

## Программа для ЭВМ «Атом.проект Базовый релиз»

**Руководство администратора безопасности**

Листов: 17

Дата: 08.11.2023

Версия: 1.0



Лист изменений

| Дата | Версия | Краткое описание изменений | ФИО |
| --- | --- | --- | --- |
| 08.11.2023 | v.1.0.0 | Документ создан | Истомин В.В. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Аннотация

В настоящем документе приведено руководство администратора безопасности по установке и настройке программы для ЭВМ «Атом.Проект: Базовый релиз» (далее – Программа).

В разделе «Общие сведения о программе» указаны назначение и функции Программы, сведения о технических и программных средствах, обеспечивающих выполнение Программы.

В разделе «Структура программы» приведены сведения о структуре программы, ее составных компонентах и модулях.

В разделе «Настройка программы» приведено описание действий по настройке Программы на условиях конкретного применения.

В разделе «Проверка программы» приведено описание способов проверки, позволяющих дать общее заключение о работоспособности Программы.

Структура и оформление настоящего документа соответствует ГОСТ 19.503-79.

Примечание. В связи с постоянным развитием Программы элементы интерфейса и значения ее фактических параметров могут отличаться от документированных.

Содержание

[1 Общие сведения о программе 7](#_Toc153796239)

[1.1 Назначение программы 7](#_Toc153796240)

[1.2 Условия применения 7](#_Toc153796241)

[1.2.1 Требования к серверу Программы «Атом.Проект: Базовый релиз» 7](#_Toc153796242)

[1.2.2 Требования к рабочим станциям 8](#_Toc153796243)

[2 Структура программы 9](#_Toc153796244)

[3 Настройка программы 10](#_Toc153796245)

[3.1 Предоставление доступа пользователю к программе 10](#_Toc153796246)

[3.2 Параметры взаимодействия с OpenID провайдером (АтомID) 13](#_Toc153796247)

[3.3 Настройка учётных данных пользователей 13](#_Toc153796248)

[3.4. Журналирование событий безопасности 15](#_Toc153796249)

[3.5. Журналирование пользовательских событий и аудит событий безопасности 15](#_Toc153796250)

[4 Получение JWT-токена. 17](#_Toc153796251)

**Глоссарий**

| **Термины/сокращения** | **Определение** |
| --- | --- |
| ЭВМ | Электронно-Вычислительная Машина |
| OpenID | Открытый стандарт децентрализованной системы аутентификации, предоставляющей пользователю возможность создать единую учётную запись для аутентификации на множестве не связанных друг с другом ресурсов |
| Каталог AD | Microsoft Active Directory. Служба каталогов, для использования групповых политик и для обеспечения единообразия настройки пользовательской рабочей среды |
| Атом.Проект, Программа, Система | Система для работы с задачами, создания графиков, дашбордов. |
| УЗ | Учетная запись |
| Пользователь | Сотрудник, получивший доступ к Программе на основании правил разграничения доступа. |
| CI/CD | Комбинация непрерывной интеграции (continuous integration) и непрерывного развертывания (continuous delivery или continuous deployment) программного обеспечения в процессе разработки |
| KeyCloak | Продукт с открытым кодом для реализации single sign-on с возможностью управления доступом, нацелен на современные приложения и сервисы. |
| GitLab | Веб-инструмент жизненного цикла DevOps с открытым исходным кодом, представляющий систему управления репозиториями кода для Git с собственной вики, системой отслеживания ошибок, CI/CD пайплайном и другими функциями |
| OpenProject | Открытое серверное веб-приложение для управления проектами и задачами (в том числе для отслеживания ошибок) |
| REST API | REST (от англ. Representational State Transfer — «передача репрезентативного состояния» или «передача „самоописываемого“ состояния») — архитектурный стиль взаимодействия компонентов распределённого приложения в сети. |
| PostgreSQL | Cвободная объектно-реляционная система управления базами данных (СУБД). |
| JWT | JSON Web Token (JWT) — это открытый стандарт (RFC 7519) для создания токенов доступа, основанный на формате JSON. |
| JSON | Текстовый формат обмена данными, основанный на JavaScript. |
| JavaScript | Мультипарадигменный язык программирования. |

# Общие сведения о программе

## Назначение программы

Программа для ЭВМ «Атом.Проект: Базовый Релиз» (далее — Программа) предназначена для работы с задачами, создания графиков, дашбордов.

Программа может использоваться для создания, изменения, задач, графиков, дашбордов.

Функциональные возможности программы:

1. Работа задачами – создание и изменение задач (значений полей и статусов). Работа с графиками – создание, настройка, определение параметров.
2. Встроенные активности – набор встроенных активностей создание и редактирование графиков, таблиц, дашбордов, работа в браузере, работа с файлами и т.д.

## Условия применения

### Требования к серверу Программы «Атом.Проект: Базовый релиз»

Требования к аппаратному обеспечению сервера Программы «Атом.Проект: Базовый релиз» приведены в таблице Таблица 1.

**Таблица 1 – Требования к аппаратному обеспечению сервера**

| **№** | **Параметр** | **Минимальное значение** | **Рекомендуемое значение** |
| --- | --- | --- | --- |
|  | Архитектура процессора | x86\_64 | x86\_64 |
|  | Тактовая частота процессора, ГГц | 1.8 | не менее 2 |
|  | Количество ядер процессора, шт. | 2 | 4 |
|  | Объем оперативной памяти, ГБ | 2 | 4 |
|  | Доступное свободное место на накопителе на жестких магнитных дисках или твердотельном накопителе, Гбайт | 20 | 50 |
|  | Пропускная способность сетевого интерфейса, Мбит/с | 100 | 1000 |

### Требования к рабочим станциям

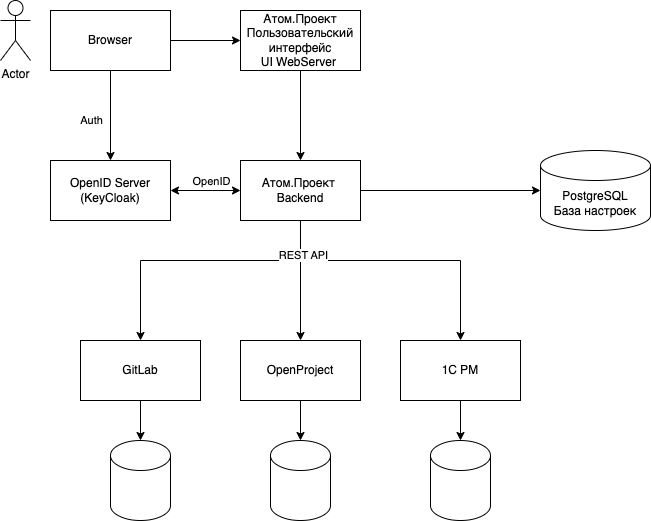
Требования к аппаратному обеспечению рабочих станций приведены в таблице Таблица 2.

**Таблица 2 – Требования к аппаратному обеспечению рабочих станций**

| **№** | **Параметр** | **Без создания**  **виртуальной машины** | | **С созданием**  **виртуальной машины** | |
| --- | --- | --- | --- | --- | --- |
| **Минимальное значение** | **Рекомендуемое значение** | **Минимальное значение** | **Рекомендуемое значение** |
|  | Архитектура процессора | x86\_64 | x86\_64 | x86\_64 | x86\_64 |
|  | Тактовая частота процессора, ГГц | 1.2 | 1.2 | 1.8 | 2 |
|  | Количество ядер процессора, шт. | 2 | 2 | 4 | 4 |
|  | Объем оперативной памяти, ГБ | 2 | 4 | 8 | 8 |
|  | Доступное свободное место на накопителе на жестких магнитных дисках или твердотельном накопителе, Гбайт | 20 | 50 | 100 | 200 |
|  | Операционная система | Windows 10, Astra Linux | Windows 10, Astra Linux | Windows 10, Astra Linux | Windows 10, Astra Linux |

# Структура программы

Структура Программы и схема взаимодействия компонентов представлены на рисунке 1.



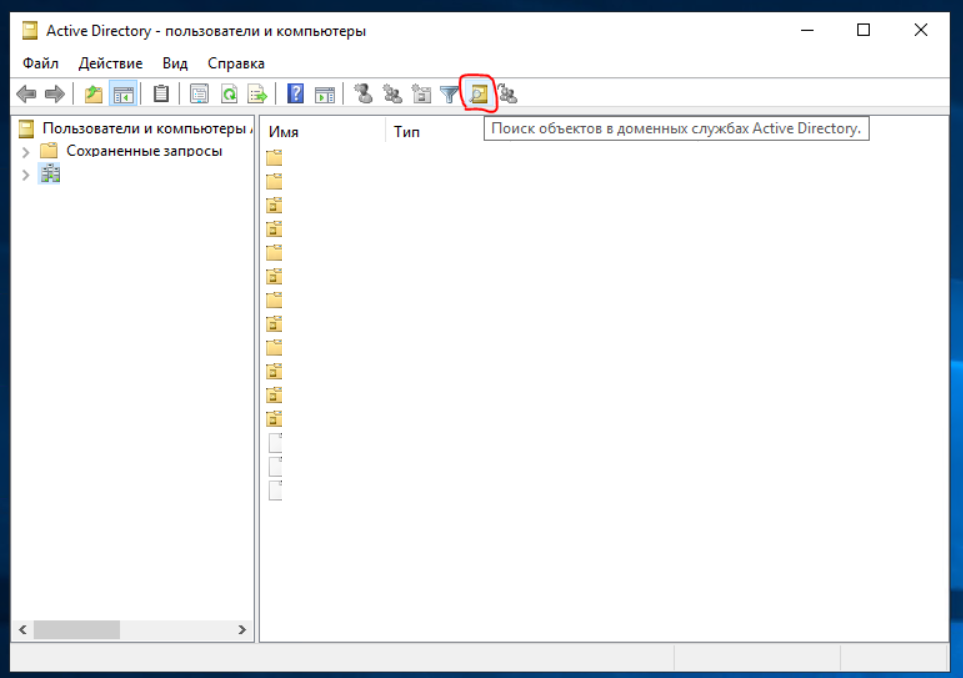
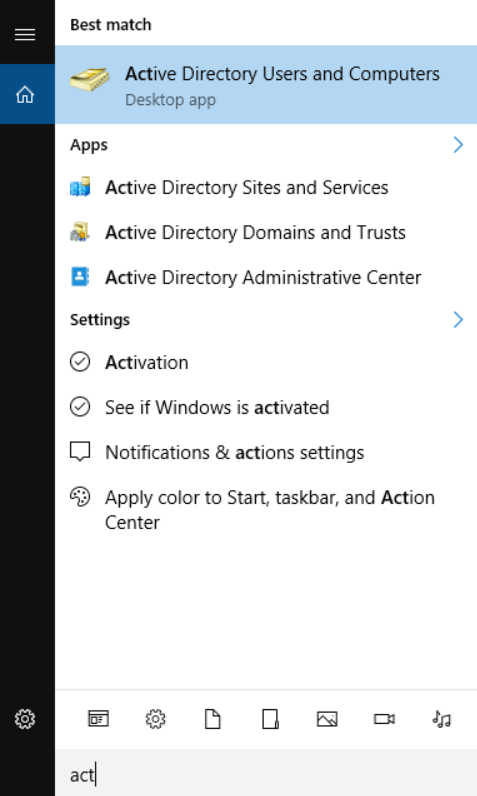
**Рисунок 1 – Структура Программы**

# Настройка программы

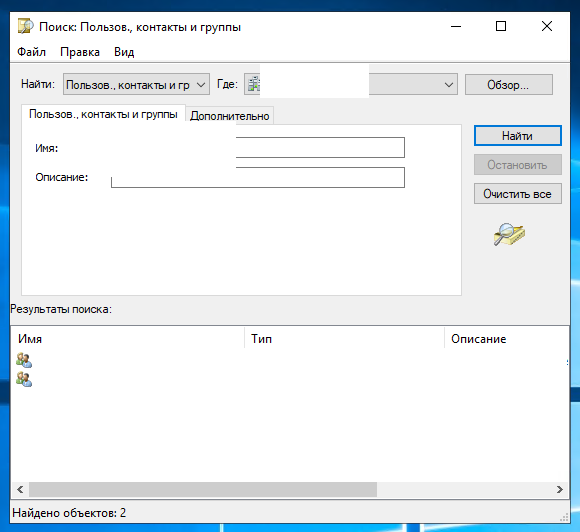
## Предоставление доступа пользователю к программе

Для доступа к программе пользователь должен быть предварительно добавлен в доменный каталог и ему должна быть предоставлена роль или назначена группа с доступом к «Атом.Проект: Базовый релиз».

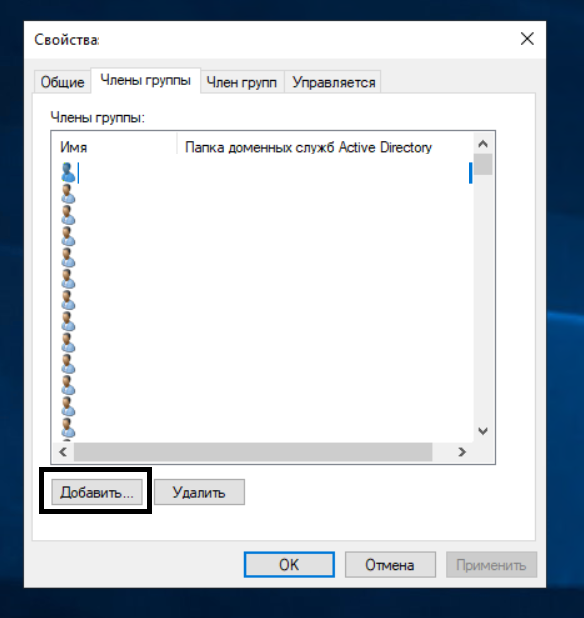
Например, Администратор безопасности заходит в Active Directory как показано на рисунках ниже.



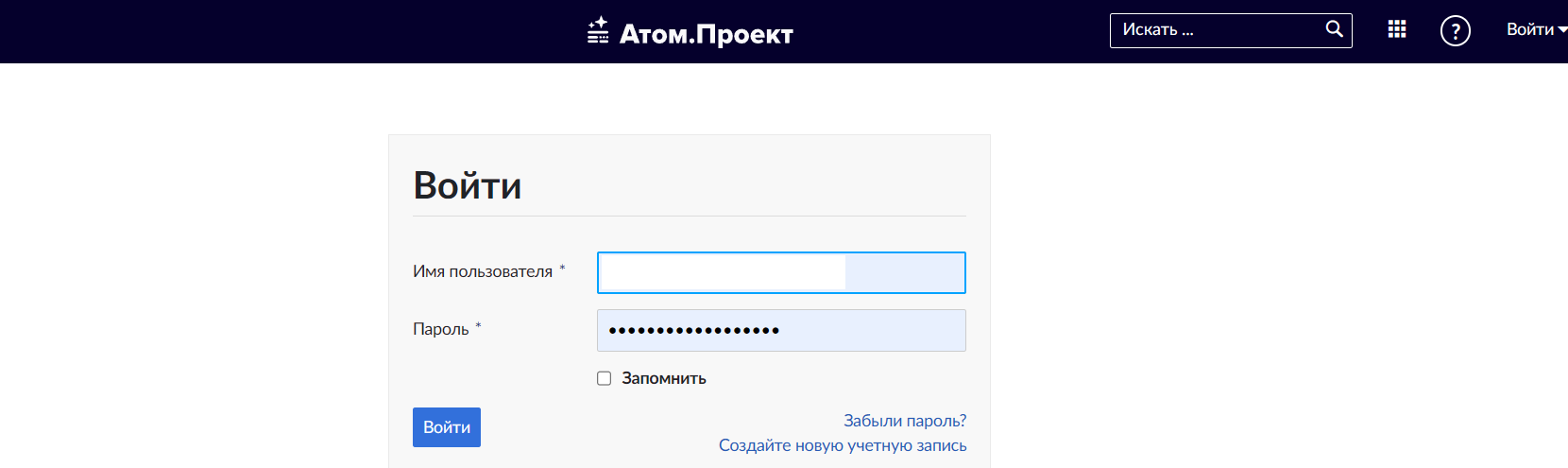
Находит необходимую группу



Добавляет в группу УЗ сотрудника



Также необходимо проверить, что учетной записи предоставлен доступ в систему: для этого перейти в браузере по адресу где установлен «Атом.Проект: Базовый релиз»



Аналогичным образом пользователю может быть предоставлен доступ ко всем «подключаемым» системам.

Форма аутентификации может отличаться от примера выше, и зависит от конкретных настроек системы аутентификации принятой в организации.

В «Атом.Проект: Базовый релиз» интегрировано взаимодействие с провайдером aутентификационной информации по протоколу OpenID в виде токена JWT.

## Параметры взаимодействия с OpenID провайдером (АтомID)

При взаимодействии с ИС «AtomID» программа «Атом.Проект: Базовый релиз» получает и использует следующую информацию о пользователе:

1. Атрибуты AD:

* Upn;
* E-mail.

1. Из них в составе JWT токенов:

* Upn;
* E-mail.

## Настройка учётных данных пользователей

В программе «Атом.Проект: Базовый Релиз» не происходит хранение учётных данных пользователей. Программа не хранит и не обрабатывает персональные данные.   
Процесс аутентификации производится во внешней системе аутентификации. Адрес провайдера OpenID указывается в конфигурационном файле keycloak.json.

Пример keycloak.json:

{

"auth-server-url": "https://<host>:<port>/auth",

"realm": "master",

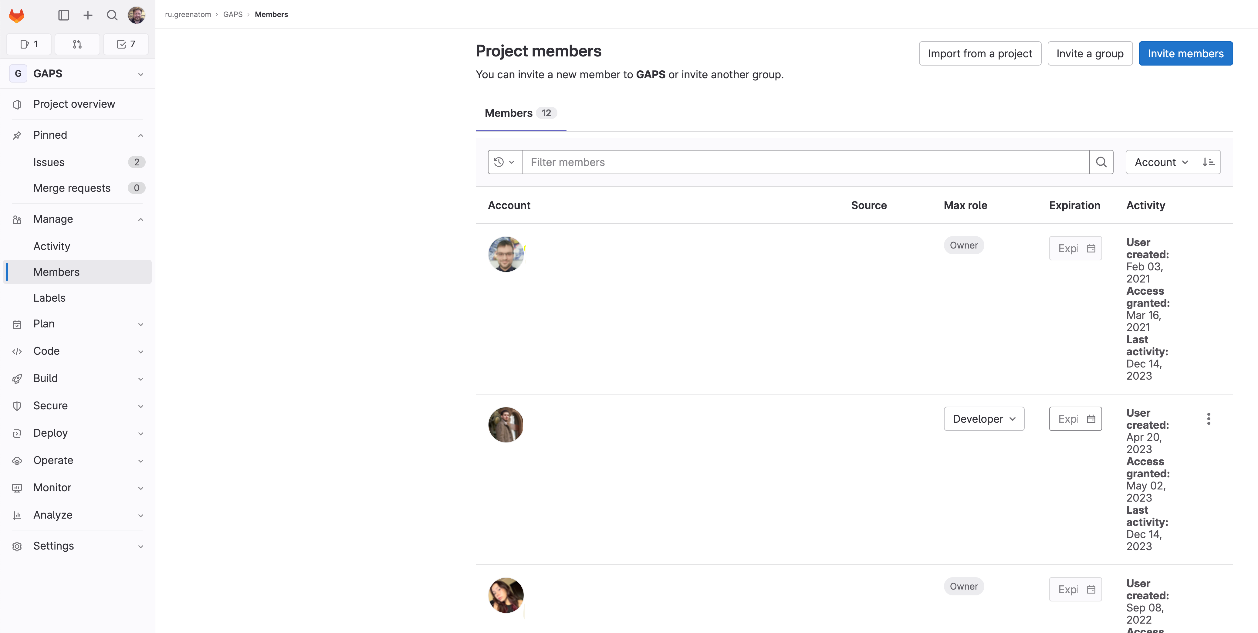
"resource": "test"

}

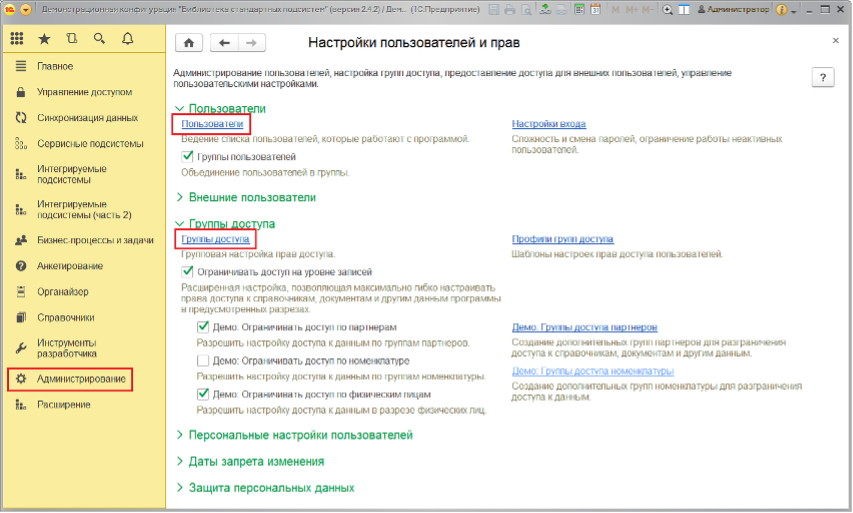
Для аутентификации и авторизации в целевой системе используется предварительно полученный клиентом из системы АтомID JWT-токен.

Права пользователя по доступу к проектам и задачам настраиваются в каждой целевой системе отдельно.

Например, в GitLab для выдачи прав на проект нужно зайти в пункт меню Manage->Members



Для систем, построенных на базе 1С, права назначаются в соответствующем пункте меню «Администрирование»



## **Журналирование событий безопасности**

Журналирование событий аутентификации происходит во внешней системе которая проводит аутентификацию и выдачу JWT. Например, для провайдеров OpenID, построенных на базе KeyCloak, вывод таких событий происходит в специальный журнальный файл. Для получения информации о настройках используемого провайдера, нужно обратиться к соответствующему руководству. Например для KeyCloak и основанных на нем провайдеров можно использовать описание расположенное по адресу <https://www.keycloak.org/server/logging.>

## **Журналирование пользовательских событий и аудит событий безопасности**

В «Атом.Проект: Базовый релиз» журналирование событий производится встроенной библиотекой logback. Настройки журналов проводится в файле logback.xml. Пример настроек:

<appender name="USER\_FILE" class="ch.qos.logback.core.rolling.RollingFileAppender">

<file>../logs/gaps-user.log</file>

<rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">

<fileNamePattern>../logs/gaps-user\_%d.log.gz</fileNamePattern>

<maxHistory>15</maxHistory>

</rollingPolicy>

<encoder class="ch.qos.logback.classic.encoder.PatternLayoutEncoder">

<pattern>%date %level [%thread] %logger{40} %msg%n</pattern>

</encoder>

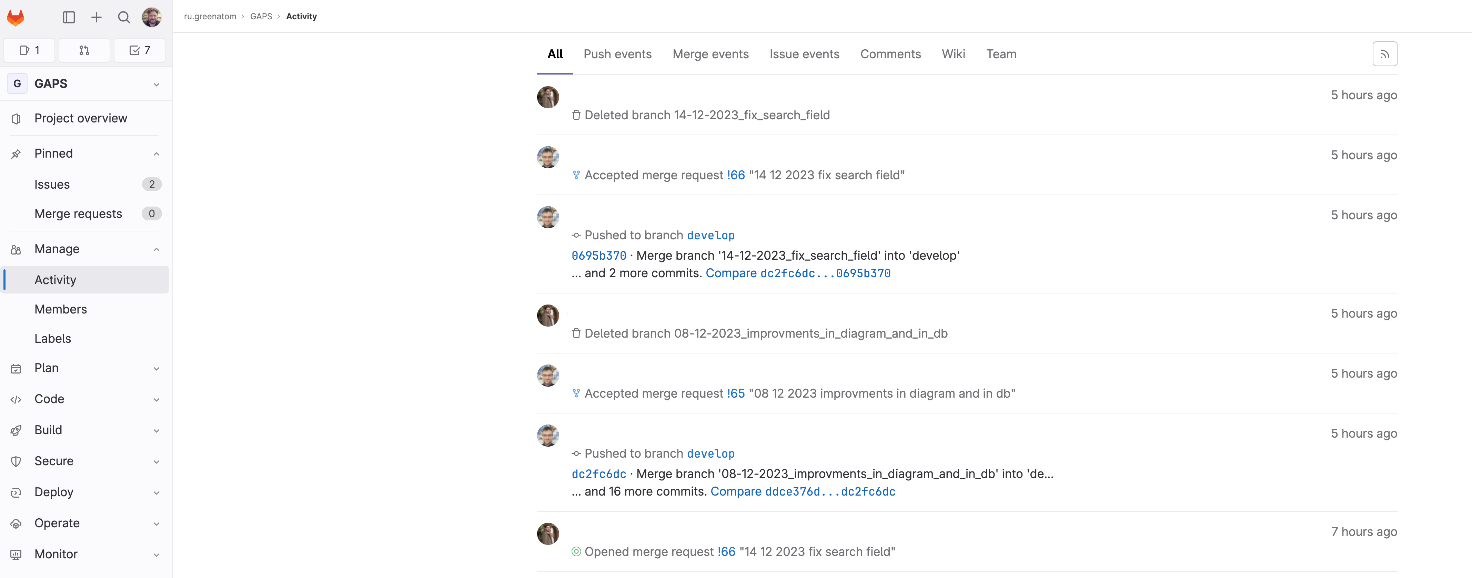
</appender>

<logger name="ru.greenatom.gaps" level="INFO" additivity="false">

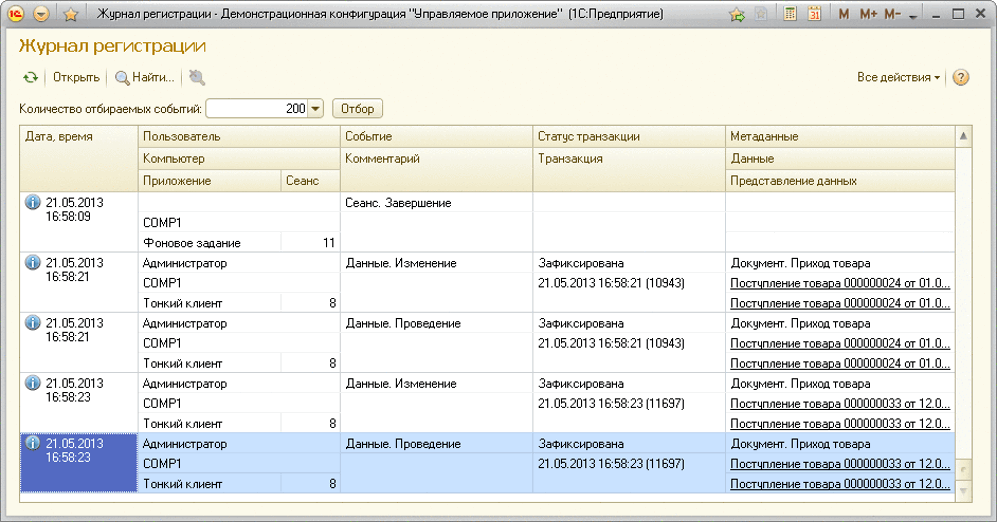
<appender-ref ref="USER\_FILE"/>

</logger>

Аудит доступа к проектам и задачам происходит средствами целевых систем. Например, в GitLab можно перейти в пункт меню Manage->Activity.

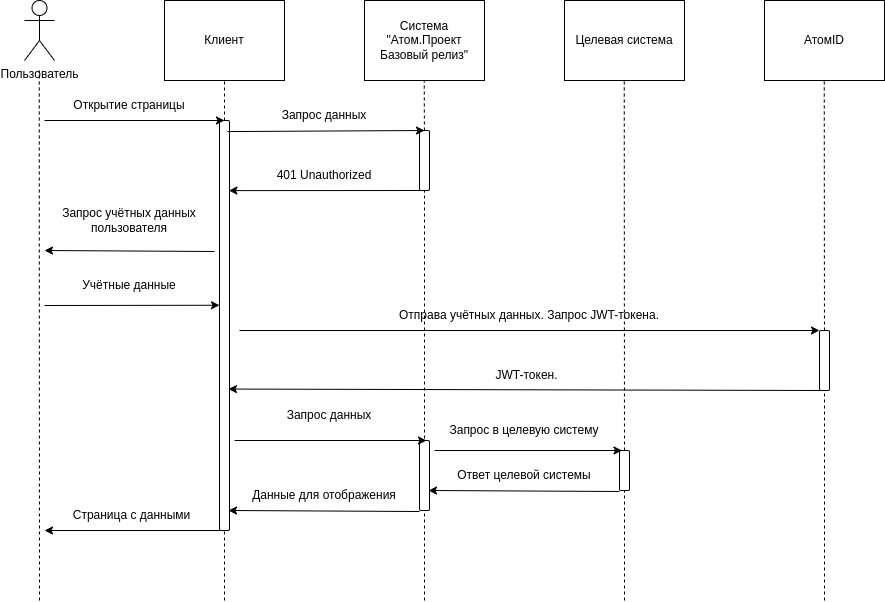


В системах построенных на базе 1С это журнал доступен в соответствующем пункте меню «Администрирование».



# Получение JWT-токена.

Схема получения JWT-токена представлена на рисунке2*.*



**Рисунок 2 – Схема получения JWT-токена.**