«Инфомаксимум»
(Общество с ограниченной ответственностью)

Proceset

Общее описание системы

2019 г.

Содержание

1. Общие положения

Настоящий документ (далее – Описание) распространяется на программное обеспечение «Proceset».

Данное Описание содержит сведения о процессах, обеспечивающих поддержание жизненного цикла Системы, а также информацию о персонале для устранения неисправностей, выявленных в ходе эксплуатации программного обеспечения.

1.1 Основные термины

Термин	Описание
BI	набор IT-технологий для сбора, хранения и анализа данных, позволяющих предоставлять пользователям достоверную аналитику в удобном формате, на основе которой можно принимать эффективные решения для управления бизнес-процессами компании
Commit	фиксация транзакции
Event log	журнал событий, содержащий список выполнений процесса и связанные с ними параметры
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
Job	связанные между собой отдельные этапы (stages), описывающие поток данных из источника данных в целевой объект данных.
RocksDB	высокопроизводительная встраиваемая СУБД на основе LSM-tree с открытым исходным кодом (лицензия Apache 2.0) от компании Facebook
Stage	набор предопределенных и редактируемых свойств, которые обеспечивают обработку данных.
Аварийный дамп	отладочная информация, позволяющая выявить причину выхода из строя Системы
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
Контроллинг	мониторинг процессных показателей и анализ структуры «фактического» процесса, а также эффективности работы участников бизнес-процесса
ПК	персональный компьютер
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
Система	автоматизированная система «Система управления рабочим временем» Proceset

Система контроля версии	система, регистрирующая изменения в исходном коде с тем, чтобы в дальнейшем была возможность вернуться к определённой версии системы
СТД	программно-аппаратный комплекс, функционирующий на базе ПО Citrix и предоставляющий доступ к ИТ-системам таким образом, что обработка данных ведется на специальном удаленном сервере, а компьютер Пользователя выполняет лишь функции ввода информации (от клавиатуры и мыши) и графического отображения информации на монитор Пользователя.
Чёрно-белые списки	список программ, мониторинг времени которых включается/ исключается из итоговой активности сотрудника

1.2 Основные сокращения

Сокращение	Описание
BI	Business Intelligence
RPA	Robotic process automation (Роботизированная автоматизация процессов)
ММАП	Модуль мониторинга активности пользователя
МНиА	Модуль настройки и аналитики
АС	Автоматизированная система
СТД	Система терминального доступа

2. Назначение Системы

2.1 Назначение и цели использования Системы

Система реализует автоматизацию информационного технологического процесса компании. Система позволяет автоматизировать внутренние процессы управления и контроля. Система позволяет в режиме реального времени анализировать работу сотрудников за компьютером, в также провести «восстановление» фактических бизнес-процессов для целей контроллинга их выполнения.

2.2 Функциональность Системы

Автоматизированная система Proceset позволяет на основе фактических данных принимать управленческие решения, направленные на перераспределение функций персонала, оптимизацию его численности, повышение производительности за счет повышения прозрачности процессов и выявления скрытых резервов рабочего времени.

Автоматизированная система анализа бизнес-процессов Proceset предоставляет пользователям возможность на постоянной основе анализировать структуру рабочего времени сотрудника с целью оптимизации выполняемых функций, выявлять сотрудников с регулярными переработками и определить причины их возникновения, произвести оптимизацию или реинжиниринг процессов, найти оптимальные сценарии их выполнения и отклонения от регламентирующей документации, определить направления для развития корпоративных информационных систем, результативно и эффективно управлять человеческим потенциалом, определять приоритеты для автоматизации и RPA.

Система предназначена для реализации следующих функций:

- Мониторинг структуры рабочего времени сотрудников
- Мониторинг времени работы с конкретными приложениями, окнами и документами
- Выявление резервов рабочего времени сотрудников
- Обнаружение реальных бизнес-процессов (в т.ч. выявление автоматизированных процессов, которые еще не описаны/не задокументированы);
- Оценка эффективности бизнес-процессов;
- Поиск узких мест в бизнес-процессах;
- Выявление отклонений реальных бизнес-процессов от регламентированных;
- Сравнительный анализ сотрудников в разрезе выполняемых операций;
- Оценка реальных трудозатрат на выполнение операций бизнес-процесса;
- Анализ и диагностика активности сотрудников за компьютерами, в т.ч. при работе с виртуализированными приложениями и виртуальными рабочими местами.

2.3 Меры безопасности разработки и поставки

Меры, предпринятые разработчиком относительно безопасности разработки и поставки:

- Разработка ведется с использованием системы контроля версии
- Для доступа к центральному репозиторию обязательна аутентификация;
- Каждый разработчик использует свои учетные данные для входа;
- Все commit проходят проверку кода;
- Сборка и подписывание приложения происходит автоматически на выделенном сервере, доступ к которому ограничен.

3. Описание Системы

3.1 Структура Системы

Система состоит из следующих компонентов (подсистем) (Приложение №1):

- Подсистема хранения данных (сервер);
- Модуль мониторинга активности пользователя (ММАП);
- Модуль настройки и аналитики (МНиА).

3.1.1 Подсистема хранения данных

Подсистема хранения данных предназначена для хранения и извлечения всей информации в полном объеме. В качестве СУБД Системы используется RocksDB. Официальный сайт с описанием - https://rocksdb.org. Официальный исходный код - https://github.com/facebook/rocksdb. Полная документация о СУБД - https://github.com/facebook/rocksdb/wiki.

RocksDB - это встроенное файловое хранилище, к которому возможно получить доступ через интерфейсы Системы с аутентификацией пользователя, а также на уровне файловой системы пользователю с соответствующими правами доступа. Доступ к БД защищается на уровне файловой системы. Подробнее как осуществляется защита описано в Руководстве администратора информационной безопасности п.8.2.

3.1.2 Модуль мониторинга активности пользователя

ММАП предназначен для автоматического сбора информации о моментах переключений пользователя между различными вкладками и окнами приложений. Модуль позволяет собирать точные данные о работе пользователя за ПК. Платформа реализации компонента: нативное исполняемое приложение, версия: 1.0.12.

3.1.3 Модуль настройки и аналитики

МНиА предназначен для настройки параметров системы: настройка ролевой модели, языка системы, часового пояса, парольной политики и т.д., а также для формирования аналитических отчётов: построение карт процесса, списка активностей в операции процесса и т.д. Платформа реализации компонента: Java SE, версия: 8u162.

3.2 Регламент работы Системы

Система функционирует непрерывно и круглосуточно при условии соблюдения соответствующих регламентов.

3.2.1 Клиентское программное и аппаратное обеспечение

Таблица 1

Рабочее место пользователя «Прикладного администратора»

Характеристика	Минимальное значение	Рекомендуемое значение
Операционная система	Windows 7, Windows 8, Windows 8.1, Windows 10	Windows 7
Процессор	Intel Core i5 и выше	Intel Core i5
Объем оперативной памяти	от 4Гб	4Гб
Объем локального диска	От 100 Мб	100 Мб

Веб-браузер	Internet Explorer v.11	Internet Explorer v.11, Google chrome

Таблица 2

Рабочее место пользователя «Аналитик»

Характеристика	**Минимальное значение**	**Рекомендуемое значение**
Операционная система	Windows 7, Windows 8, Windows 8.1, Windows 10	Windows 7
Процессор	Intel Core i5 и выше	Intel Core i5
Объем оперативной памяти	от 4Гб	4Гб
Объем локального диска	100 Мб	100 Мб
Веб-браузер	Internet Explorer v.11	Internet Explorer v.11, Google chrome
ПО	Data Stage	Data Stage

Таблица 3

Рабочее место пользователя «Бизнес администратор»

Характеристика	**Минимальное значение**	**Рекомендуемое значение**
Операционная система	Windows 7, Windows 8, Windows 8.1, Windows 10	Windows 7
Процессор	Intel Core i5 и выше	Intel Core i5
Объем оперативной памяти	от 4Гб	4Гб
Объем локального диска	100 Мб	100 Мб
Веб-браузер	Internet Explorer v.11	Internet Explorer v.11, Google chrome
ПО	Data Stage	Data Stage

Таблица 4

Рабочее место пользователя «Администратор ИБ»

Характеристика	**Минимальное значение**	**Рекомендуемое значение**
Операционная система	Windows 7, Windows 8, Windows 8.1, Windows 10	Windows 7
Процессор	Intel Core i5 и выше	Intel Core i5
Объем оперативной памяти	от 4Гб	4Гб
Объем локального диска	100 Мб	100 Мб
Веб-браузер	Internet Explorer v.11	Internet Explorer v.11, Google chrome

Таблица 5

Рабочее место анализируемого сотрудника

Характеристика	Минимальное значение	Рекомендуемое значение
Операционная система	Windows 7, Windows 8, Windows 8.1, Windows 10	Windows 7
Процессор	Intel Pentium 1000 Мгц	Intel Pentium 1700 Мгц
Объем оперативной памяти	100 Мб (требуется агенту мониторинга)	200 Мб
Объем локального диска	200 Мб свободного места на жестком диске для агента + 100 Мб для хранения статистики, до ее отправки на сервер.	600 Мб

Под рабочим местом сотрудника подразумевается рабочая станция, на которую будет установлен агент мониторинга (ММАП).

3.2.2 Серверное программное и аппаратное обеспечение

Аппаратное обеспечение: Сервер
Входные данные (опытная эксплуатация):

- Количество пользователей с логами – 300;
- Количество пользователей с компьютерной активностью – 300;
- Количество пользователей с аналитическими данными (аналитики) – 10.

Таблица 6

Минимальные системные требования к обеспечению (опытная эксплуатация)

Характеристика	Минимальное значение
Платформа	x86_64
Частота процессора, ГГц	3,4
Количество физ. потоков, более	4
Объем оперативной памяти, Гб	16,00
Пропускная способность оперативной памяти	не менее 15000 МБ/сек
Объем локального диска сервера, Гб/месяц	2,00
Скорость чтения/записи диска	не менее 300 МБ/сек, рекомендуемое – SSD

Входные данные (промышленная эксплуатация):

- Количество пользователей с логами – 3000;
- Количество пользователей с компьютерной активностью – 3000;
- Количество пользователей с аналитическими данными (аналитики) – 60.

Таблица 7

Минимальные системные требования к обеспечению (промышленная эксплуатация)

Характеристика	Минимальное значение
Платформа	x86_64
Частота процессора, ГГц	3,0
Количество физ. потоков, более	16

Характеристика	Минимальное значение
Объем оперативной памяти, Гб	32,00
Пропускная способность оперативной памяти	не менее 15000 МБ/сек
Объем локального диска сервера, Гб/месяц	19,96
Скорость чтения/записи диска	не менее 300 МБ/сек, рекомендуемое - SSD

Входные данные (промышленная эксплуатация, тиражирование на новых бизнес-заказчиков):

- Количество пользователей с логами – 5000;
- Количество пользователей с компьютерной активностью – 5000;
- Количество пользователей с аналитическими данными (аналитики) – 100.

Таблица 8

Минимальные системные требования к обеспечению (промышленная эксплуатация, тиражирование на новых бизнес-заказчиков)

Характеристика	Минимальное значение
Платформа	x86_64
Частота процессора, ГГц	2,5
Количество физ. потоков, более	32
Объем оперативной памяти , Гб	64,00
Пропускная способность оперативной памяти	не менее 15000 МБ/сек
Объем локального диска сервера, Гб/месяц	33,27
Скорость чтения/записи диска	не менее 300 МБ/сек, рекомендуемое - SSD

3.3 Описание функционирования системы

3.3.1 Функционирование подсистемы хранения данных

Доступ к базе данных защищается на уровне файловой системы. Для просмотра базы данных необходимо использовать специальную утилиту. (см. Руководство администратора информационной безопасности П.4.)

3.3.2 Функционирование модуля мониторинга активности пользователя

Для работы ММАП используется отдельный тип авторизации, основанный на ключах API с минимальными правами доступа. При установке/настройке в папке C:\ProgramData\ProcesetAgent создается файл конфигурации settings.cfg, в котором в открытом виде хранится адрес сервера. Доступ к данным можно настроить посредством групповой политики Windows (см в Руководство администратора п. 8.2). Агент мониторинга имеет ограниченные права доступа, права доступа регламентируются в рамках привилегии «Агент мониторинга» см. п.3.5.1.19.

3.3.3 Модуль настройки и аналитики

МНиА является основным и используется для настройки Системы, а также для анализа бизнес-процессов. Для работы с модулем необходимо использовать веб-браузер. Модуль выполняет следующие функции:

1. Настройка системы:
   1.1. Настройка общих параметров системы;
   1.2. Настройка почтового сервера;
   1.3. Настройка программ удаленного входа;
   1.4. Настройка мониторинга;
   1.5. Настройка фильтра по активности;
   1.6. Настройка токенов;
   1.7. Настройки безопасности.
2. Настройка сведений о компании:
   2.1. Создание и настройка логинов сотрудников;
   2.2. Настройка должностей;
   2.3. Настройка ролевой модели.
3. Загрузка данных лога.
4. Обработка данных лога.
5. Построение аналитических отчётов.

В модуле настройки и аналитики происходит логирование всех объектов безопасности. (см. Руководство администратора информационной безопасности). Для работы в модуле необходимо авторизоваться в системе, при этом необходимо иметь назначенную роль доступа, а также включенный доступ в систему. Настройка модуля должна осуществляется Прикладным администратором системы. (см. Руководство прикладного администратора, п. 4).

3.4 Внутреннее сетевое взаимодействие

3.4.1 Взаимодействие ММАП с сервером

3.4.1.1 Цель обмена

- Получение настроек от сервера;
- Передача собранной информации об активности сотрудника;
- Удаленное обновление агентов;
- Отправка аварийных дампов агента.

3.4.1.2 Объем и состав передаваемых/принимаемых данных

- В режиме получения настроек от сервера: формат обмена json, объем данных до 100 Кб (в случае использования черно-белых списков объём данных может увеличиться);
- Активность сотрудников: при работе сотрудника за ПК с периодичностью 1 раз в 5 минут отправляется упакованный zip-архив с информацией об активности сотрудника, размером до 5 Кб. В случае потери связи с сервером, агент аккумулирует информацию об активности сотрудника, и при восстановлении связи передает все ранее не отправленные данные;
- Удаленное обновление агентов: в случае обновления системы агенты удаленно скачивают новую версию и обновляются на неё, средний объем обновлений – 30 Мб;
- Отправка аварийных дампов агента: в случае аварийного завершения работы агента формируется дамп, который позже отправляется на сервер, размер передаваемого дампа до 150 Кб.

3.4.1.3 Порт

Порт настраивается в конфигурационном файле, по умолчанию используется 8010 порт.

3.4.1.4 Протокол

Все взаимодействие осуществляется по https протоколу, возможна настройка посредством конфигурационного файла.

3.4.2 Взаимодействие МНиА с сервером

3.4.2.1 Цель обмена

Целями обмена является:

- Получение собранной информации об активности сотрудника;
- Загрузка и передача данных логов других систем;
- Настройка Системы.

3.4.2.2 Объем и состав передаваемых/принимаемых данных

Работа модуля МНиА представляет из себя классическую работу веб-приложения (html, js, css, картинки, ajax-запросы).

3.4.2.3 Порт

Порт настраивается в конфигурационном файле, по умолчанию используется порт 8010.

3.4.2.4 Протокол

Все взаимодействие осуществляется по https протоколу, возможна настройка посредством конфигурационного файла.

3.4.3 Интерфейсы между компонентами Системы

Таблица 9

Интерфейсы между компонентами Системы

№	Название интерфейса	Тип подключения (протокол) потребителя	Потребитель	Поставщик	Объекты данных
1	Proceset agent	Https	Модуль настройки и аналитики	Модуль мониторинга активности пользователя	Компьютерная активность: • Заголовки окон • Названия документов и пути файлов • Названия вкладок для 1С и Microsoft Excel • URL интернет-браузеров • Названия программ • Моменты времени переключения окон на передний план • Моменты времени событий от нажатия клавиш клавиатуры и мыши Информация об активной сессии пользователя: • Имя пользователя • Логин пользователя • Часовой пояс пользователя • Домен пользователя Информация о компьютере: • название компьютера

№	Название интерфейса	Тип подключения (протокол) потребителя	Потребитель	Поставщик	Объекты данных
					• название рабочей группы • имя домена
3	Веб-интерфейс	Https	Пользователь системы	Модуль настройки и аналитики	– Анализируемые данные (Активность сотрудников, логи и т.п.) – html, js, css и т.п.

При разворачивании Системы только во внутренней сети, взаимодействие с внешней сетью (интернет) не предполагается, взаимодействие с DMZ не осуществляется.

3.5 Ролевая модель

3.5.1 Привилегии ролей доступа

Настройка и управление ролевой моделью производится через веб-интерфейс Системы, по следующим путям:

- Ролевая модель - «Меню»/ «Настройки»/ «Роли доступа»;
- Права доступа для Ключей API - «Меню»/ «Настройки»/ «Настройки системы»/ «Ключ API»;

Ролевая модель позволяет решать задачи для каждого типа пользователей. В Системе реализовано разграничение доступа пользователей:

- к функциональным возможностям Системы;
- к данным Системы (к справочникам о сотрудниках, мониторинг работы которых обеспечивает Система;
- к аналитическим отчетам Системы;
- к инструменту GraphQL.

Разграничение доступа пользователей к функциям и данным Системы реализовано с использованием ролевой модели и разграничением прав доступа для Ключей API. Каждому пользователю Системы могут назначаться роли доступа. Возможные действия пользователя в Системе определяются набором привилегий, соответствующих назначенной роли.

В веб-интерфейсе Системы для каждой роли доступа устанавливается набор разрешенных операций доступа по отношению к группе конкретных объектов. Для ролей доступа Системы доступны для назначения следующие операции доступа: R – чтение, W – изменение, где под изменением подразумевается возможность создания и удаления объекта.

Для Ключей API невозможно назначение ролей доступа. Для каждого Ключа API назначаются привилегии доступа отдельно, и могут иметь следующие операции доступа: R – чтение, W – изменение, C – создание, D – удаление. Система контроля доступа является «закрытой». Изначально объект не доступен никому. Привилегии доступа указаны в таблице 10.

Таблица 10

Привилегии доступа в Системе

Название	**Возможные Операции в Ролях доступа**	**Возможные операции для Ключей API**	**Страницы в Системе**
Привилегия «Общие настройки системы»	RW	RW	«Настройки»/ «Настройка системы»/ «Общие данные»
Привилегия «Почтовый сервер»	RW	RW	«Настройки»/ «Настройка системы»/ «Почтовый сервер»
Привилегия «Программы удалённого входа»	RW	RWCD	«Настройки»/ «Настройка системы»/ «Программы удаленного входа»
Привилегия «Параметры мониторинга»	RW	RW	«Настройки»/ «Настройка системы»/ «Мониторинг»
Привилегия «Фильтры активностей»	RW	RWCD	«Настройки»/ «Настройка системы»/ «Фильтр по активностям»
Привилегия «Ключи API»	RW	RWCD	«Настройки»/ «Настройка системы»/ «Ключ API»
Привилегия «Политика безопасности»	RW	RW	«Настройки»/ «Настройка системы»/ «Безопасность»
Привилегия «Лог»	RW	RCD	«Меню»/ «Конфигуратор»/ «Лог»
Привилегия «Активность»	RW	RC	«Меню»/ «Конфигуратор»/ «Активность»
Привилегия «Диагностика»	R	R	«Меню»/ «Диагностика»
Привилегия «Дистрибутив агента мониторинга»	R	R	«Меню»/ «Скачать агент»
Привилегия «Сотрудники и отделы»	RW	RWCD	«Настройки»/ «Настройка сотрудников»/ «Список сотрудников»
Привилегия «Доступы сотрудников»	RW	RW	«Настройки»/ «Настройка сотрудников»/ «Профиль сотрудника»
Привилегия «Должности»	RW	RWCD	«Настройки»/ «Настройка сотрудников»/ «Должности»
Привилегия «Роли доступа»	RW	-	«Настройки»/ «Настройка сотрудников»/ «Роли доступа»
Привилегия «Доступ к аналитическим отчётам»	RW	RW	«Настройки»/ «Настройка сотрудников»/ «Профиль сотрудника»
Привилегия «Личные настройки»	W	-	«Настройки»/ «Настройка сотрудников»/ «Профиль сотрудника»
Привилегия «Инструмент GraphQL»	R	-	-
Привилегия «Агент мониторинга»	-	R	«Username»

3.5.1.1 Привилегия «Общие настройки системы»

Привилегия «Общие настройки системы» отвечает за настройку следующих параметров Системы:

- Язык системы (общесистемный)
- Начало недели
- Формат инициалов
- База данных

Если у привилегии «общие настройки системы» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют право на просмотр значений параметров: язык системы, начало недели, формат инициалов, база данных. В веб-интерфейсе параметры представлены на страницах «Настройки»/ «Настройка системы»/ «Общие данные» и на «Настройки»/ «Настройка системы»/ «База данных».

Если у привилегии также выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют возможность изменять значения параметров: язык системы, начало недели, формат инициалов, а также осуществлять загрузку обезличенной базы данных.

3.5.1.2 Привилегия «Почтовый сервер»

Привилегия «Почтовый сервер» отвечает за настройку почтового сервера Системы. Если у привилегии «настройка почтового сервера» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют право на просмотр значений следующих параметров почтового сервера:

- Электронная почта
- Адрес
- Порт
- Шифрование
- Имя пользователя

Если у привилегии также выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют возможность изменять значения указанных выше параметров почтового сервера, в том числе и значение параметра «Пароль. Значение параметра «Пароль» почтового сервера недоступно для просмотра. Настройка параметров «Настройка почтового сервера» производится через веб-интерфейс: «Настройки»/ «Настройка системы»/ «Почтовый сервер».

3.5.1.3 Привилегия «Программы удалённого входа»

Привилегия «Программы удалённого входа» отвечает за настройку мониторинга программ удаленного входа в Системе. Если у привилегии «программы удалённого входа» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют право на просмотр значений следующих параметров: название программ удалённого входа. Пользователю будут доступны для просмотра все программы удалённого входа, которые используются в системе для сбора активности.

Если у привилегии выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют возможность изменять значение параметра «Название программы», которые используются для удалённого входа, а также создавать и удалять программы удалённого входа. Настройка параметров «Настройка

программ удалённого входа» производится через веб-интерфейс: «Настройки»/ «Настройка системы»/ «Программы удалённого входа».

Для Ключей API возможно отдельно назначить операцию доступа C – создание и D – удаление. Если установлено соединение по Ключ API, в котором установлены операции доступа, то возможно задавать значение «Название программы», которые используются для удалённого входа и удалять любую программу из списка программ удаленного входа.

3.5.1.4 Привилегия «Параметры мониторинга»

Привилегия «Параметры мониторинга» отвечает за настройку мониторинга в Системе. Привилегия «параметры мониторинга» отвечает за настройку следующих параметров мониторинга:

- Режим accessibility
- Агент собирает события
- Период бездействия

Если у привилегии «настройка параметров мониторинга» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ к Ключу API с данной привилегией имеют право на просмотр значений параметров, указанных выше. Если у привилегии также выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API с данной привилегией имеют возможность изменять значения указанных выше параметров. В веб-интерфейсе настройка параметров производится: «Настройки»/ «Настройка системы»/ «Мониторинг».

3.5.1.5 Привилегия «Фильтры активностей»

Привилегия «Фильтры активностей» отвечает за настройку фильтров по активностям (черно-белые списки). Если у привилегии «настройка фильтра по активностям» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API с данной привилегией имеют право на просмотр значений следующих параметров:

- Тип фильтра по активности
- Название программ для фильтра по активности

Для просмотра будет доступно какой фильтр по активности задан в системе, а также все программы, настроенные для заданного фильтра.

Если у привилегии выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API с данной привилегией имеют возможность изменять значение параметра «Название программы», который используется в фильтрации по активности, а также задавать значение фильтра по активности. В веб-интерфейсе настройка параметров производится: «Настройки»/ «Настройка системы»/ «Фильтр по активностям».

Для Ключей API возможно отдельно назначить операцию доступа C – создание и D – удаление. Если установлено соединение через Ключ API, в котором установлены операции доступа, то возможно задавать значение параметра «Название программы», который используется для фильтрации по активности и удалять любую программу из списка фильтра.

3.5.1.6 Привилегия «Ключи API»

Привилегия «Ключи API» отвечает за настройку Ключей API, с помощью которых осуществляется внешние и внутренние интеграции. Если у привилегии «Ключи API» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на просмотр значений следующих параметров:

- Название Ключа API
- Значение Ключа API
- Режим аутентификации
- Доступ к списку процессов Ключа API
- Привилегии Ключа API

Если у привилегии выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют возможность изменять значения существующих параметров, таких как: «Название Ключа API», «Доступ к списку процессов Ключа API», а также создавать и удалять Ключи API и задавать значения дня них. Параметр «Код доступа» конфигурируется системой и недоступен для изменения. В веб-интерфейсе настройка параметров производится: «Настройки»/ «Настройка системы»/ «Ключи API».

Для Ключей API возможно отдельно назначить операцию доступа C – создание и D – удаление. Если установлено соединение по Ключ API, в котором установлены данные операции доступа, то возможно создавать и удалять Ключи API в Системе.

3.5.1.7 Привилегия «Политика безопасности»

Привилегия «Политика безопасности» отвечает за настройку следующих параметров безопасности Системы:

- Проверка безопасности пароля
- Минимальная длина пароля
- Ограниченный срок действия пароля
- Срок действия пароля
- Ограничение количества попыток входа
- Количество допустимых попыток входа
- Оповещение о блокировке пользователей
- Экспорт списка сотрудников
- Статус сотрудника
- Доступ в систему

Если у привилегии «Политика безопасности» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на просмотр значений параметров, указанных выше.

Если у привилегии также выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют возможность изменять значения:

- Проверка безопасности пароля
- Минимальная длина пароля
- Ограниченный срок действия пароля
- Срок действия пароля
- Ограничение количества попыток входа

- Количество допустимых попыток входа
- Оповещение о блокировке пользователей
- Доступ в систему

И выполнять экспорт списка сотрудников. В веб-интерфейсе просмотр и настройка параметров производится: «Настройки»/ «Настройка системы»/ «Безопасность». Параметр «Оповещение о блокировке пользователей» в веб-интерфейсе представлен на странице: «Настройки»/ «Сотрудники»/ Профиль сотрудника»/ «Настройка доступа». Параметр «Экспорт списка сотрудников» в веб-интерфейсе представлен на странице: «Настройки»/ «Сотрудники». Параметр «Доступ в систему» в веб-интерфейсе представлен на странице: «Настройки»/ Профиль сотрудника»/ «Безопасность и вход»

3.5.1.8 Привилегия «Лог»

Привилегия «Лог» отвечает за настройку загрузки объектов типа: лог. Если у привилегии «Лог» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на просмотр всех объектов типа – лог. Пользователю будут доступны для просмотра все объекты типа - лог, которые были загружены в Систему. Если у привилегии выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют возможность загружать (создавать) объект – лог, а также удалять его. В веб-интерфейсе настройка параметров производится: «Настройки»/ «Загрузка данных»/ «Лог».

Для Ключей API возможно отдельно назначить операцию доступа C – создание и D – удаление. Если установлено соединение по Ключ API, в котором установлены данные операции доступа, то возможно создавать и удалять объект лог. Изменение лога невозможно, операция доступа W недоступна для Ключей API.

Если включена привилегия с операцией доступа W, то при загрузке лога в Системе могут быть автоматически созданы сотрудники.

3.5.1.9 Привилегия «Активность»

Привилегия «Активность» отвечает за настройку загрузки объектов типа: активность. Если у привилегии «Активность» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на просмотр всех объектов типа – активность. Пользователю будут доступны для просмотра объекты типа - активность, которые были загружены в Систему.

Если у привилегии выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют возможность загружать (создавать) объект – активность. Удаление загруженной активности в систему - невозможно. В веб-интерфейсе настройка параметров производится: «Настройки»/ «Загрузка данных»/ «Активность».

Для Ключей API возможно отдельно назначить операцию доступа C – создание. Если установлено соединение по Ключ API, в котором установлены данные операции доступа, то возможно создавать объект активность. Изменение и удаление активности невозможно, операция доступа W и D недоступны для Ключей API.

Если включена привилегия с операцией доступа W, то при загрузке активности в Системе могут быть автоматически созданы сотрудники.

3.5.1.10 Привилегия «Диагностика»

Привилегия «Диагностика» отвечает за настройку доступа к диагностике в Системе. У привилегии «диагностика» возможен выбор исключительно одной операции доступа R – чтение. Все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на просмотр следующих значений параметров:

- Название компьютеров (имя учётной записи ПК, на которую установлен агент мониторинга)
- Версия агента мониторинга (который установлен на ПК пользователя)
- Последнее время отклика агента (время, в которое последний раз приходила активность с агента мониторинга)
- Сотрудник (данные активности сотрудников)
- Программы (данные активности сотрудников, детализированная по программам)

Также всем сотрудникам, у которых назначена роль доступа с значением привилегии - R, имеют право на выполнение следующий действий:

- Фильтрация по версиям агента мониторинга
- Фильтрация по времени отклика агента
- Переход в профиль конкретного сотрудника
- Фильтрация активности по периоду
- Фильтрация активности по сотруднику

Доступен просмотр данных только тех сотрудников, к которым имеется доступ. Доступ к сотрудникам настраивается индивидуально для каждого пользователя, а не в рамках ролей доступа. В веб-интерфейсе настройка параметров производится: «Настройки»/ «Диагностика».

3.5.1.11 Привилегия «Дистрибутив агента мониторинга»

Привилегия «Дистрибутив агента мониторинга» отвечает за доступ к скачиванию дистрибутива агента мониторинга в Системе. У привилегии «Дистрибутив агента мониторинга» возможен выбор исключительно одной операции доступа R – чтение. Все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на настройку и скачивание агентов мониторинга. Возможна настройка и скачивание следующих агентов мониторинга:

- Агент Windows
- Агент Mac
- Агент GPO

Скачивание и настройка агентов мониторинга осуществляется через веб-интерфейс: «Настройки»/ «Скачать агент».

3.5.1.12 Привилегия «Сотрудники и отделы»

Привилегия «Сотрудники и отделы» отвечает за настройку Сотрудников и отделов в Системе. Если у привилегии «Сотрудники и отделы» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на просмотр значений следующих параметров:

- Список сотрудников
- Имя сотрудника

- Фамилия сотрудника
- Отчество сотрудника
- Место в иерархии сотрудника
- Название отделов
- Табельный номер сотрудника;
- Должность сотрудника;
- Отдел сотрудника;
- Часовой пояс сотрудника;
- Электронная почта сотрудника

Если у привилегии «Сотрудники и отделы» выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на изменение значений следующих параметров:

- Имя сотрудника
- Фамилия сотрудника
- Место в иерархии сотрудника
- Название отделов
- Табельный номер сотрудника;
- Должность сотрудника;
- Отдел сотрудника;
- Часовой пояс сотрудника;
- Электронная почта сотрудника
- Отправление приглашения в систему, а также создание, удаление сотрудников и групп (отделов).

Для Ключей API возможно отдельно назначить операцию доступа C – создание, D – удаление. Если установлено соединение по Ключ API, в котором установлены данные операции доступа, то возможно создавать сотрудника/отдел (операция C), удалять сотрудника/отдел (операция D).

В списке сотрудников отображаются только те сотрудники и их параметры, к которым имеет доступ пользователь. В веб-интерфейсе настройка параметров производится: «Настройки»/ «Сотрудники».

3.5.1.13 Привилегия «Доступы сотрудников»

Привилегия «Доступы сотрудников» отвечает за возможность настройки доступа Сотрудников в Системе. Если у привилегии «Доступы сотрудников» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на просмотр значений следующих параметров:

- Роль доступа сотрудника
- Доступ ко всем сотрудникам
- Выборочный доступ к сотрудникам
- Логин для входа в систему
- Список учетных записей (Источники сбора активности)

Если у привилегии «Доступы сотрудников» выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на изменение значений следующих параметров:

- Роль доступа сотрудника
- Доступ ко всем сотрудникам

- Выборочный доступ к сотрудникам
- Логин для входа в систему
- Пароль для входа в систему
- Список учетных записей (Источники сбора активности)

В веб-интерфейсе настройка параметров производится: «Настройки»/ «Сотрудники»/ Профиль сотрудника»/ «Настройка доступа».

3.5.1.14 Привилегия «Должности»

Привилегия «Должности» отвечает за настройку должностей в Системе. Если у привилегии «Должности» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на просмотр значений следующих параметров:

- Список должностей
- Название должности

Если у привилегии «Должности» выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на изменение значения параметра: «Название должности», а также возможность создания и удаление объекта должность.

В веб-интерфейсе настройка параметров производится: «Настройки»/ «Должности». На странице отображаются только принадлежность должности к тем сотрудникам к которым у пользователя существует доступ.

Для Ключей API возможно отдельно назначить операцию доступа C – создание, D – удаление. Если установлено соединение по Ключ API, в котором установлены данные операции доступа, то возможно создавать должность (операция C), удалять должность (операция D).

3.5.1.15 Привилегия «Роли доступа»

Привилегия «Роли доступа» отвечает за настройку Ролей доступа в Системе. Если у привилегии «Роли доступа» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют право на просмотр значений следующих параметров:

- Список ролей доступа
- Название роли доступа
- Привилегии роли доступа

Если у привилегии «Роли доступа» выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют право на изменение значения параметров:

- Название роли доступа
- Привилегии роли доступа

А также имеют права на создание и удаления ролей доступа. В веб-интерфейсе настройка параметров производится: «Настройки»/ «Роли доступа». На странице отображаются только принадлежность роли доступа к тем сотрудникам к которым у пользователя существует доступ. Назначение данной привилегии невозможно для Ключей API.

3.5.1.16 Привилегия «Доступ к аналитическим отчётам»

Привилегия «Доступ к аналитическим отчётам» отвечает за настройку доступа к аналитическим отчётам в Системе. Если у привилегии «Доступ к аналитическим отчётам» выбрана операция доступа R - чтение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API, имеют право на просмотр значений параметра «Доступ к списку процессов».

Если у привилегии «Доступ к аналитическим отчётам» выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, и все, кому предоставлен доступ по Ключу API имеют право на просмотр значений параметра «Доступ к списку процессов». В веб-интерфейсе настройка параметров производится: «Настройки»/ «Сотрудники» / «Профиль сотрудника» / «Настройки доступа».

Список процессов – это аналитический отчёт, который имеет вложенный отчёт «Карта процесса», и получение доступа к списку процессов подразумевает получения доступа ко всем аналитическим данным Системы.

3.5.1.17 Привилегия «Личные настройки»

Привилегия «Личные настройки» отвечает за настройку доступа к личным настройкам в Системе. У привилегии возможно выбрать только операцию доступа – W (изменение). Доступ на просмотр личных настроек существует у всех пользователей системы.

Если у привилегии выбрана операция доступа W - изменение, то все сотрудники, у которых назначена роль доступа с таким значением привилегии, имеют возможность изменять значение следующего параметра:

- Язык
- Пароль

Настройка параметра «личные настройки» производится через веб-интерфейс: «Меню»/ «Username».

3.5.1.18 Привилегия «Инструмент GraphQL»

Привилегия «Инструмент GraphQL» отвечает за настройку доступа к инструменту GraphQL в Системе. У привилегии возможно выбрать только операцию доступа – R (чтение). По привилегии R – пользователь получает доступ к инструменту GraphQL (подробнее о инструменте GraphQL в Руководство администратора см. 6) Привилегию невозможно назначить для Ключей API.

3.5.1.19 Привилегия «Агент мониторинга»

Привилегия «Агент мониторинга» отвечает за соединение агентам мониторинга и сервера в Системе. Привилегию невозможно применить для ролей доступа. Привилегию можно назначить исключительно для Ключей API. Привилегия предназначена для агента мониторинга. Операция доступа R (чтение) предоставляет возможность:

- Получать актуальную версии агента мониторинга;
- Получать дистрибутив агента мониторинга для обновления;
- Получать настройки агента мониторинга;
- Получать ФИО сотрудника по внутреннему идентификатору сотрудника;
- Получать список поддерживаемых протоколов агентских данных;
- Загружать данные с активностью агента мониторинга;
- Загружать дамп-файлы агента мониторинга;
- Получение черно-белых списков;

3.5.2 Доступ к сотрудникам и отделам

Доступ к сотруднику и к его данным назначается на странице: Настройки доступа в параметре: «Доступные сотрудники». Доступ к отделу назначается также в этом параметре.

Доступ к отделу означает, что сотрудник получает доступ ко всем сотрудникам этого отдела согласно иерархии и к данным этих сотрудников. Если в отдел добавляется сотрудник, то к нему предоставляется доступ тем сотрудникам, у которых данный отдел находится в доступе. Также если сотрудник перемещается/удаляется из отдела, то доступ к нему пропадает у тех сотрудников, у которых данный отдел в доступе.

Параметр «Доступные сотрудники» появляется в Настройки доступа только при следующих условиях:

Назначена роль доступа, сотруднику, который просматривает страницу со следующими привилегиями:

- Привилегия «Сотрудники и отделы»;
- Привилегия «Доступы сотрудников»;

3.5.3 Доступ к аналитическим отчётам

Доступ к аналитическим отчётам назначается на странице: «Настройки доступа», в параметре: «Доступ к списку процессов». Параметр «Доступ к списку процессов» появляется в «Настройки доступа» у сотрудника только при следующих условиях: Назначена роль доступа со следующими привилегиями:

- Привилегия «Доступ к аналитическим отчётам»
- Привилегия «Доступы сотрудников»;

В отчётах предоставляется только информация по тем сотрудникам/отделам, которые есть в доступе у пользователя. Исключение из правила: аналитический отчёт «Список процессов», «Карта процесса». Аналитический отчёт «Список процессов» имеет сводную информацию по всем сотрудникам. Если сотруднику предоставляется доступ к отчёту «Список процессов», он имеет возможность просматривать карту процессов по всему процессу и по всем сотрудникам. Фильтрация возможна исключительно по доступным сотрудникам и отделам.

Аналитический отчёт «Карта процесса» имеет сводную информацию по всем сотрудникам, которые анализируются. Данные содержат информацию из логов других систем и агентов мониторинга, поэтому разграничение доступа по сотрудникам в рамках данного аналитического отчёта невозможно. Если сотруднику предоставляется доступ к отчёту «Карта процессов», он имеет возможность просматривать карту процессов по всему процессу и по всем сотрудникам. В детализации карты процессов (Список активностей в операции процесса) сотрудник имеет возможность просматривать исключительно информацию по всем доступным сотрудникам.

По умолчанию, первому пользователю, который устанавливает систему (прикладной администратор) по умолчанию включается доступ к аналитическим отчётам.

3.5.4 Доступ к диагностике

Доступ к отчёту «Диагностика» предоставляется в том случае, если у сотрудника назначена роль доступа с привилегией «Диагностика». Данные диагностики отображаются исключительно по доступным сотрудникам.

3.5.5 Предустановленные роли доступа

По умолчанию после установки Системы существует пять ролей доступа:

- «Прикладной администратор» (ПА);
- «Администратор ИБ» (АИБ);
- «Бизнес-администратор» (БА);

- «Аналитик» (А);
- «Аудитор ДВА» (АДВА).

Матрица прав доступа по привилегиям для предустановленных ролей приведена в таблице ниже.

Таблица 11

Матрица прав доступа по привилегиям для предустановленных ролей

Название	**ПА**	**АИБ**	**БА**	**А**	**АДВА**
Привилегия «Общие настройки системы»	RW	R	-	-	R
Привилегия «Почтовый сервер»	RW	R	-	-	R
Привилегия «Программы удалённого входа»	RW	R	-	-	R
Привилегия «Параметры мониторинга»	RW	R	RW	-	R
Привилегия «Фильтры активностей»	RW	R	RW	-	R
Привилегия «Ключи API»	RW	R	-	-	R
Привилегия «Политика безопасности»	RW	R	-	-	R
Привилегия «Лог»	RW	R	R	-	R
Привилегия «Активность»	RW	R	R	-	R
Привилегия «Диагностика»	R	R	R	-	R
Привилегия «Дистрибутив агента мониторинга»	R	R	-	-	R
Привилегия «Сотрудники и отделы»	RW	R	R	R	R
Привилегия «Доступы сотрудников»	RW	R	-	-	R
Привилегия «Должности»	RW	R	-	-	R
Привилегия «Роли доступа»	RW	R	-	-	R
Привилегия «Доступ к аналитическим отчётам»	RW	R	RW	-	R
Привилегия «Личные настройки»	W	W	W	W	R
Привилегия «Инструмент GraphQL»	R	R	-	-	R

Роль «Прикладной администратор» имеет возможность вносить изменения в конфигурацию Системы, включая средства защиты.

Полномочия по использованию web-интерфейса предоставляются всем ролям доступа. Полномочия по использованию инструмента GraphQL предоставляются исключительно следующим ролям доступа:

- «Прикладной администратор»;
- «Администратор ИБ»;
- «Аудитор ДВА».

3.5.6 Матрица конфликтных ролей доступа

Таблица 12

Матрица конфликтных ролей

	«Прикладной администратор»	**«Бизнес администратор»**	**«Администратор ИБ»**	**«Аналитик»**	**«Аудитор ДВА»**
«Прикладной администратор»		X	X	X	X
«Бизнес администратор»	X		X		X
«Администратор ИБ»	X	X		X	X
«Аналитик»	X		X		X
«Аудитор ДВА»	X	X	X	X	

Символ «X» в таблице означает невозможность совмещения ролей.

3.5.7 Дополнительная информация по ролям доступа

- Первому пользователю системы назначается роль доступа «Прикладной администратор»;
- При установке нового модуля никому не даётся никакой роли доступа в нём;
- Имя роли доступа должно быть уникально. Задать одинаковое значение "имя" роли доступа невозможно;
- Удалить роль доступа «Прикладной администратор» невозможно.
- Если в Системе остался один сотрудник, у которого назначена роль доступа с привилегией «Роли доступа» с операцией доступа W, то в таком случае:
    - Невозможно у этой роли доступа изменить/выключить данную привилегию;
    - У данного сотрудника в профиле в «Общие данные сотрудника» обязательно должны быть заполнены поля «Электронная почта», «Пароль» (для возможности восстановления пароля и авторизации);
    - У данного сотрудника в профиле в «Настройки доступа» нельзя удалить роль доступа, у которой назначена привилегия «Роли доступа», в том случае если роль доступа является последней из всех, в которой включена привилегия «Роли доступа»;

3.5.8 Права доступа для Ключей API

Для каждого ключа API можно назначить права доступа. Соединение с внешними системами происходит через конкретный ключ API, которому назначены определенный набор прав доступа. Права доступа для Ключа API назначаются при назначении операций доступа в привилегии R – чтение, W – изменение, C – создание, D – удаление. Для Ключа API возможно назначение следующих привилегий:

- Привилегия «Общие настройки системы»
- Привилегия «Почтовый сервер»
- Привилегия «Программы удалённого входа»
- Привилегия «Параметры мониторинга»
- Привилегия «Фильтры активностей»
- Привилегия «Ключи API»
- Привилегия «Политика безопасности»
- Привилегия «Лог»
- Привилегия «Активность»
- Привилегия «Диагностика»

- Привилегия «Дистрибутив агента мониторинга»
- Привилегия «Сотрудники и отделы»
- Привилегия «Доступы сотрудников»
- Привилегия «Должности»
- Привилегия «Доступ к аналитическим отчётам»
- Привилегия «Агент мониторинга»

Подробнее о каждой привилегии указано в п. 3.5.1.

4. Интеграции Системы с АС

4.1 Взаимодействие между Системами и АС

Взаимодействия между Системой и другими АС осуществляется с помощью двухсторонней SSL-аутентификации и путем использования, предоставляемого API Системы. Работа API Системы описана в документе «Руководство администратора информационной безопасности» (см., п. 6).

Для установления безопасного соединения с клиентской авторизацией между интеграцией и сервером необходимо создать безопасный ключ API. (см Руководство прикладного администратора, п. 2.2.1.)

На стороне интеграции необходимо настроить https и хранилище сертификатов, после чего можно делать Graphql запросы к серверу.

4.2 Системы для интеграции

4.2.1 ММАП (Агент мониторинга)

Внутренняя интеграция ММАП и МНиА реализуется для автоматической передачи информации о моментах переключений пользователя из агента мониторинга в БД. Цели взаимодействия, перечни и форматы передаваемой информации при интеграции представлены в п. 3.4.1. На этапе опытной эксплуатации и промышленного внедрения интеграция реализуется с помощью API системы. Инструкция по созданию безопасного соединения ММАП и МНиА представлена в Руководстве прикладного администратора п.1.4.1. Безопасным является соединение, в котором используется механизм взаимной аутентификации.

4.3 Протокол передачи данных

Передача данных между модулями, а также сторонними системами осуществляется по протоколу Https.

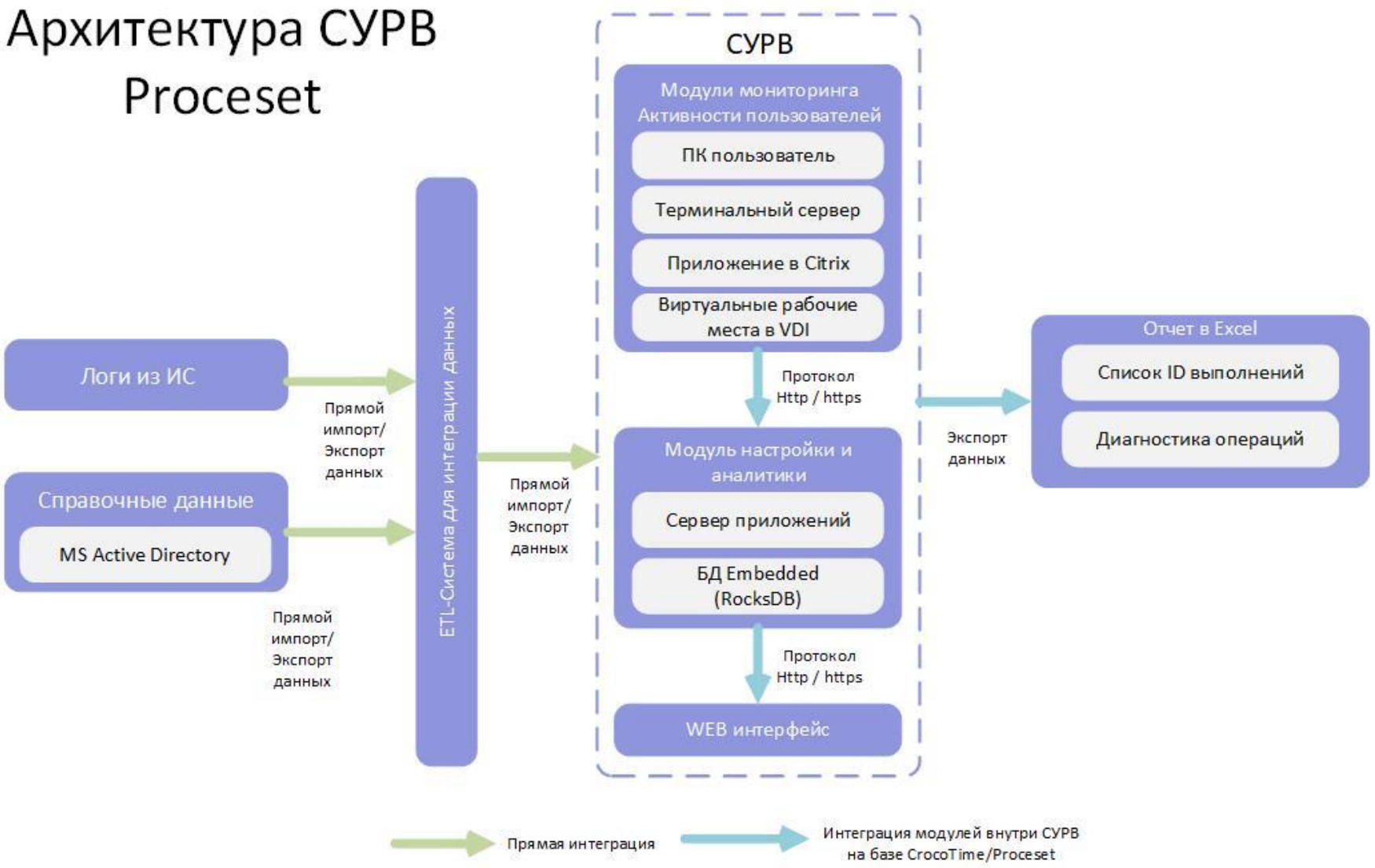
4.5 Аутентификация между Системами и АС

Между сервером и Агентом мониторинга (ММАП) осуществляется взаимная аутентификация посредством Ключей API. Для каждого Ключа API задаётся набор привилегий, в рамках которых регламентируются права доступа в Системе. (см. 3.5.1) Взаимная аутентификация предполагает авторизацию клиентов на сервере с помощью клиентских SSL сертификатов. Инструкция по настройки агентов мониторинга по безопасному соединению см. Руководство администратора п. 4.3.3.

Взаимная аутентификация с другими АС также предполагает авторизацию клиентов на сервере с помощью клиентских SSL сертификатов. Инструкция по настройки Ключей API представлена в Руководство администратора п.3.1.3.

Приложение №1

Схема взаимодействия внутренних компонентов Системы, а также взаимодействия со смежными системами



Приложение № 2

Права доступа пользователей

№	Название роли в АС	Предоставляемые права и полномочия в терминах АС	Роль имеет возможность вносить изменения в конфигурацию АС, включая средства защиты
1	«Прикладной администратор»	- Просмотр и изменение общих настроек системы; - Просмотр и изменение настроек почтового сервера; - Просмотр, создание, удаление, изменение программ удалённого входа; - Просмотр и изменение настроек параметров мониторинга; - Просмотр, создание, удаление, изменение фильтров по активностям; - Просмотр, создание, удаление, изменение ключей API; - Просмотр и изменение настроек политики безопасности; - Просмотр, создание (загрузка), удаление объекта лог; - Просмотр, создание (загрузка) объекта активность; - Просмотр диагностики; - Скачивание агента мониторинга; - Просмотр, создание, удаление, изменение общих данных о сотрудниках Системы; - Просмотр, изменение доступов сотрудников Системы; - Просмотр, создание, удаление, изменение общих данных о должностях; - Просмотр, создание, удаление, изменение ролей доступа; - Просмотр, изменение настройки доступа к аналитическим отчётам; - Просмотр и изменение личных настроек; - Доступ к инструменту GraphQL; - Полный доступ ко всем данным всех сотрудников, которые существуют к Системе; - Доступ ко всем аналитическим отчётам, которые существуют в Системе;	да
	«Администратор ИБ»	- Просмотр общих настроек системы; - Просмотр настроек почтового сервера; - Просмотр программ удалённого входа;	нет

№	Название роли в АС	Предоставляемые права и полномочия в терминах АС	Роль имеет возможность вносить изменения в конфигурацию АС, включая средства защиты
		- Просмотр настроек параметров мониторинга; - Просмотр фильтров по активностям; - Просмотр настроек ключей API; - Просмотр настроек политики безопасности; - Просмотр объекта лог; - Просмотр объекта активность; - Просмотр диагностики; - Скачивание агента мониторинга; - Просмотр общих данных о сотрудниках Системы; - Просмотр доступов сотрудников Системы; - Просмотр общих данных о должностях; - Просмотр настроек ролей доступа; - Просмотр доступа к аналитическим отчётам; - Просмотр и изменение личных настроек; - Доступ к инструменту GraphQL; - Полный доступ ко всем данным всех сотрудников, которые существуют к Системе; - Доступ к доступным аналитическим отчётам.	
2	«Бизнес Администратор»	- Просмотр и изменение настроек параметров мониторинга; - Просмотр и изменение настроек фильтров по активностям; - Просмотр объекта лог; - Просмотр объекта активность; - Просмотр диагностики; - Просмотр общих данных о доступных сотрудниках Системы; - Просмотр и настройка доступа к аналитическим отчётам; - Просмотр и изменение личных настроек; - Доступ к общим данным только доступных сотрудников, которые существуют к Системе; - Доступ к доступным аналитическим отчётам.	нет
4	«Аналитик»	- Просмотр общих данных о доступных сотрудниках Системы; - Просмотр и изменение личных настроек; - Доступ к доступным аналитическим отчётам.	нет
5	«Аудитор ДВА»	- Просмотр общих настроек системы; - Просмотр настроек почтового сервера;	нет

№	Название роли в АС	Предоставляемые права и полномочия в терминах АС	Роль имеет возможность вносить изменения в конфигурацию АС, включая средства защиты
		- Просмотр программ удалённого входа; - Просмотр настроек параметров мониторинга; - Просмотр фильтров по активностям; - Просмотр настроек ключей API; - Просмотр настроек политики безопасности; - Просмотр объекта лог; - Просмотр объекта активность; - Просмотр диагностики; - Скачивание агента мониторинга; - Просмотр общих данных о сотрудниках Системы; - Просмотр доступов сотрудников Системы; - Просмотр общих данных о должностях; - Просмотр настроек ролей доступа; - Просмотр доступа к аналитическим отчётам; - Просмотр и изменение личных настроек; - Доступ к инструменту GraphQL; - Полный доступ к общим данным всех доступных сотрудников, которые существуют к Системе; - Доступ к доступным аналитическим отчётам.	