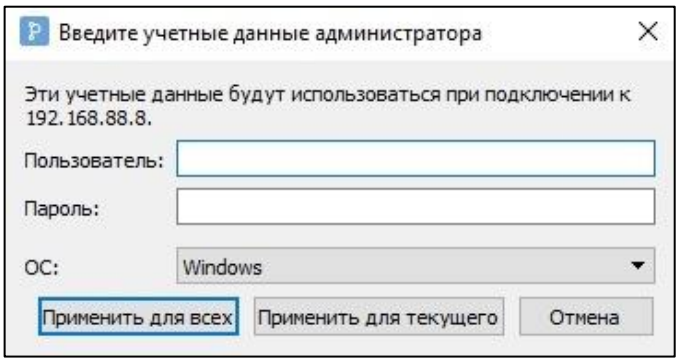

Рисунок 16 - Восстановление доступа

2.3.3.8 Пакет GPO

После скачивания пакета GPO (см. 2.2.4) необходимо разархивировать архив с файлами, открыть командную строку от имени администратора.

Для установки через политику GPO пользователь ПК должен обладать правами администратора предприятия (admin enterprise) или администратора домена (admin domain).

Далее необходимо ввести команду для установки GPO пакета, в которой указать название установочного файла (agent_setup) и файла настроек (setting_mst). Команда для установки GPO пакета регламентируется политиками Windows.

2.4 Запуск и остановка агента мониторинга

2.4.1 Запуск агента мониторинга

Для запуска агента мониторинга не требуется ручное действие. Агент мониторинга автоматически запускается после установки, а также при старте операционной системы.

Агент мониторинга состоит из службы (agent_service.exe) и инспектора (agent_inspector.exe).

Служба agent_service.exe – приложение, которое запускает инспекторов в каждой пользовательской сессии, выгружает их из неактивной сессии, перезапускает в случае сбоя. Служба agent_service.exe автоматически загружается при загрузке Windows. Процесс службы всегда один.

Инспектор – приложение агента мониторинга. Его запускает служба agent_service.exe в каждой пользовательской сессии автоматически. Процессов инспектора может быть несколько (в диспетчере задач несколько agent_inspector.exe, по одному в каждой активной сессии).

2.4.2 Остановка агента мониторинга

Закрыть службу agent_service.exe агента мониторинга невозможно. Возможно «снять задачу» процесса agent_service.exe (для этого пользователь должен обладать администраторскими правами Windows). После перезагрузки ПК процесс agent_service.exe запустится автоматически, даже если он был закрыт в предыдущей пользовательской сессии.

Для того, чтобы остановить приложение агента мониторинга, его можно только удалить. Удаление может произвести только пользователь с администраторскими правами Windows (см. 2.5).

2.5 Удаление агента мониторинга

2.5.1 Удаление агента мониторинга на одном ПК

Удаление агента мониторинга на конкретном ПК осуществляется следующим образом:

- Перейти в C:\Program Files\ProcesetAgent;
- Открыть agent_setup.exe;
- Подтвердить процесс удаления агента мониторинга.

2.5.2 Массовое удаление агентов мониторинга

Массовое удаление агентов мониторинга (сразу на нескольких ПК) осуществляется с помощью «удалённого установщика» (см. 2.3.3):

- Открыть «удалённый установщик»;
- Выделить необходимые ПК, на которых установлены агенты мониторинга;
- Нажать «удалить агенты»;
- Подтвердить действие.

2.6 Обновление агента мониторинга

Обновление агента мониторинга производится в автоматическом режиме, кроме случая, когда агенты мониторинга устанавливаются посредством политики GPO и в настройках политики параметр «автообновления» выключен. (см 2.2.4). Обновление агентов возможно произвести в ручном режиме. Восстановление старой версии агента мониторинга невозможно.

2.6.1 Автообновление

Раз в час происходит соединение агента мониторинга и сервера, агент запрашивает информацию по новому обновлению. Если на сервер загружена новая версия агента, то агент производит скачивание обновления и осуществляет его установку.

При установке новой версии агент мониторинга производит резервное копирование (бекап) текущей версии. Если обновление проходит успешно (без ошибок), то данные резервного копирования удаляются. Если при обновлении произошли ошибки, то агент восстанавливает старую версию с помощью данных резервного копирования.

2.6.2 Ручное обновление

Ручное обновление агента мониторинга можно осуществить в приложениях:

1. Удалённый установщик (см. 2.3.33);
2. Конфигуратор агента;
3. Локальный установщик (установщик агента) (см. 2.3.2).

Для обновления с помощью удалённого установщика необходимо:

- Запустить удаленный установщик;
- Выделить необходимые ПК, на которых требуется обновления агента мониторинга;
- Нажать «Обновить агенты»;
- Подтвердить действие.

Для обновления с помощью конфигуратора агента мониторинга необходимо:

- Запустить конфигуратор агента. (расположение агента: C:\Program Files\ProcesetAgent; название приложения: agent_configurator.exe);
- Нажать «Обновить агента».

Для обновления с помощью локального установщика агента мониторинга необходимо:

- Открыть новую версию agent_setup.exe;
- Подтвердить действие обновления агента мониторинга.

Ручное обновления с помощью локального установщика происходит, если устанавливается новая версия локального установщика (agent_setup.exe).

Новую версию можно ставить на уже установленную старую, установщик автоматически предложит обновить версию агента мониторинга.

3. Настройка Системы

Для корректной работы и управления сотрудниками в Системе существует ряд настроек. «Настройки» находятся в левом меню, которое открывается по клику на пиктограмму «Меню» в левом верхнем углу (Рисунок 17).

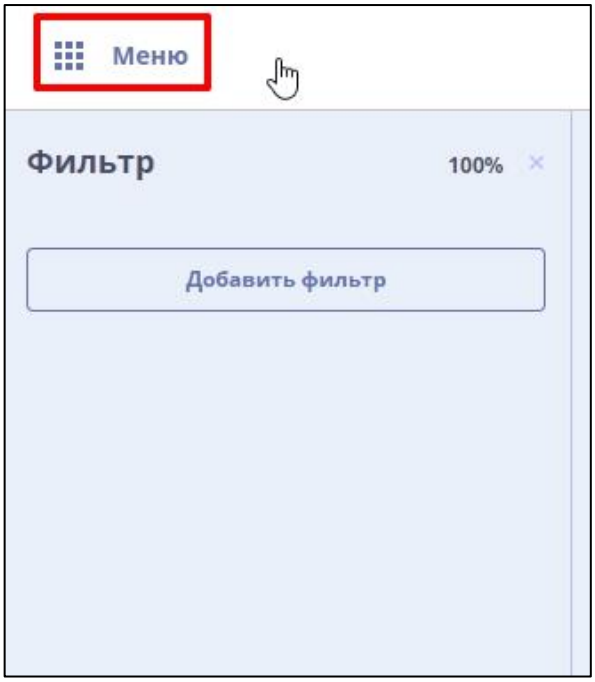

Рисунок 17 - Меню

Все настройки Системы разделены на две группы:

- «Настройка системы»;
- «Настройка компании».

Произвести переход в разделы настроек можно через «Меню».
«Настройки системы» включает в себя следующее настройки:

- Общие данные;
- Почтовый сервер;
- Ключи API;
- Мониторинг;
- Фильтр по активностям;
- Программы удаленного входа;
- Безопасность;
- База данных.

В Настройка можно также перейти на следующие страницы:

- Сотрудники;
- Должности;
- Роли доступа.

3.1 Раздел «Настройка системы»

3.1.1 Общие данные

На странице «Общие данные» можно задать/изменить следующие параметры: (Рисунок 18):

- изменить язык системы;
- указать начало недели
- задать формат инициалов

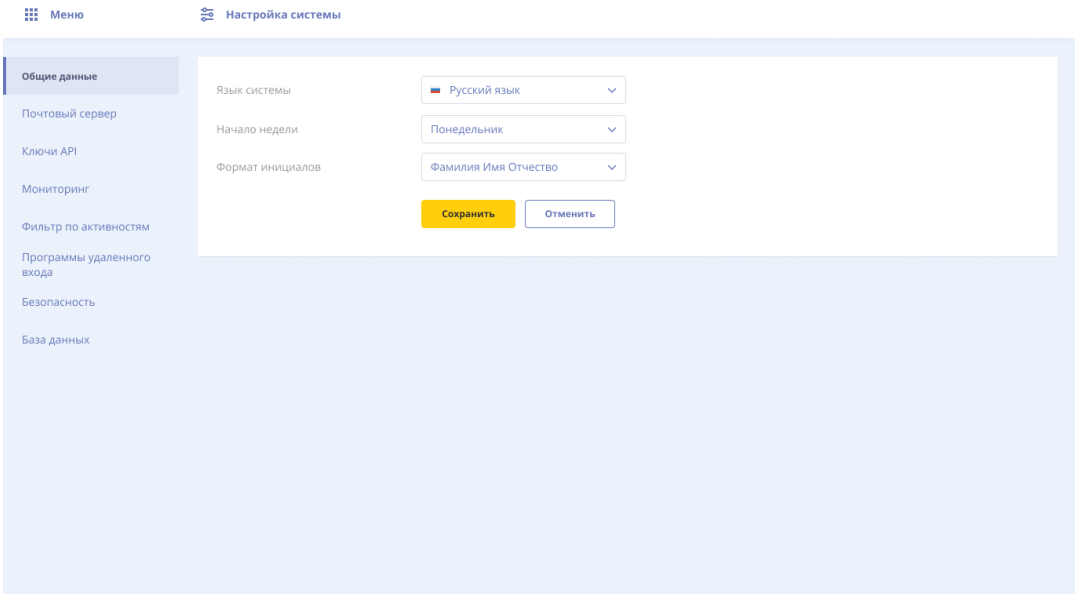

Рисунок 18 - Настройка общих параметров системы

3.1.2 Почтовый сервер

На странице «Почтовый сервер» (Рисунок 19) настраивается работа с уведомлениями на почту администратора: о смене пароля, блокировках пользователей, а также для отправки приглашений новым сотрудникам. Для настройки необходимо указать все параметры почтового сервера:

- адрес электронной почты;
- адрес сервера;
- порт для соединения;
- выбрать значение «шифрованное соединение» (TLS/SSL/Выкл);
- имя пользователя;
- пароль.

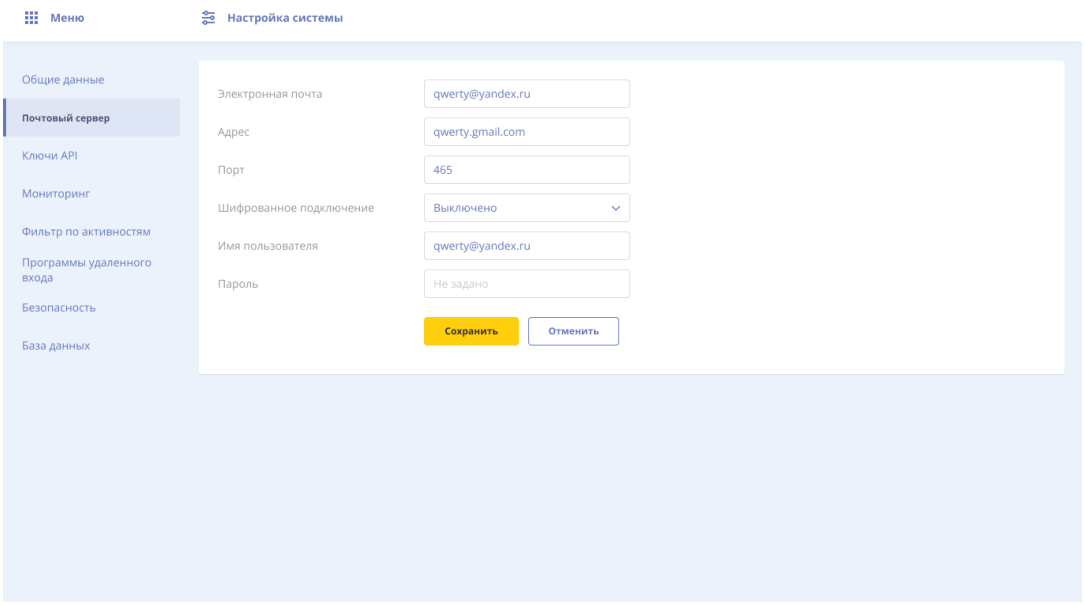

Рисунок 19 - Настройка почтового сервера

Поддерживаемые протоколы шифрования почтового сервера:

- без шифрования;
- SSL;
- TLS.

В целях безопасности рекомендуется использовать протокол шифрования почтового сервера TLS.

3.1.3 Ключи API

На странице «Ключи API» (Рисунок 20) можно сгенерировать Ключи API. Ключи API позволяют настроить интеграционное соединение, получить данные из Системы, а также настроить соединение с ММАП (агент мониторинга).

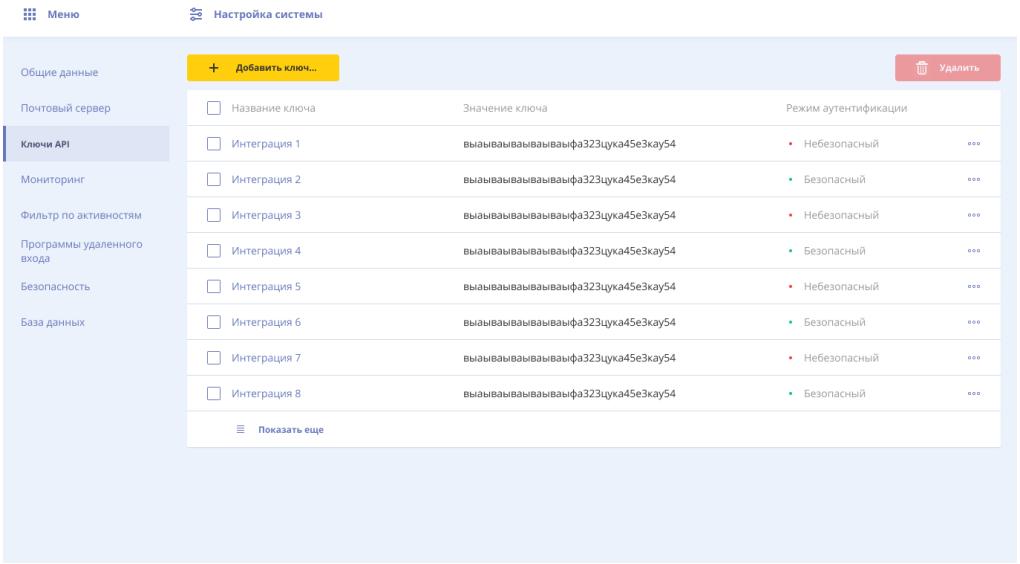

Рисунок 20 - Настройка ключей API

Ключи API предназначен для авторизации внешних запросов от различных внешних интеграций, в том числе и агента мониторинга. Настройка соединение с агентом мониторинга указана в п.2.2.1, 2.2.2, 2.3.1.

Для настройки соединения с помощью двухсторонней SSL-аутентификации необходимо создать «безопасный» ключ. (Рисунок 21)

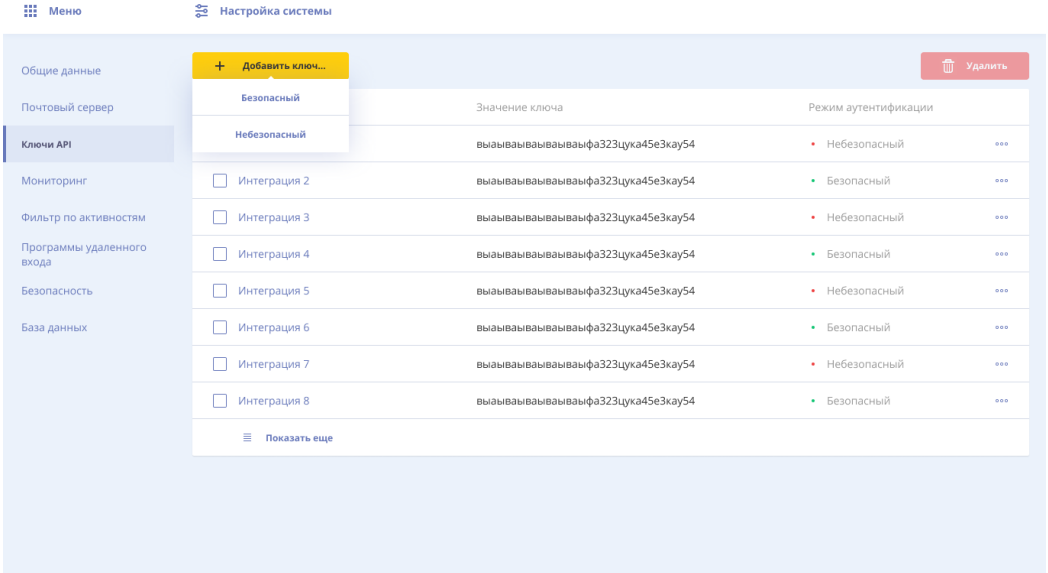

Рисунок 21 - Добавление ключа API

Для создания безопасного ключа необходимо:

- Ввести название ключа API;
- Загрузить клиентский сертификат безопасности;

Для безопасного ключа API необходимо загрузить SSL сертификат, который в последствии будет использован для аутентификации при интеграции. (Рисунок 22)

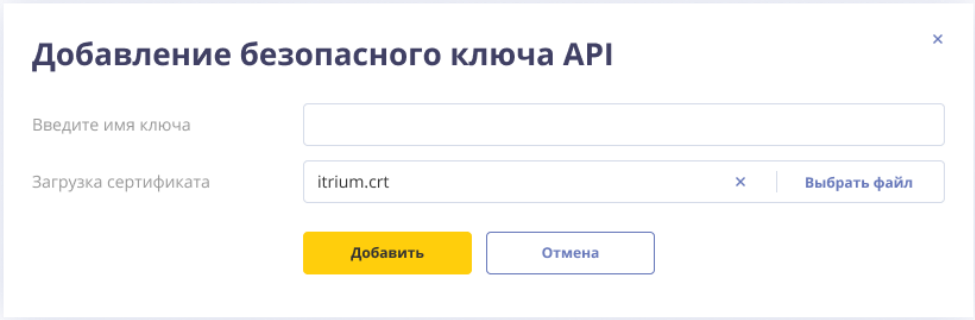

Рисунок 22 - Добавление безопасного ключа API

Далее в привилегиях Ключа API устанавливаем необходимые операции доступа для Ключа API. (Рисунок 23) Подробнее с привилегиями в системе можно ознакомится в Общем описании системы п. 3.5.1. После настройки в привилегиях Ключа API необходимо выбрать значение параметра «Доступ к списку процесса» (вкл/выкл). Если значение будет вкл., то по данному ключу можно получить доступ к списку процессов, ко всем вложенным отчётам, а также всем аналитическим данным в этих отчётах.

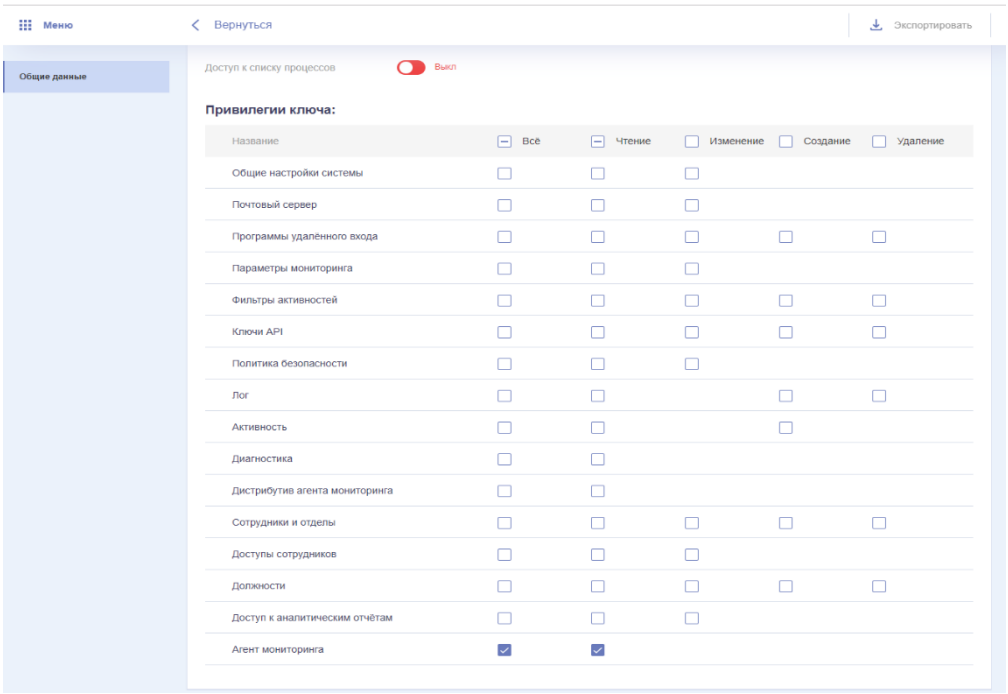

Рисунок 23 - привилегии для ключа API

Далее на стороне внешней системы необходимо произвести настройку https соединения, хранилища сертификатов, и также клиентских сертификатов. После чего можно выполнять Graphql запросы к Системе. Для возможности соединения в Системе в обязательном порядке должна быть выполнена настройка клиентской авторизации. (см. п.4.1)

3.1.4 Мониторинг

На странице «Мониторинг» (Рисунок 24) настраивается точность сбора активности, её вид и время, после которого начинается считаться неактивность. Можно настроить следующие параметры:

- Точность (стандартная, улучшенная). Точность агента мониторинга влияет только на сбор активности по браузерам (URL, заголовок) основанных на проекте Chromium (Google Chrome, Chromium, Chromium Portable, Yandex, Opera Internet Browser, Sputnik).
  При включении режима «улучшенная» точность, агент мониторинга включает у браузера режим accessibility (например, для Google Chrome настройки этого режима можно увидеть по адресу Chrome://Accessibility/). В этом режиме агент может более точно отслеживать URL и соответствующий ему заголовок, даже во время смены web-адреса или его редактирования. Однако, при включенном accessibility на некоторых сложных, с точки зрения построения DOM-структуры страниц, web-системах возможны ошибки, приводящие к падению вкладки браузера.
  При включении режима «стандартная» точность, агент мониторинга не изменяет режим работы браузеров и работает в штатном режиме.
- Активность (вся, стандартная). В режиме «вся» активность собираются все события (и программные, и от реальных устройств – клавиатуры или «мыши»), в режиме «стандартная» активность - только от реальных устройств (программные игнорируются).
- Считать, как время без активности (возможно значение от 1 до 5 минут). Параметр указывает, через какое время бездействия (отсутствие действий на клавиатуре и/или «мыши» ПК), временной промежуток признается как время без активности за ПК.

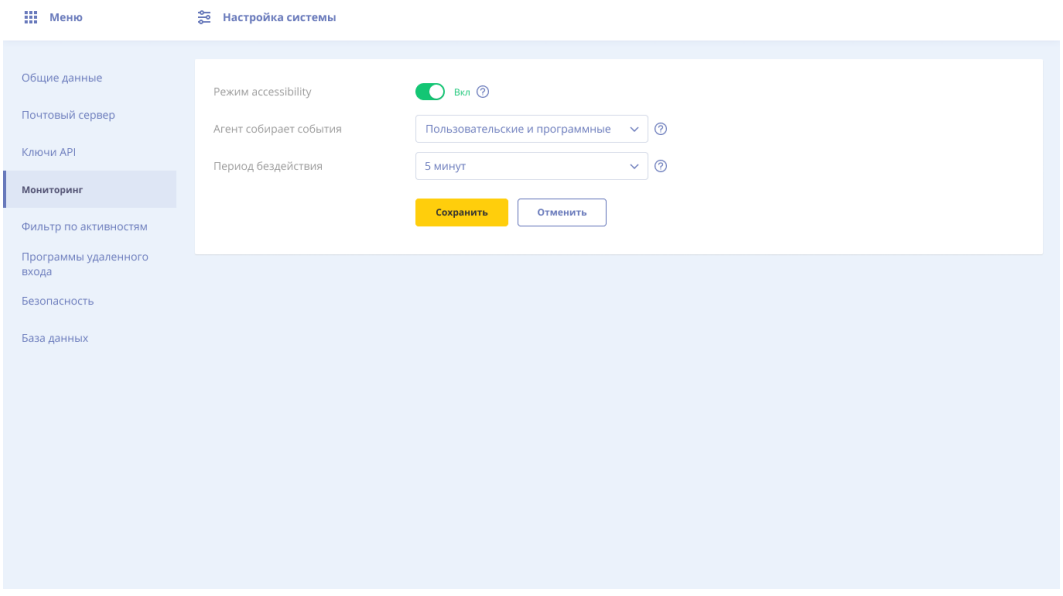

Рисунок 24- Настройка мониторинга

3.1.5 Фильтры по активностям

На странице «Фильтры по активностям» (Рисунок 25) возможно создать белый и чёрный список программ, по которым будет собираться или игнорироваться активность сотрудников.

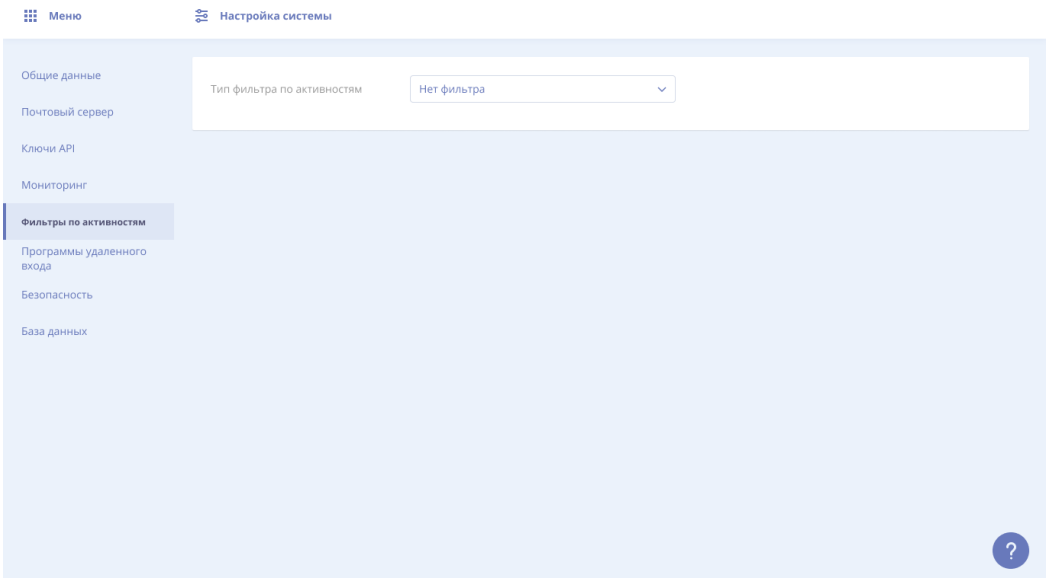

Рисунок 25 - Настройка фильтра по активностям

Если выбрано:

- «Белый список» – отображается только статистика по активностям из белого списка.
- «Чёрный список» – отображается только статистика по активностям, не включенным в чёрный список.
- Нет фильтра – отображается вся статистика по активностям.

Некоторые программы, такие как Microsoft Word, в разных версиях могут называться по-разному. Для того чтобы объединить все версии необходимо использовать знак «*», поставив его после названия (например, Word*). При этом будут игнорироваться все символы, стоящие после звездочки. Таким образом, программы с названием Word 2003, Word 11, Word 2016 автоматически будут объединены.

Приложения для добавления в чёрный и белый списки нужно задавать в виде масок по названию, в том виде, в котором они заданы в свойствах exe-файла, на вкладке «Общие», в строке «Описание» (Рисунок 26).

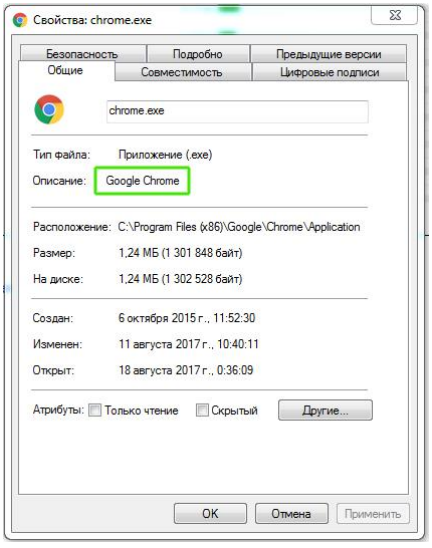

Рисунок 26 - Общие свойства файла

3.1.6 Программы удалённого входа

Основное назначение программ удаленного входа – разрешение конфликтных ситуаций, когда одновременно приходит статистика по сотруднику с 2-х агентов мониторинга. Конфликтная ситуация может возникнуть в случае, если агент мониторинга установлен на основном компьютере сотрудника, за которым он осуществляет работу, и на компьютере, к которому он осуществляет удалённое подключение. Страница «Программы удалённого входа» позволяет разрешить конфликтные ситуации и определить какая активность с 2-х агентов мониторинга истинна.

На страницу «Программы удалённого входа» необходимо добавлять все программы, с помощью которых сотрудники осуществляют удалённое подключение. Если название программы есть в списке и Система одновременно получает активность с 2-х агентов, одна из которых это активность программы из списка, то Система фиксирует вторую активность как истинную.

Например, агент мониторинга, который стоит на основном ПК передал активность, что сотрудник работал в программе Virtual Box (программа для запуска виртуальных машин). Второй агент мониторинга, который стоит на удалённом ПК, передал данные, что работа идет в Microsoft Word. Указание удалённой программы в списке «Программ удалённого входа» позволит указать, что конечная активность происходит именно в программе Microsoft Word

Настройка фильтра осуществляется через web-интерфейс: «Настройки системы»/ «Программы удалённого входа».

Для добавления программы в список программ удалённого доступа необходимо нажать «Добавить программу» и ввести название программы, которую необходимо учитывать как программу удалённого входа (Рисунок 27).

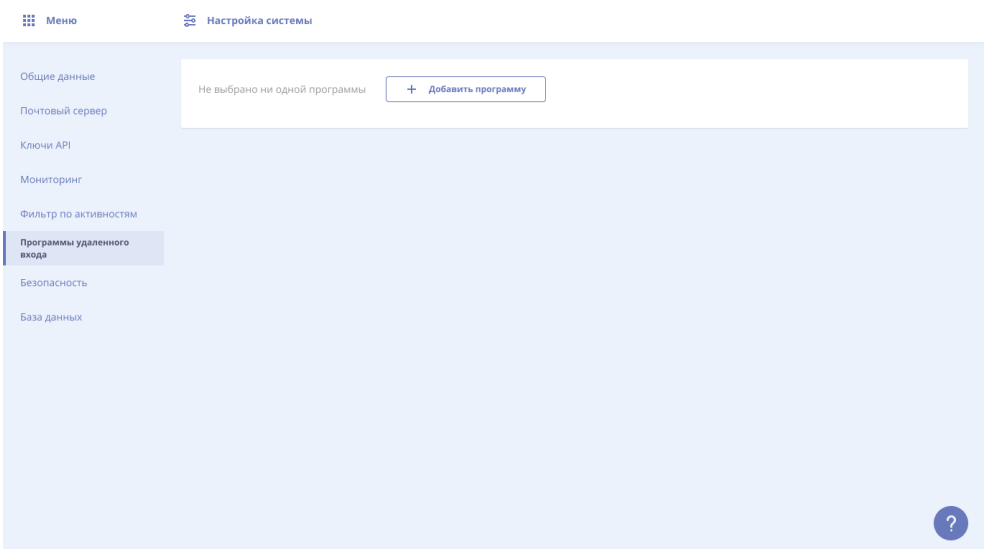

Рисунок 27 - Настройка программ удалённого входа

Название приложения для добавления в список программ удалённого доступа, нужно задавать в том виде, в котором они заданы в свойствах exe-файла, на вкладке «Общие», в строке «Описание» (Рисунок 26).

3.1.7 Безопасность

Настройка параметров безопасности осуществляется на странице: «Настройки»/ «Настройки системы»/ «Безопасность» (Рисунок 28). Полное описание работы с вкладкой безопасности представлены в общем описании системы.

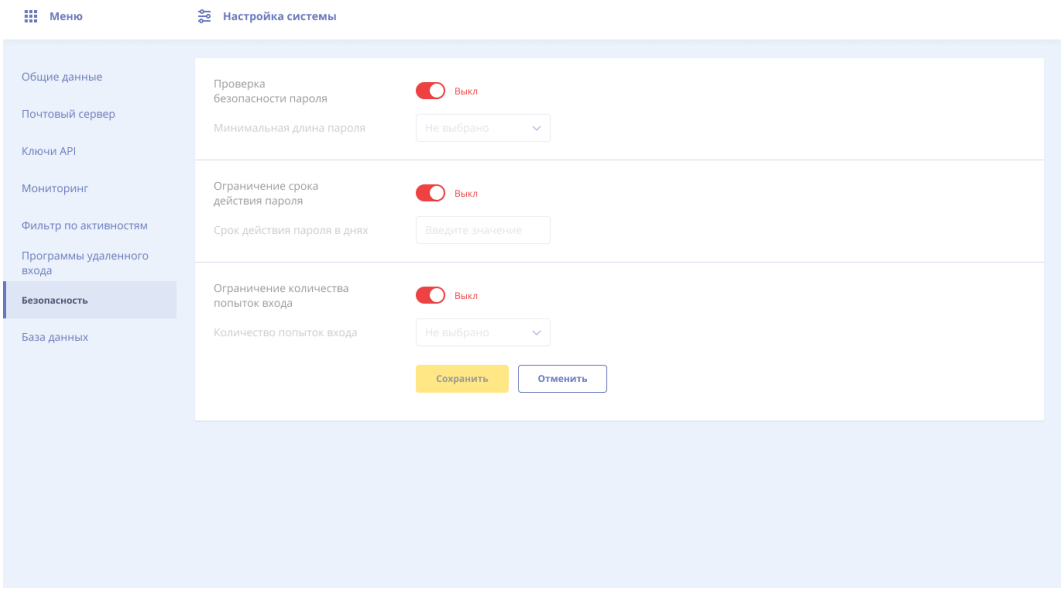

Рисунок 28 - Настройка безопасности

3.1.8 База данных

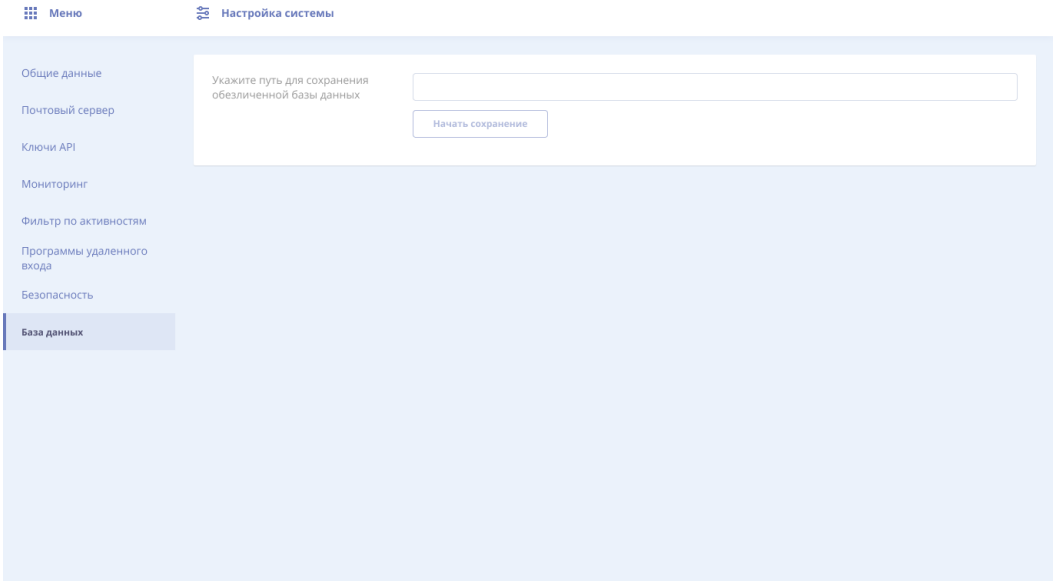

Рисунок 29 - Копия базы данных

На вкладке «База данных» можно сделать копию обезличенной БД. (Рисунок 29) Для запуска процесса необходимо указать путь (директорию), куда сохранится обезличенная БД. Более подробная инструкция представлена в п.4.7

3.2 Раздел «Настройка компании»

3.2.1 Сотрудники

В этой группе объединены настройки для управления сотрудниками, должностями, ролями доступа. На вкладке «Сотрудники» (Рисунок 30) представлена структура компании с сотрудниками, группами, отделами. Данная структура может быть настроена индивидуально.

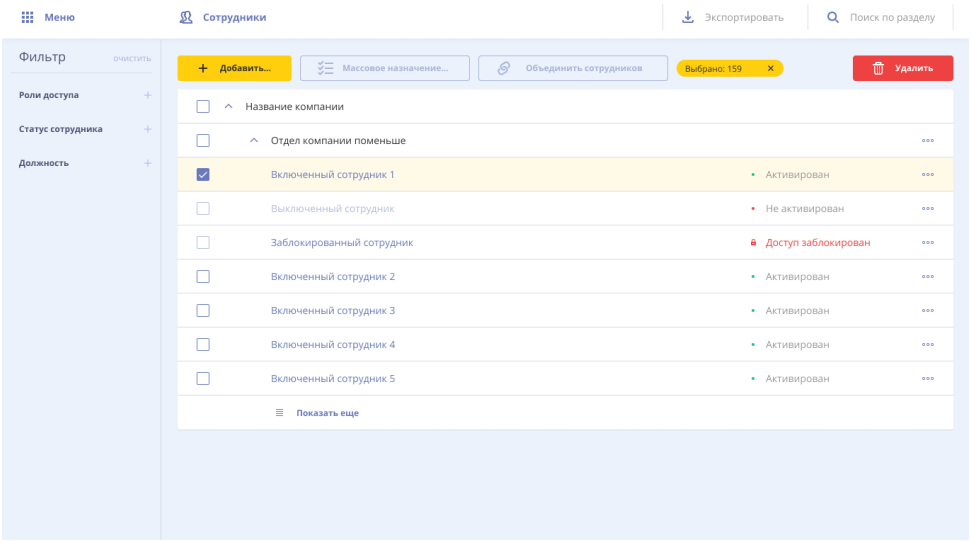

Рисунок 30 - Страница «Сотрудники»

Функционал Системы позволяет добавлять новые (Рисунок 31) и редактировать подразделения и сотрудников (Рисунок 32) по мере необходимости.

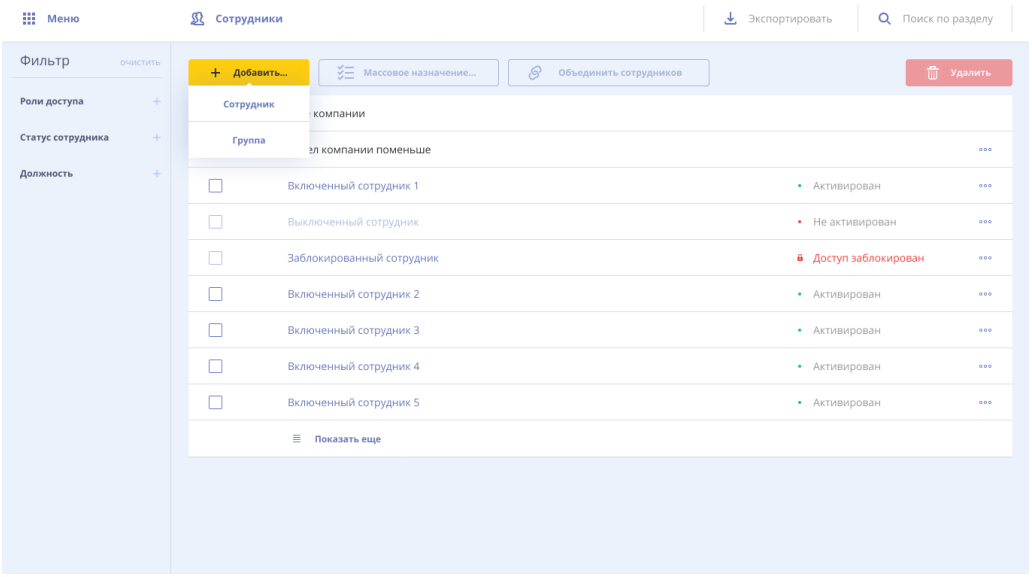

Рисунок 31 - Добавление сотрудников/групп

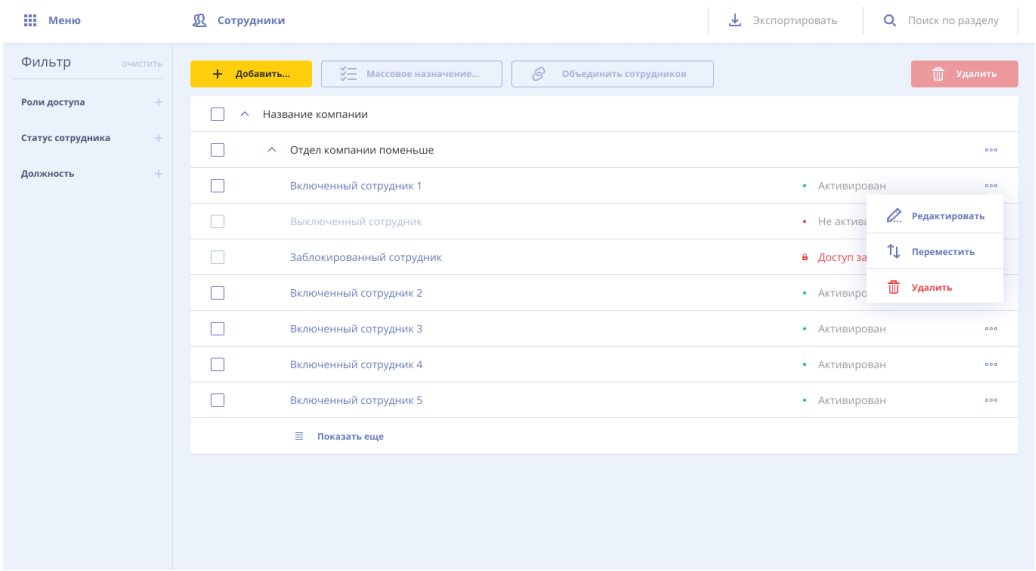

Рисунок 32 - Действия с сотрудниками/группами

3.2.1.1 Массовые действия

Для удобства в системе предусмотрен функционал массовых действий. Массово можно назначить (Рисунок 33):

- Доступ в систему (Вкл/Выкл);
- Роли доступа (назначение/удаление);
- Должности (назначение/удаление);
- Часовой пояс;
- Перемещение;
- Язык в системе;

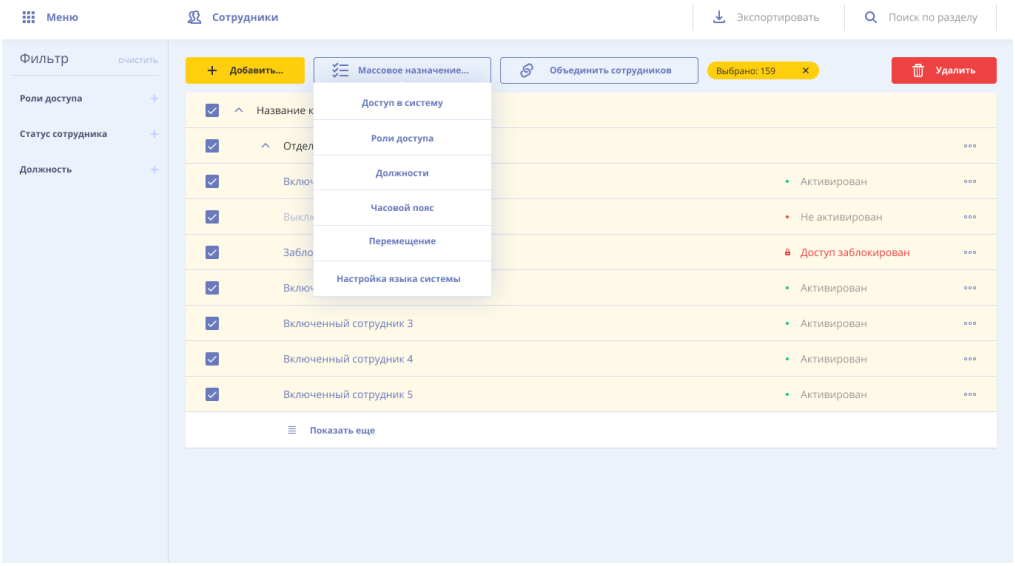

Рисунок 33 - Массовые действия

3.2.1.2 Профиль сотрудника

В Профиле сотрудника, на вкладке «Общие данные» (Рисунок 34) можно изменить следующие параметры:

- Фамилия;
- Имя;
- Отчество;

- Язык системы;
- Должность сотрудника;
- Место в структуре компании;
- Табельный номер
- Электронная почта;
- Выбор часового пояса;

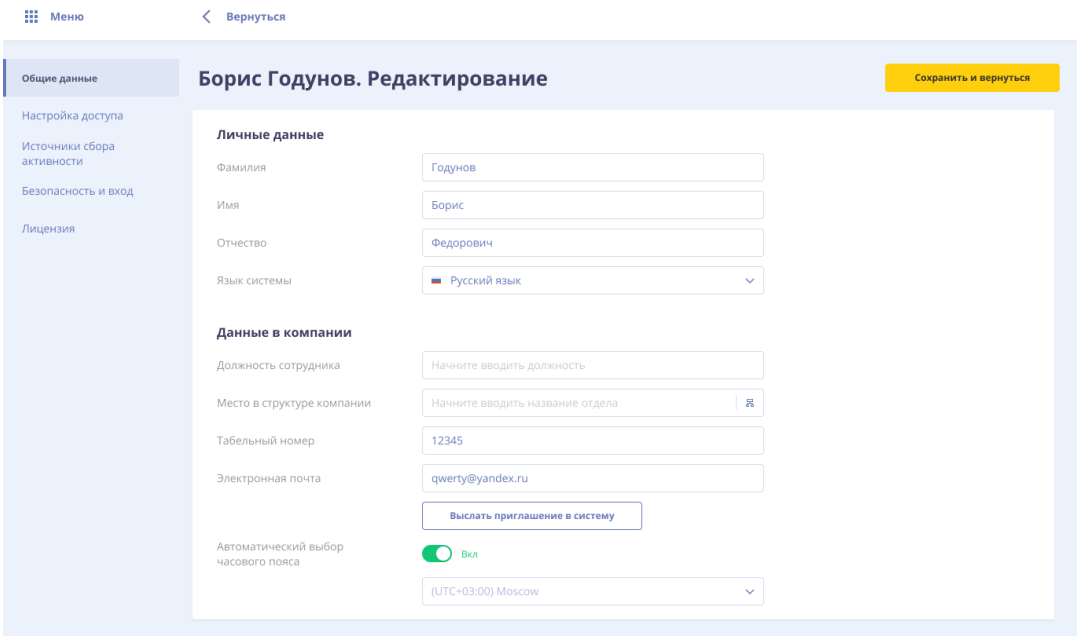

Рисунок 34 - Профиль сотрудника

На вкладке «Настройки доступа» (Рисунок 35) возможно настроить следующие параметры:

- Роли доступа
- Доступ к списку процессов
- Оповещение о блокировке пользователей
- Доступ ко всем сотрудникам
- Выборочный доступ к сотрудникам

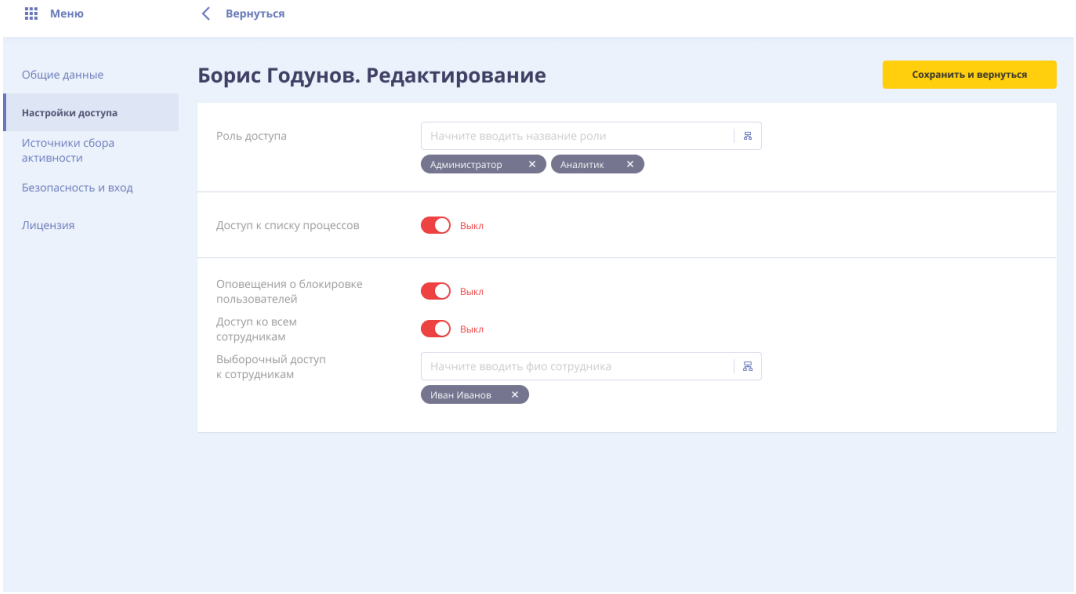

Рисунок 35 - Настройка доступа

На вкладке «Источники сбора активности» (Рисунок 36) показывается список учетных записей, от которых приходит активность для этого сотрудника.

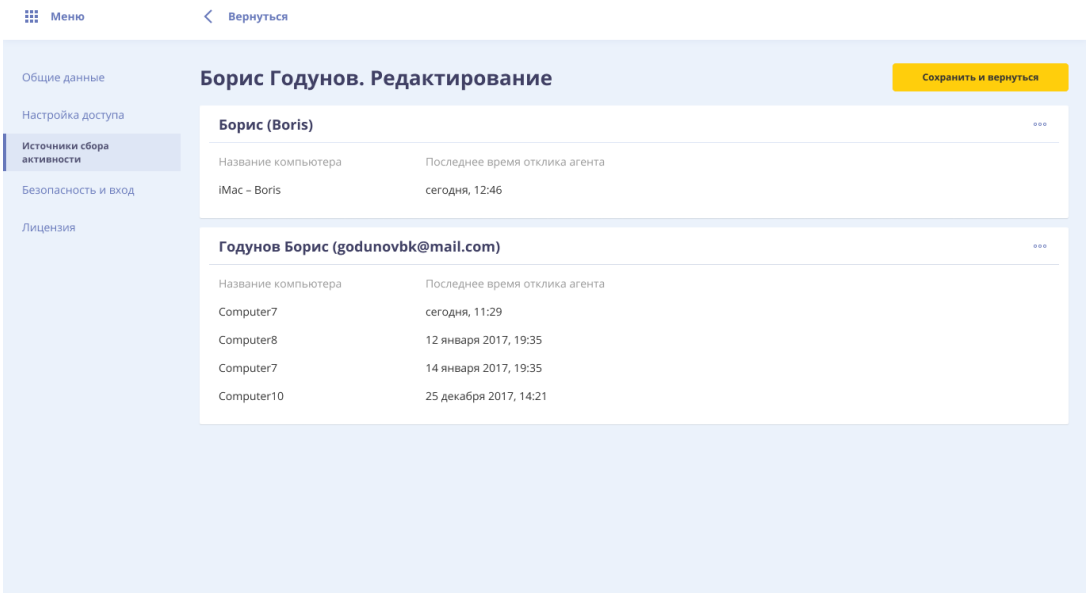

Рисунок 36 - Источники сбора активностей

Учётная запись может быть двух типов:

1. Локальная:
   - Имя учётной записи (под которой авторизован пользователь на ПК). В скобках указывается логин, под которым авторизован пользователь на ПК;
   - Название компьютера (где располагается агент);
   - Последнее время отклика агента.

У локальной учётной записи всегда один источник (компьютер).

2. Доменная
   - Имя учётной записи (под которой авторизован пользователь на ПК). В скобках указывается логин, под которым авторизован пользователь в домене.
   - Название компьютера (где располагается агент);
   - Последнее время отклика агента.

У доменной учётной записи может быть несколько источников.

Источники сбора активности можно открепить в другого сотрудника или в нового, а также удалить (Рисунок 37).

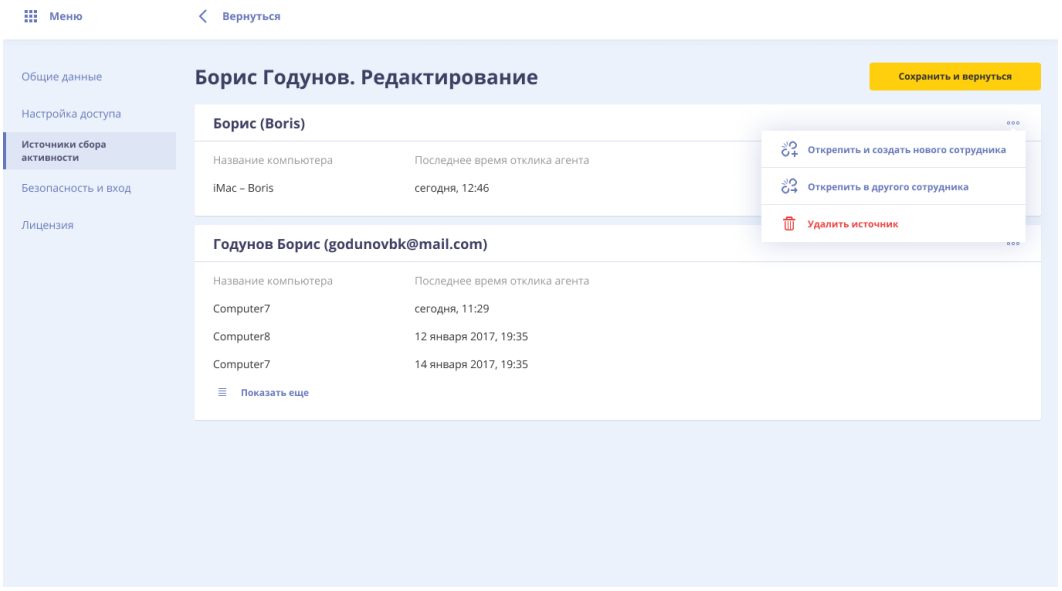

Рисунок 37 - Источники сбора активностей

На вкладке «Безопасность и вход» (Рисунок 38) представлены следующие параметры:

- Доступ в систему
- Логин для входа в систему
- Пароль для входа в систему

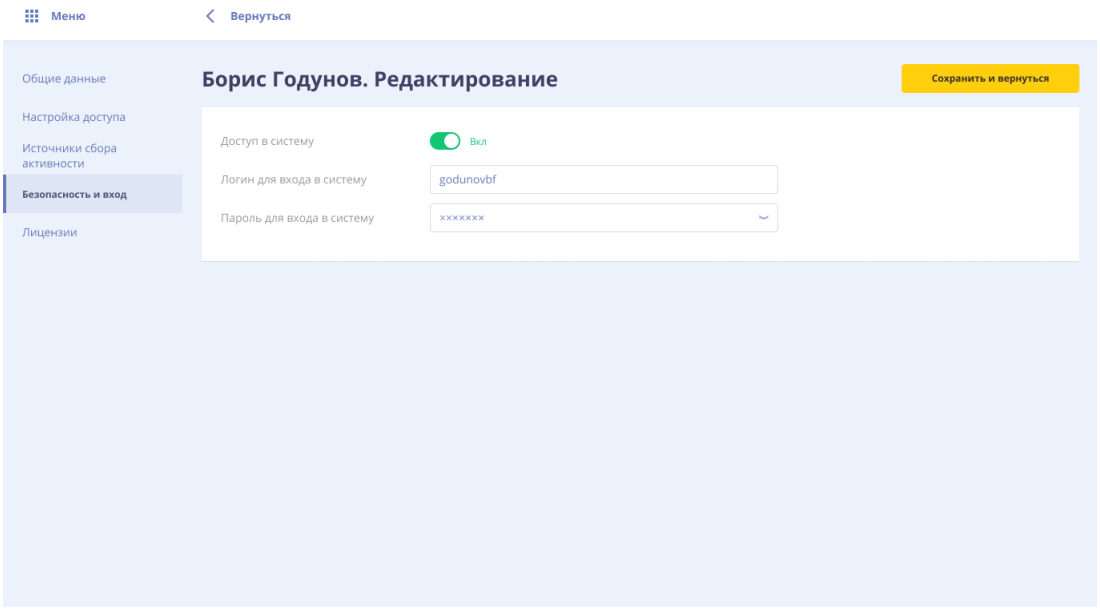

Рисунок 38 - Вкладка безопасность и вход

3.2.1.3 Должность

На странице «Должности» (Рисунок 39) можно добавить и отредактировать должности, которые занимают сотрудники, участвующие в исследуемых процессах.

Рисунок 39 - Массовые действия на странице «Должности»

3.2.2 Роли доступа

На странице «Роли доступа» (Рисунок 40) создаются роли, согласно политике безопасности компании.

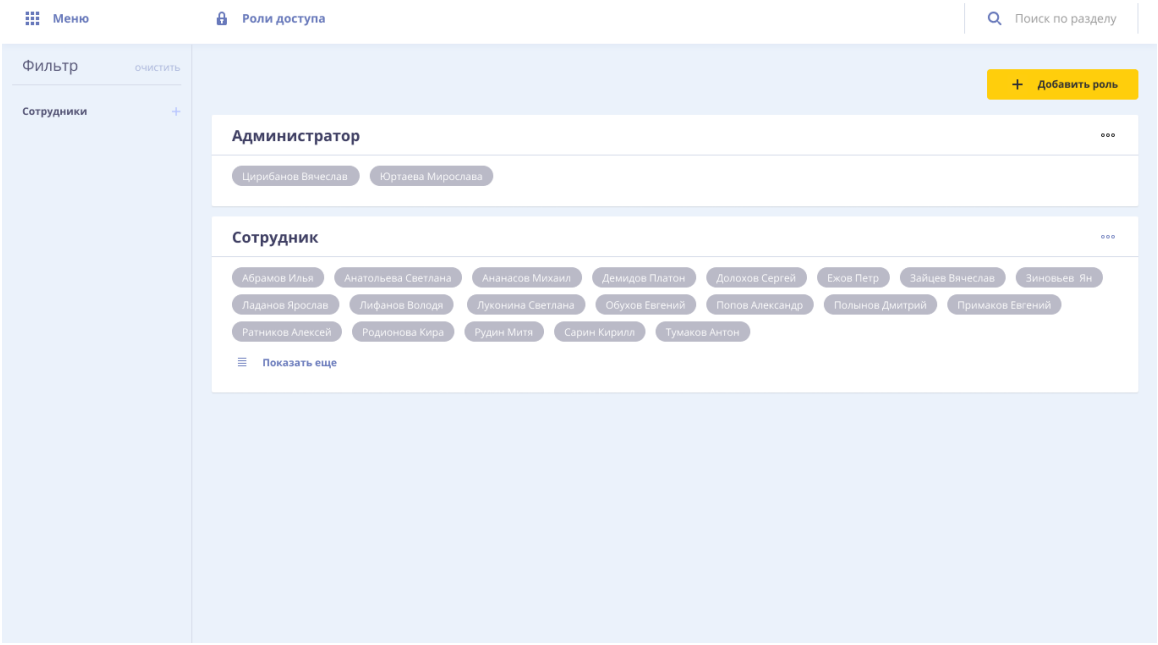

Рисунок 40 - Массовые действия на странице «Роли доступа»

Каждой роли доступа можно присвоить своё уникальное имя и настроить привилегии согласно политике. Полная политика ролевой модели представлена в Общем описании Системы (см. Общее описание системы, п. 3.5.)

4. Работа с системой

4.1 Настройка клиентской авторизации на сервере

Для установки клиентской авторизации необходимо отредактировать файл конфигурации:
C:\ProgramData\Infomaximum\config\com.infomaximum.subsystem.frontend.json

В секции "connectors" следует прописать следующие настройки:

- ssl_cert_store - полный путь к файлу хранилища сертификатов. Поддерживаемые форматы: JKS, PKCS#12
- ssl_cert_store_password - пароль хранилища сертификатов
- trust_store - полный путь к файлу хранилища доверенных сертификатов. Поддерживаемые форматы: JKS, PKCS#12
- trust_store_password - пароль хранилища доверенных сертификатов. Если пароли хранилища сертификатов и хранилища доверенных сертификатов одинаковые, то это поле можно не заполнять.
- crl - полный путь к файлу отозванных сертификатов (Не обязательное)

Пример:

```
"connectors": [
    {
      "protocol": "https",
      "ssl_cert_store": "c:/keystore.p12",
      "port": 8010,
      "host": "0.0.0.0",
      "ssl_cert_store_password": "password",
      "trust_store": "c:/truststore",
      "trust_store_password": "password",
      "crl": "c:/crl.crl"
    }
  ]
```

4.2 Экспорт списка пользователей

Экспорт списка пользователей системы можно осуществить на странице: «Сотрудники». Для экспорта списка пользователей необходимо нажать «Экспортировать» и выбрать тип экспорта пользователей (Рисунок 36):

- Экспорт всех сотрудников (пользователей)
- Экспорт всех активных сотрудников (пользователей)

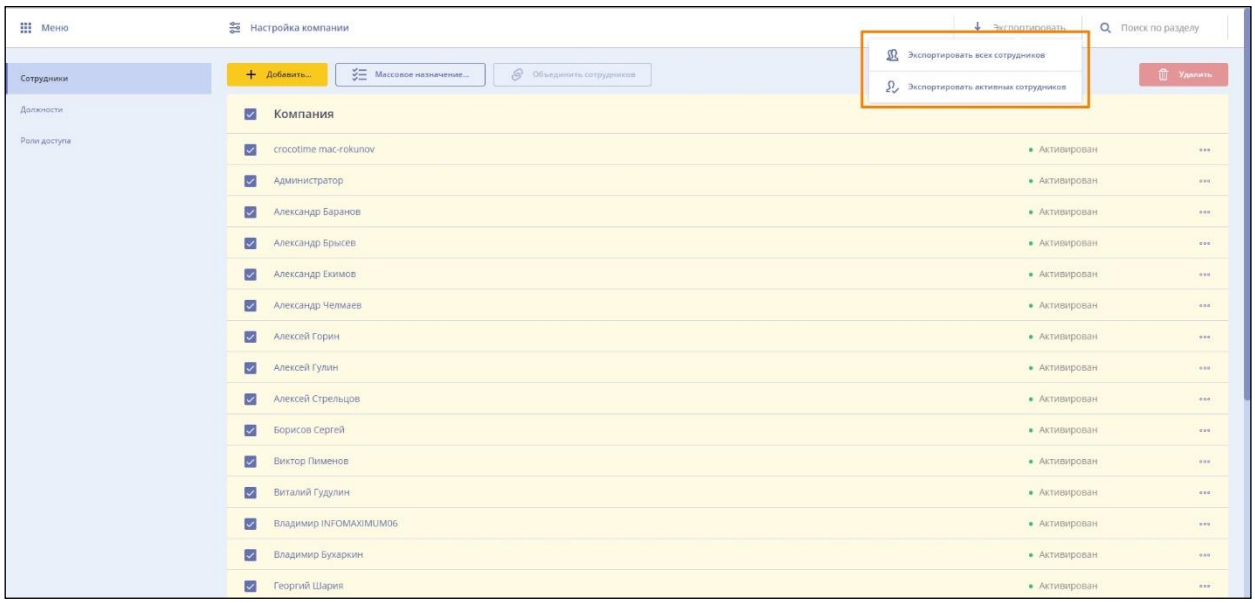

Рисунок 41 - Экспорт сотрудников

При экспорте всех сотрудников происходит экспорт всех пользователей Системы, которые существует в каталоге Системы. При экспорте всех активных сотрудников

происходит экспорт всех активных пользователей системы, которые на данный момент, в текущую минуту пользуются Системой.

Экспорт осуществляется в файл MS Excel. Экспортируемый файл представлен по формату предоставления данных о пользователях Системы.

Колонки:

- Логин сотрудника
- Фамилия Имя Отчество сотрудника
- Дата и время последнего входа в Систему
- Дата и время последней смены пароля
- Факт блокировки
- IP-адрес, с которого произошел последний вход в Систему
- Список ролей доступа, назначенных сотруднику
- Список включенных привилегий сотруднику
- Дата и время последнего запроса по сессии, SHA256 от строкового значения сессии

4.3 Работа в GraphQL

[1] Для написания отдельных запросов к базе данных Системы используется инструмент GraphQL (см. Руководство администратора информационной безопасности, п. 6).

4.4 Управление объектами системы

- Управление пользователями Системы (см. Руководство администратора информационной безопасности, раздел 7.1.);
- Управление группами Системы (см. Руководство администратора информационной безопасности, раздел 7.2.);
- Управление ролями доступа Системы (см. Руководство администратора информационной безопасности, раздел 7.3.).

4.5 Настройка системного времени

Синхронизация системного времени происходит между модулями ММАП (Агент мониторинга) и МНА. (см. Общее описание системы п. 3.1.1) Системное время в модулях принимает значение, установленное на сервере. Система получает значение системного времени в формате Unix от операционной системы на котором развернут сервер. Сервером является специализированный ПК или специализированное оборудование, на котором развернута Система. Настройка, изменение системного времени регламентируется посредством windows политик.

4.5.1 Получение системного времени

Для просмотра системного времени, установленного в Системе необходимо воспользоваться инструментом GraphQL (см. Руководство администратора информационной безопасности, п. 6). Сформировать запрос через веб-интерфейс:

```
{server
  {time}}
```

Получаем значение time.

Рисунок 42 - Запрос системного времени

Значение time представлено в формате Unix. Все события записываются в журнал аудита и базу данных в локальном времени сервера.

4.5.2 Настройка часового пояса сотрудника

Настройка часового пояса может производится для каждого пользователя Системы индивидуально. Настройка осуществляется через веб-интерфейс на странице: «Настройки»/ «Настройка компании»/ «Профиль сотрудника». (см. п. 3.2.1.2) Для автоматического выбора значения параметра «часовой пояс» необходимо чтобы параметр «автоматический выбор часового пояса» находился в состоянии «Вкл». «Автоматический выбор часового пояса» подразумевает, что у сотрудника будет выбран часовой пояс, назначенный на сервере Системы. Если же данный параметр находится в состоянии «Выкл», то необходимо выбрать нужный часовой пояс вручную (в формате UTC) для конкретного сотрудника.

4.6 Резервное копирование БД

Система периодически (раз в сутки, в 00:00:00) выполняет резервное копирование (бэкап базы данных). Резервное копирование по умолчанию осуществляется в системную папку: C:/ProgramData/Infomaximum/backup.

Параметры базы данных настраиваются в файле: com.infomaximum.subsystem.database. json.

Путь к файлу: C:/ProgramData/Infomaximum/config/com.infomaximum.subsystem. database.json.

Контроль целостности по контрольным суммам осуществляется при каждой загрузке Системы. Периодически в процессе работы Системы контроль целостности по контрольным суммам не осуществляется. В состав Системы встроены средства отладки, которые невозможно удалить, но можно контролировать его активацию, для этого необходимо отслеживать все изменения в службе «infomaximum», в частности, команду запуска. Восстановить БД возможно с помощью специальной утилиты. (см. п. Руководство администратора информационной безопасности 4.2)

4.7 Сохранение копии обезличенной базы данных

Для сохранения обезличенной БД Системы необходимо чтобы у пользователя Системы была назначена роль доступа с включенной привилегией «Общие настройка системы» с операцией доступа W (изменение). (см. Общее описание системы, п. 3.5.1.1).

Сохранение обезличенной БД можно произвести двумя способами:

- Через веб-интерфейс Системы на странице «Настройки» / «Настройки системы» / «База данных»

Для запуска процесса необходимо указать путь (директорию), куда сохранится обезличенная БД.

- Через GraphQL при выполнения следующего запроса:

```
mutation{
  database{
    copy_depersonalized_database(path:"c:/database")

  }
}
```

Где, «c:/database» путь сохранения обезличенной БД.

Для выполнения запроса GraphQL у пользователя должна быть назначена роль доступа с включенной привилегией «Инструмент GraphQL» с операцией доступа R. (см. Общее описание системы, п. 3.5.1.18).

Сохранение происходит на сервер, где установлена Система. Папка для сохранения должна быть создана заранее и должна быть пустой.