|  |  |
| --- | --- |
|  | **УТВЕРЖДАЮ** |
|  | Генеральный директор  ООО «ОМС Солюшн» |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.Б. Груданов |
|  | «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

**Сиcтема контроля прав доступа**

**«Матрица доступа»**

**Описание программы**

**Лист утверждения**

58.29.29-001-29233469-2020 13 01 – ЛУ

2020

|  |  |
| --- | --- |
| **УТВЕРЖДЕН** |  |
| 58.29.29-001-29233469-2020 13 01 – ЛУ |  |

**Сиcтема контроля прав доступа**

**«Матрица доступа»**

**Описание программы**

58.29.29-001-29233469-2020 13 01

На 35 листах

2020

АННОТАЦИЯ

В данном программном документе приведено описание программного средства контроля (анализа) защищенности информации «Система контроля прав доступа «Матрица доступа»», децимальный номер 58.29.29-001-29233469-2020, (далее – Система).

В разделе «Общие сведения» приведено краткое описание возможностей ПО Системы.

В разделе «Функциональное назначение» приведено описание назначения ПО Системы и ограничения, накладываемые на область применения ПО Системы.

В разделе «Описание логической структуры» приведены алгоритмы и методы работы, описание структуры ПО Системы и связи с другими системами.

В разделе «Используемые технические средства» указаны минимальные требования к аппаратному и программному обеспечениям.

В разделе «Вызов и загрузка» представлен способ вызова компонентов ПО Системы.

В разделах «Входные данные» и «Выходные данные» указаны сведения о входных и выходных данных.

В разделе «Перечень терминов» приведены объяснения терминов, используемых в документе.

В разделе «Перечень сокращений» приведены расшифровки сокращений, используемых в документе.

СОДЕРЖАНИЕ

[1. Общие сведения 6](#_Toc53048043)

[1.1. Обозначение и наименование 6](#_Toc53048044)

[1.2. Программное обеспечение, необходимое для функционирования Системы 6](#_Toc53048045)

[1.3. Языки программирования, на которых написано ПО Системы 6](#_Toc53048046)

[1.4. Требования и условия технического характера 7](#_Toc53048047)

[1.5. Требования и условия технологического характера 7](#_Toc53048048)

[2. Функциональное назначение 8](#_Toc53048049)

[2.1. Назначение Системы 8](#_Toc53048050)

[2.2. Сведения о функциональных ограничениях на применение 9](#_Toc53048051)

[3. Описание логической структуры 10](#_Toc53048052)

[3.1. Структура Системы с описанием функций составных частей и связи между ними 10](#_Toc53048053)

[3.2. Алгоритм функционирования Системы 11](#_Toc53048054)

[3.3. Используемые методы 12](#_Toc53048055)

[3.3.1. Субъекты доступа 12](#_Toc53048056)

[3.3.2. Объекты доступа 12](#_Toc53048057)

[3.3.3. Управление идентификаторами субъектов доступа Системы 13](#_Toc53048059)

[3.3.4. Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory 17](#_Toc53048060)

[3.3.5. Контроль реализации правил разграничения доступом 18](#_Toc53048061)

[3.3.6. Контроль реализации полномочий пользователей 19](#_Toc53048062)

[3.4. Связь файлов исходных текстов и функций безопасности, реализуемых Системой 21](#_Toc53048063)

[3.5. Связи Системы с другими программами 28](#_Toc53048064)

[4. Используемые технические средства 29](#_Toc53048065)

[4.1. Требования технического и техноллогического характера при выполнении компиляции Системы 29](#_Toc53048066)

[4.2. Последовательность действий при выполнении компиляции 29](#_Toc53048067)

[4.3. Требования к программному и аппаратному обеспечению, необходимому для работы Системы 30](#_Toc53048068)

[5. Вызов и загрузка 32](#_Toc53048069)

[5.1. База данных 32](#_Toc53048070)

[5.2. Веб-модуль 32](#_Toc53048071)

[5.3. АРМ пользователей 32](#_Toc53048072)

[6. Входные данные 33](#_Toc53048073)

[7. Выходные данные 34](#_Toc53048074)

[Перечень терминов 35](#_Toc53048075)

[Перечень сокращений 36](#_Toc53048076)

# Общие сведения

## Обозначение и наименование

В данном документе приведено описание изделия «Система контроля прав доступа «Матрица доступа»», децимальный номер 58.29.29-001-29233469-2020 (далее – Система).

Обозначение изделия в программной документации и заказе – Система контроля прав доступа «Матрица доступа».

Контрольные суммы файлов дистрибутива и неизменных файлов, установленного ПО Системы рассчитаны по алгоритму «Уровень-2, программно» с использованием программного средства «ФИКС» (версия 2.0.2) (сертификат соответствия требованиям по безопасности информации № 1548, выдан ФСТЭК России 15 января 2008 года, действителен до 15 января 2020 года, срок технической поддержки до 15 января 2025 года) и представлены в формуляре.

## Программное обеспечение, необходимое для функционирования Системы

Система предназначена для функционирования на серверах под управлением ОС MS Windows Server. Если используется английская версия ОС, то перед установкой продукта необходимо настроить поддержку русского языка в настройках «Языки и стандарты» («Regional settings»).

Доступ с помощью веб-браузера Google Chrome (или любого другого на базе chromium: Яндекс.Браузер, Vivaldi и т.д.) в Систему осуществляется через Web-сервер. Для записи, чтения и хранения информации в структурированном виде Система взаимодействует с балансировщиком нагрузки PgBouncer, а он, в свою очередь, с СУБД Postgre SQL. Для хранения кэшей используется резидентная СУБД Redis.

## Языки программирования, на которых написано ПО Системы

Для написания Системы используются языки программирования Python (платформа Django), TypeScript (платформа Angular), SQL (СУБД PostgreSQL, Программные коннекторы), С# (Программные коннекторы).

## Требования и условия технического характера

Для работы Системы каких-либо особых требований и условий технического характера не предъявляется.

## Требования и условия технологического характера

Для работы Системы каких-либо особых требований и условий технологического характера не предъявляется.

# Функциональное назначение

## Назначение Системы

Система обеспечивает выполнение следующих функциональных требований:

* формирование актуальной матрицы текущих прав доступа пользователей в корпоративных информационных ресурсах;
* возможность контекстного поиска записей в сформированной матрице доступа по объектам или субъектам доступа;
* отображение текущих прав доступа для заданного пользователя корпоративного информационного ресурса;
* возможность сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона;
* сравнение сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений;
* ведение истории прав доступа.

Система предназначена для контроля реализации правил разграничения доступом и формирования актуальной матрицы прав доступа пользователей к корпоративным информационным ресурсам/системам (далее – Защищаемые системы), а также выявления произошедших изменений в правах доступа. Подключение Системы к защищаемым системам осуществляется посредством программных коннекторов с использованием встроенных механизмов (API-функции, процедуры и т.д.) данных систем. Реализация программных коннекторов не предполагает установки дополнительных программных компонентов на серверы защищаемых систем.

Система является программным средством контроля (анализа) защищенности информации, реализующим меру защиты информации «Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе» (АНЗ.5) в соответствии с требованиями документов «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (введены в действие приказом ФСТЭК России № 17 от 11.02.2013), «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (введены в действие приказом ФСТЭК России № 21 от 18.02.2013) и «Меры защиты информации в государственных информационных системах» (утверждены директором ФСТЭК России 11.02.2014), в части:

* контроль заведения и удаления учетных записей пользователей,
* контроль реализации правил разграничения доступом,
* контроль реализации полномочий пользователей.

## Сведения о функциональных ограничениях на применение

Функциональных ограничений на применение Системы не предусмотрено.

# Описание логической структуры

## Структура Системы с описанием функций составных частей и связи между ними

Система состоит из следующих компонентов:

* ПО «Система контроля прав доступа «Матрица доступа»»;
* СУБД;
* Программные коннекторы (первого и второго типа).

Назначение компонентов, составляющих ядро Системы, приведено в таблице ниже (Таблица 3.1).

**Таблица 3.1 − Назначение компонент**

| Компонент | Назначение |
| --- | --- |
| ПО «Система контроля прав доступа «Матрица доступа»» | Выполнение функций контроля реализации правил разграничения доступом, формирования матрицы прав доступа и предоставление интерфейсов взаимодействия (работа с Системой выполняется через веб-интерфейс) |
| СУБД | Хранение конфигурационных параметров Системы, сформированных версий матрицы доступа подключенных защищаемых систем |
| Программные коннекторы | Интеграция Системы с защищаемыми системами |

Управление Системой осуществляется с АРМ администратора посредством веб-консоли управления.

ПО, обеспечивающее выполнение функциональных возможностей Системы, устанавливается на сервер приложений. Программные коннекторы для подключения к защищаемым системам также устанавливаются на сервер приложений.

Хранение конфигурационных параметров Системы, а также хранение сформированных матриц текущих прав доступа для защищаемых систем осуществляется на сервере баз данных.

Сервер приложений и сервер СУБД могут быть развернуты на одном физическом, либо виртуальном сервере.

Общая схема архитектуры Системы представлена на рисунке ниже (Рис. 3.1).

**Структурная схема Системы**



Рис. 3.1

## Алгоритм функционирования Системы

Функционал Системы основан на следующем алгоритме:

* запуск задач синхронизации с контролируемыми информационными ресурсами;
* формирование эталонной матрицы прав доступа пользователей;
* выявление отличий от сформированной эталонной матрицы прав доступа пользователей, путем проведения периодических синхронизаций с защищаемыми информационными ресурсами, либо получением данных о новых правах доступа из журналов событий Windows;
* информирование пользователя Системы о выявленных отличиях от эталонной матрицы прав доступа;
* формирование новой эталонной матрицы прав доступа.

## Используемые методы

Система обеспечивает реализацию функции – меры защиты информации «Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе» (АНЗ.5) в части:

* контроль заведения и удаления учетных записей пользователей,
* контроль реализации правил разграничения доступом,
* контроль реализации полномочий пользователей.

### Субъекты доступа

В Системе в качестве субъектов доступа должны определяться пользователи и группы пользователей защищаемых систем.

Выделяют следующие роли пользователей:

* Администратор
  + - Таблица БД «core\_user\_groups»;
    - Функция работы с объектом администратор «is\_admin» (*файл \DiffApp\core\auth\permissions.py)*
* Контролер;
  + - Таблица БД «core\_user\_groups»;
    - Функция работы с объектом контролер «is\_admin\_or\_superuser\_or\_controller» (*файл \DiffApp\core\auth\permissions.py)*
* Оператор.
  + - Таблица в БД «core\_user\_groups»;
    - Функция работы с объектом оператор «has\_access\_to\_server» (*файл \DiffApp\core\auth\permissions.py* )

### Объекты доступа

В Системе в качестве объектов доступа идентифицируются:

* каталоги общего доступа (для файловых серверов на базе MS Windows);
  + - Таблица БД «ntfs\_ace»;
    - Класс работы с каталогами «NTFSClient» (*файл \DiffApp\clients\ntfs\client.py*).
* коллекция метаданных (для ИС «1С: Предприятие»);
  + - Таблица БД «ones\_ace»;
    - Класс работы с метаданными «OneSClient» (*файл DiffApp\clients\ones\client.py*);
* карточки, папки и справочники (для СЭД «Docsvision»);
  + - Таблица БД «dv\_ace»;
    - Класс работы с объектами «DocsVisionClient» (*файл DiffApp\clients\dv\clients\dvclient.py*).
* списки подсайтов, сайт коллекции и списки, доступные для каждого подсайта (для корпоративного портала на базе MS Sharepoint);
  + - Таблица БД «mssp\_ace»;
    - Класс работы с объектиами «SharePointClient» (*файл DiffApp\clients\mssp\client.py*).
* БД, таблицы, схемы и метаданные (для СУБД MS SQL Server).
  + - Таблица БД «mssql\_ace»;
    - Класс работы с объектиами «MsSqlClient» (*файл DiffApp\clients\mssql\client\client.py*)











### Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory

Система предоставляет возможность контроля заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory. Это обеспечивается реализацией следующих функциональных возможностей:

1. построение матрицы вхождения пользователей в группы безопасности службы каталогов MS Active Directory;
2. возможность контекстного поиска записей в сформированной матрице по пользователям и группам безопасности службы каталогов MS Active Directory;
3. возможность сохранения сформированной матрицы в качестве эталона;
4. сравнение сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений.

Привязка к исходным текстам\_\_\_\_\_

Алгоритм реализации функции построения матрицы вхождения пользователей в группы безопасности службы каталогов MS Active Directory представлен на блок-схеме (Рисунок 3.2).

Алгоритм реализации возможности контекстного поиска записей в сформированной матрице по пользователям и группам безопасности службы каталогов MS Active Directory представлен на блок-схеме (Рисунок 3.3).

Алгоритм реализации возможности сохранения сформированной матрицы в качестве эталона представлен на блок-схеме (Рисунок 3.4).

Алгоритм реализации функции сравнения сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений представлен на блок-схеме (Рисунок 3.5).

**Блок схема алгоритма реализации функции построения матрицы вхождения пользователей в группы безопасности службы каталогов MS Active Directory**

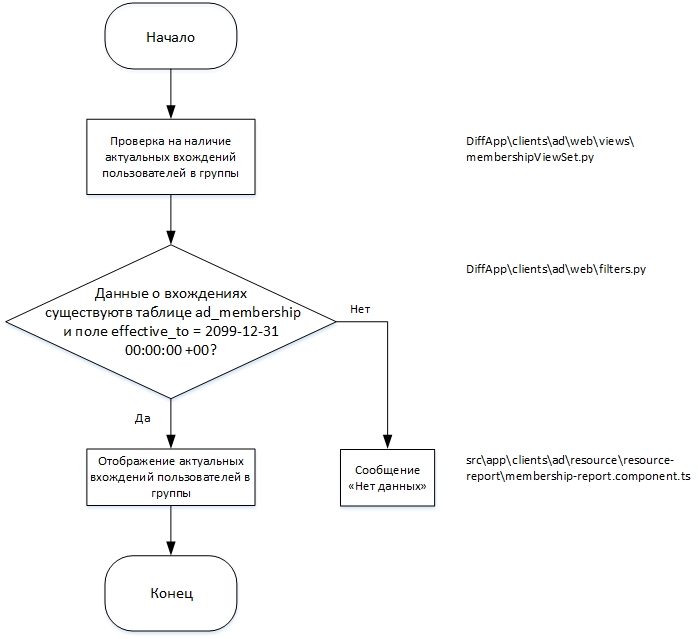


Рисунок 3.2

**Блок схема алгоритма реализации возможности контекстного поиска записей в сформированной матрице по пользователям и группам безопасности службы каталогов MS Active Directory**

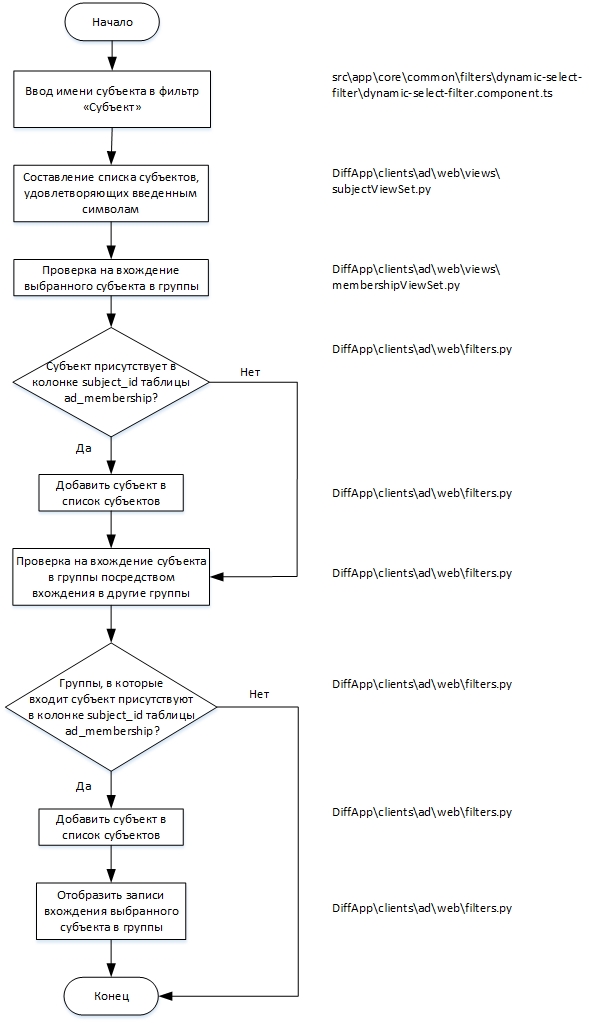
****

Рисунок 3.3

**Блок схема алгоритма реализации возможности сохранения сформированной матрицы в качестве эталона**

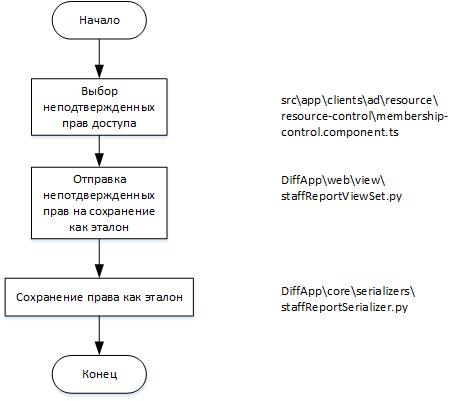


Рисунок 3.4

**Блок схема алгоритма реализации функции сравнения сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений**



Рисунок 3.5

### Контроль реализации правил разграничения доступом

Система предоставляет возможность контроля реализации правил разграничения доступом в защищаемой системе с дискреционной либо ролевой моделями управления доступом. Это обеспечивается посредством построения матрицы текущих прав доступа пользователей в защищаемой системе с дискреционной либо ролевой моделями управления доступом.

Привязка к исходным текстам\_\_\_\_\_

Алгоритм выполнения функции контроля реализации правил разграничения доступом представлен на блок-схемах Рисунок 3.6 - Рисунок 3.14.

**Блок схема алгоритма выполнения функции контроля реализации правил разграничения доступом. Файловый сервер.**

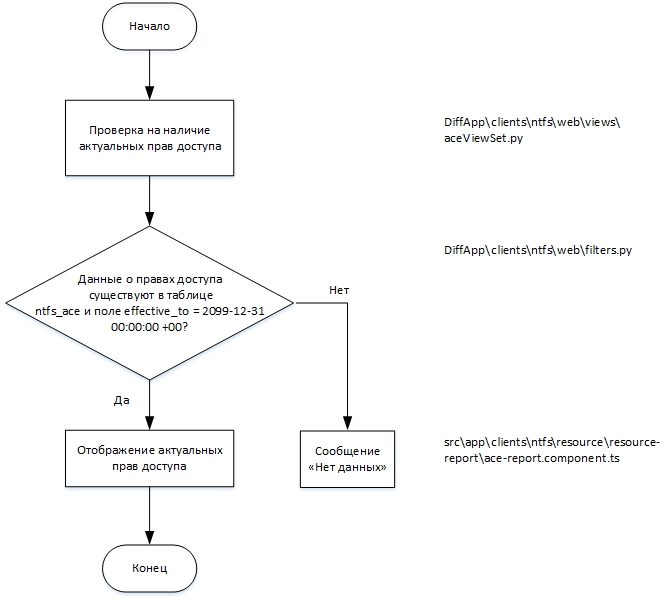


Рисунок 3.6

**Блок схема алгоритма выполнения функции контроля реализации правил разграничения доступом. 1С Предприятие (Дискреционная модель управления доступом).**

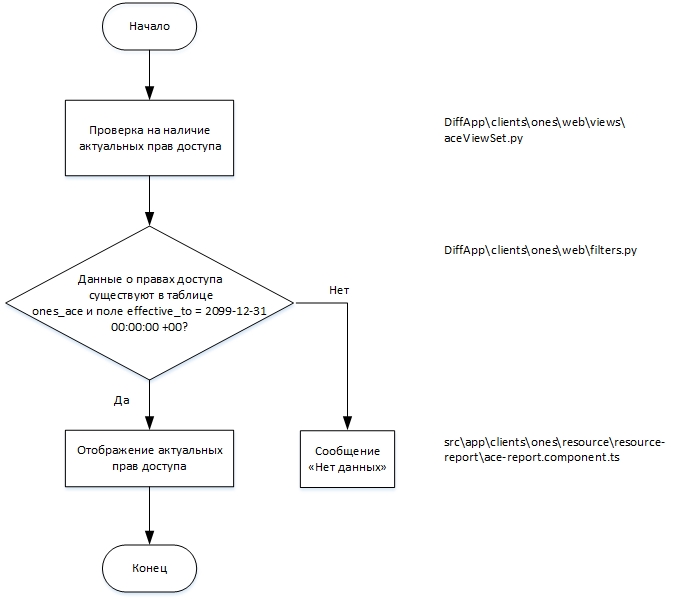


Рисунок 3.7

**Блок схема алгоритма выполнения функции контроля реализации правил разграничения доступом. 1С Предприятие (Ролевая модель управления доступом).**

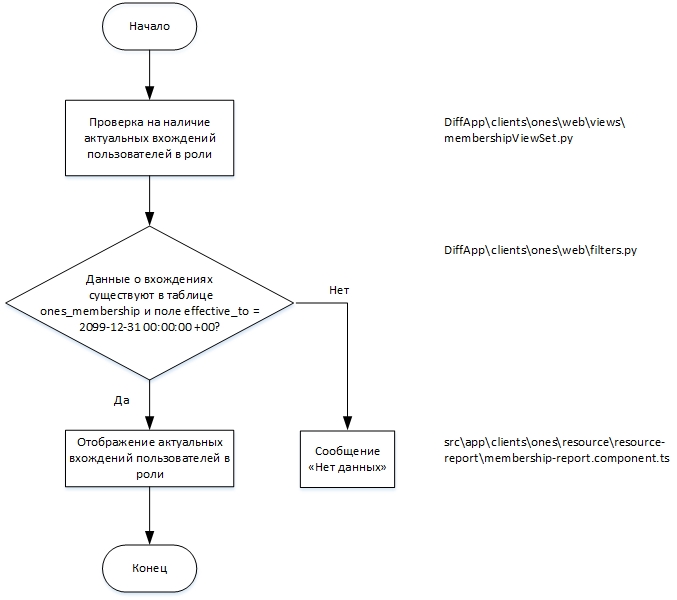


Рисунок 3.8

**Блок схема алгоритма выполнения функции контроля реализации правил разграничения доступом. СЭД Docsvision (Дискреционная модель управления доступом).**

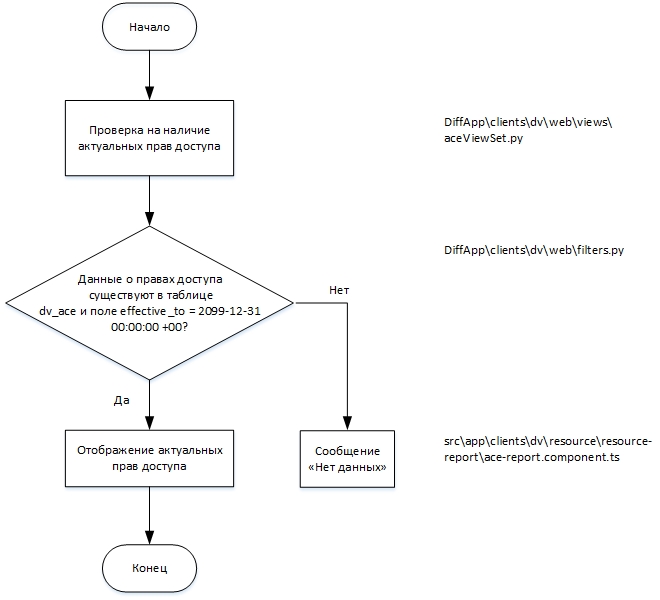


Рисунок 3.9

**Блок схема алгоритма выполнения функции контроля реализации правил разграничения доступом. СЭД Docsvision (Ролевая модель управления доступом).**

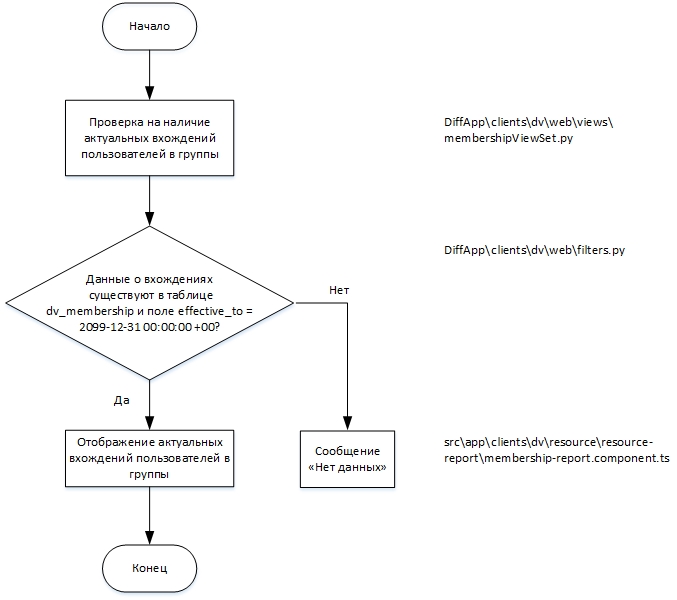


Рисунок 3.10

**Блок схема алгоритма выполнения функции контроля реализации правил разграничения доступом. MS Sharepoint (Дискреционная модель управления доступом).**

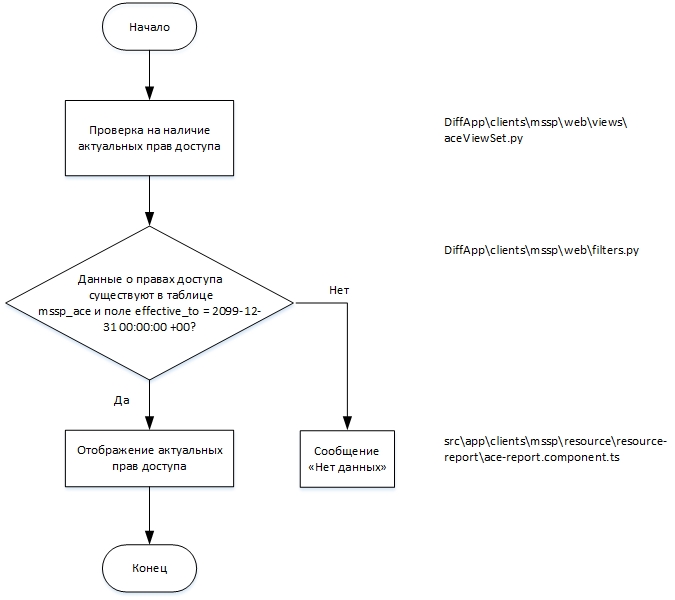


Рисунок 3.11

**Блок схема алгоритма выполнения функции контроля реализации правил разграничения доступом. MS Sharepoint (Ролевая модель управления доступом).**

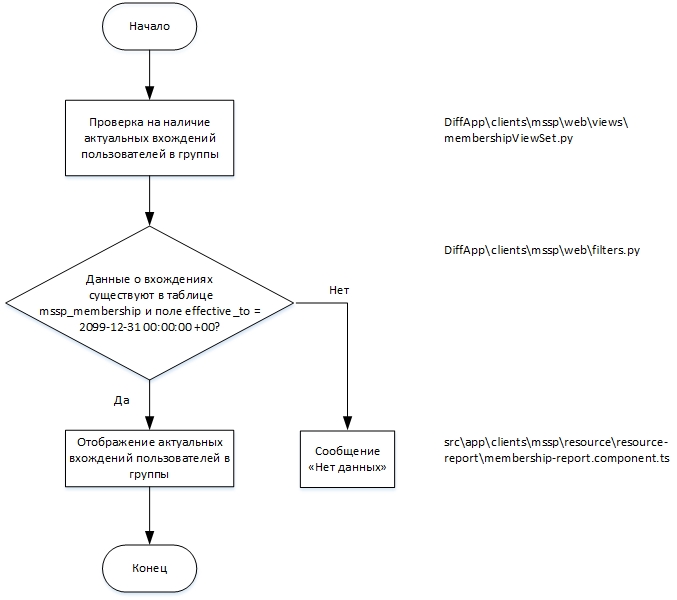


Рисунок 3.12

**Блок схема алгоритма выполнения функции контроля реализации правил разграничения доступом. MS SQL Server (На уровне БД)**

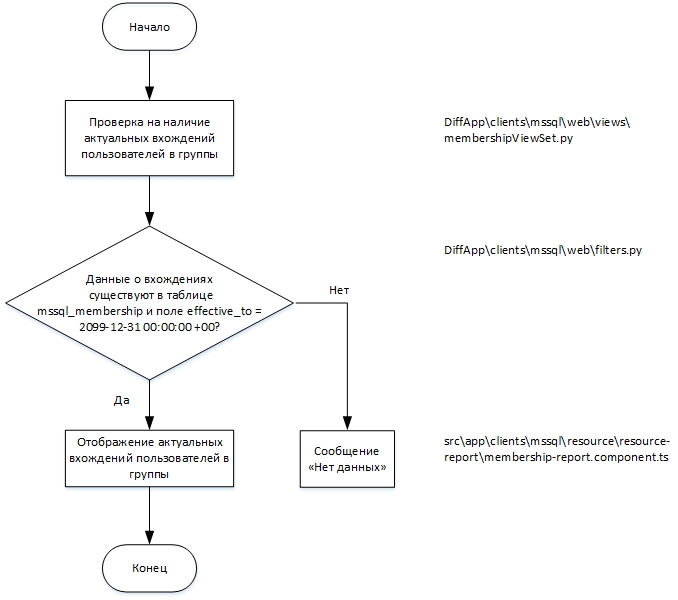


Рисунок 3.13

**Блок схема алгоритма выполнения функции контроля реализации правил разграничения доступом. MS SQL Server (На уровне сервера)**

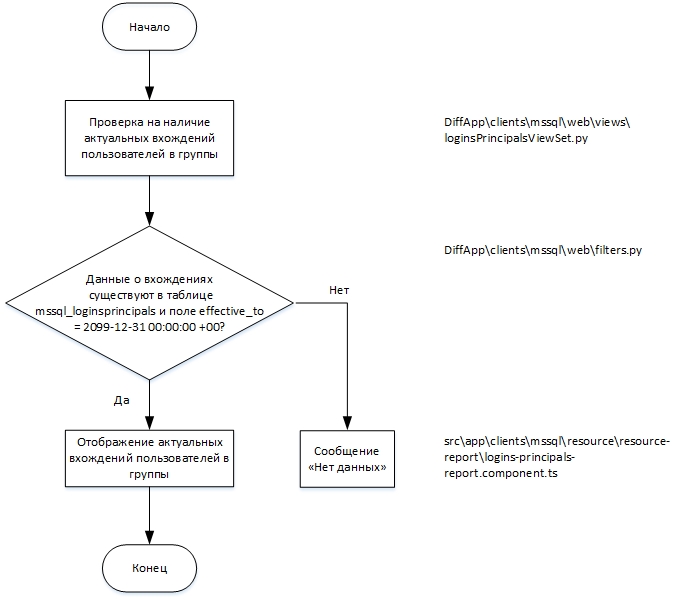


Рисунок 3.14

### Контроль реализации полномочий пользователей

Система предоставляет возможность контроля реализации полномочий пользователей в защищаемой системе. Это обеспечивается реализацией следующих функциональных возможностей:

1. возможность контекстного поиска записей в сформированной матрице доступа по объектам доступа защищаемой системы;
2. отображение текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом;
3. возможность сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона;
4. сравнение сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений;
5. ведение истории прав доступа.

Привязка к исходным текстам\_\_\_\_\_

Алгоритм реализации возможности контекстного поиска записей в сформированной матрице доступа по объектам доступа защищаемой системы представлен на блок-схемах Рисунок 3.15 - Рисунок 3.18.

Алгоритм реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом представлен на блок-схеме Рисунок 3.19 - Рисунок 3.27.

Алгоритм реализации функции сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона представлен на блок-схеме Рисунок 3.28 - Рисунок 3.32

Алгоритм реализации функции сравнения сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений представлен на блок-схеме Рисунок 3.33 - Рисунок 3.37.

Алгоритм реализации функции ведения истории прав доступа представлен на блок-схеме Рисунок 3.38 - Рисунок 3.42.

**Блок схема алгоритма реализации возможности контекстного поиска записей в сформированной матрице доступа по объектам доступа защищаемой системы.**

**Файловый сервер.**

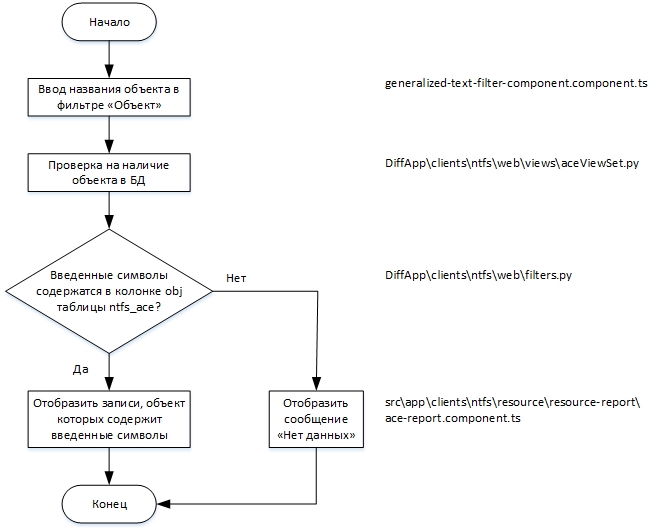
Рисунок 3.18

Рисунок 3.15

**Блок схема алгоритма реализации возможности контекстного поиска записей в сформированной матрице доступа по объектам доступа защищаемой системы.**

**1С Предприятие.**

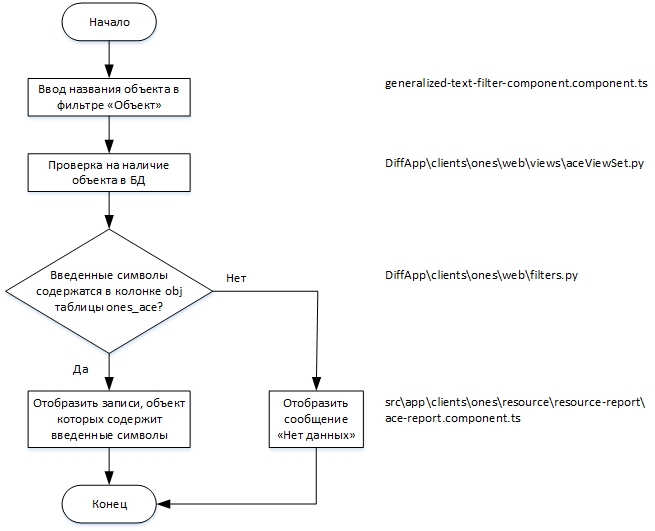


Рисунок 3.16

**Блок схема алгоритма реализации возможности контекстного поиска записей в сформированной матрице доступа по объектам доступа защищаемой системы.**

**СЭД Docsvision.**

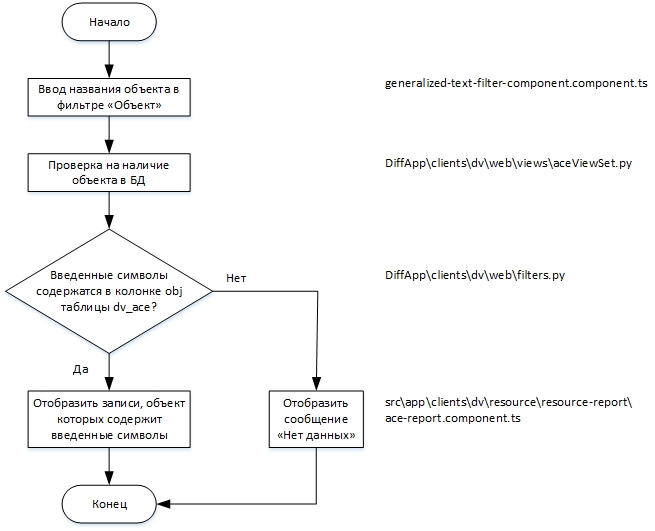
****

Рисунок 3.17

**Блок схема алгоритма реализации возможности контекстного поиска записей в сформированной матрице доступа по объектам доступа защищаемой системы.**

**MS Sharepoint.**

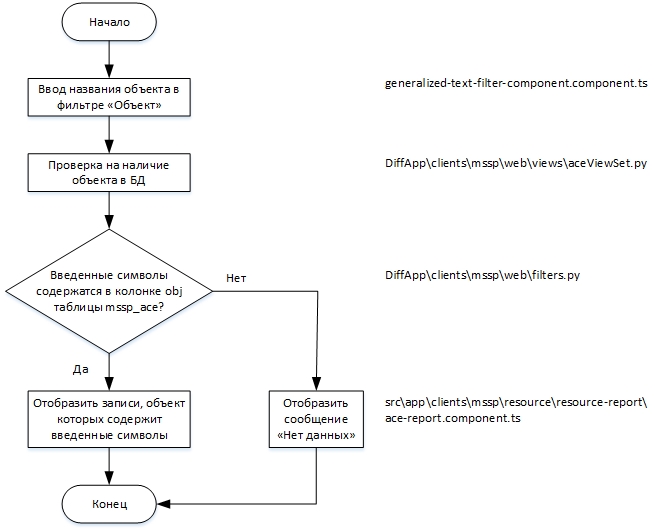
****

Рисунок 3.18

**Блок схема алгоритма реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом. Файловый сервер.**

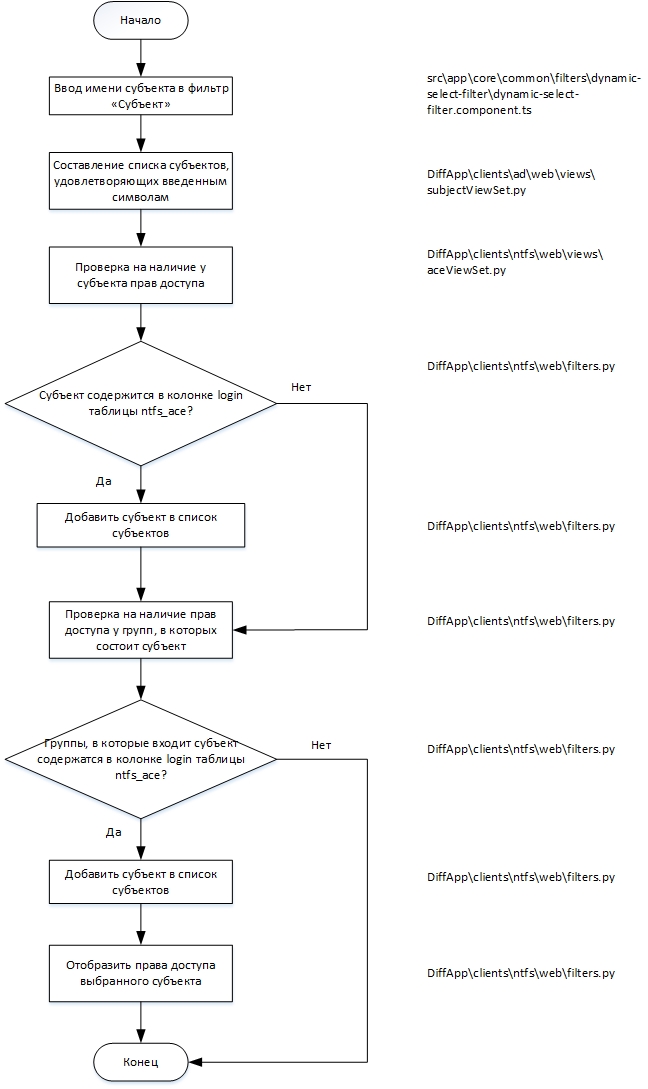
****

Рисунок 3.19

**Блок схема алгоритма реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом. 1C Предприятие (Дискреционная модель управления)**

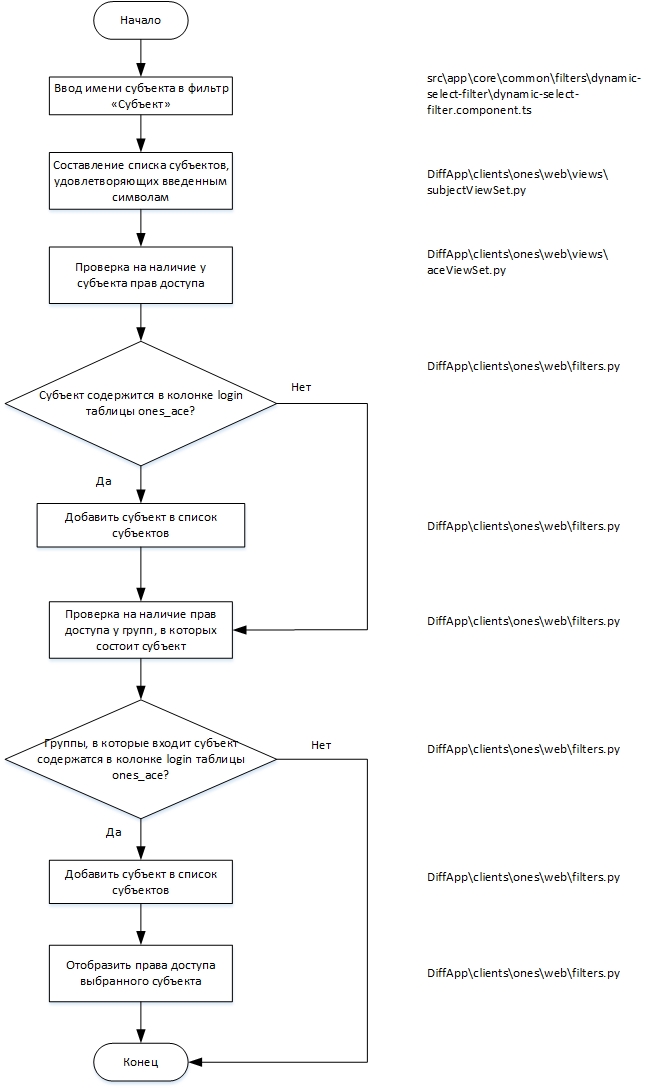
****

Рисунок 3.20

**Блок схема алгоритма реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом. 1C Предприятие (Ролевая модель управления)**

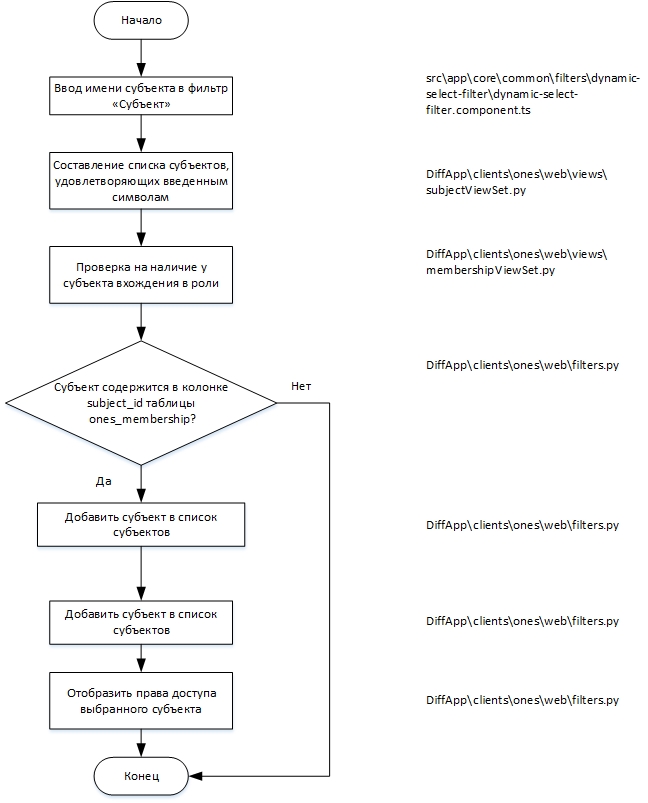


Рисунок 3.21

**Блок схема алгоритма реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом. СЭД Docsvision (Дискреционная модель управления)**

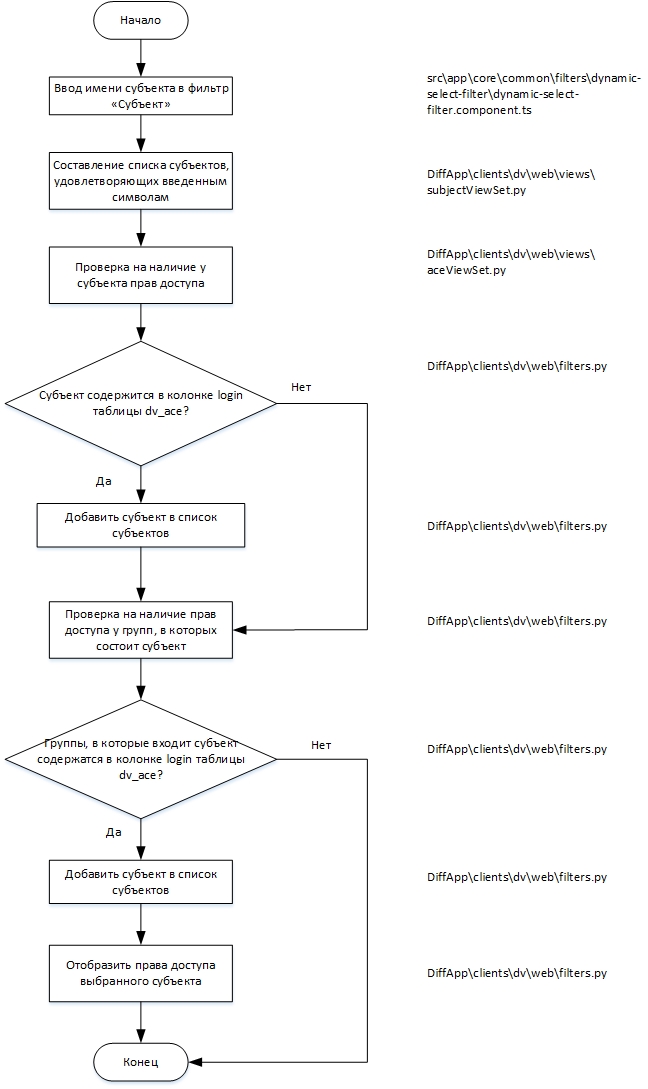


Рисунок 3.22

**Блок схема алгоритма реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом. СЭД Docsvision (Ролевая модель управления)**

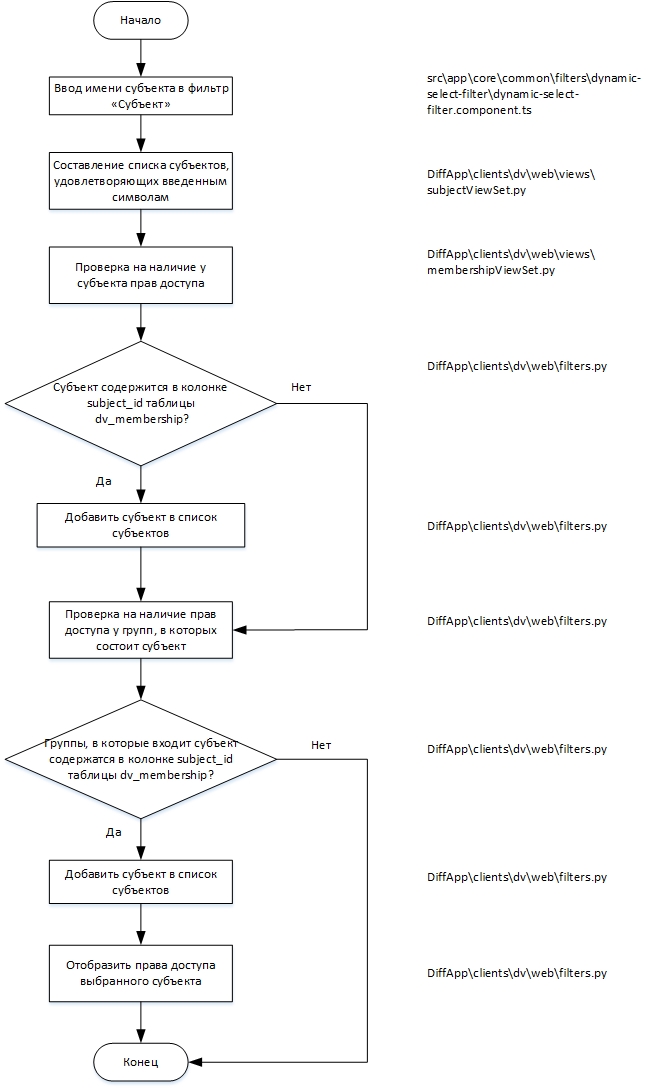


Рисунок 3.23

**Блок схема алгоритма реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом. MS Sharepoint (Дискреционная модель управления)**

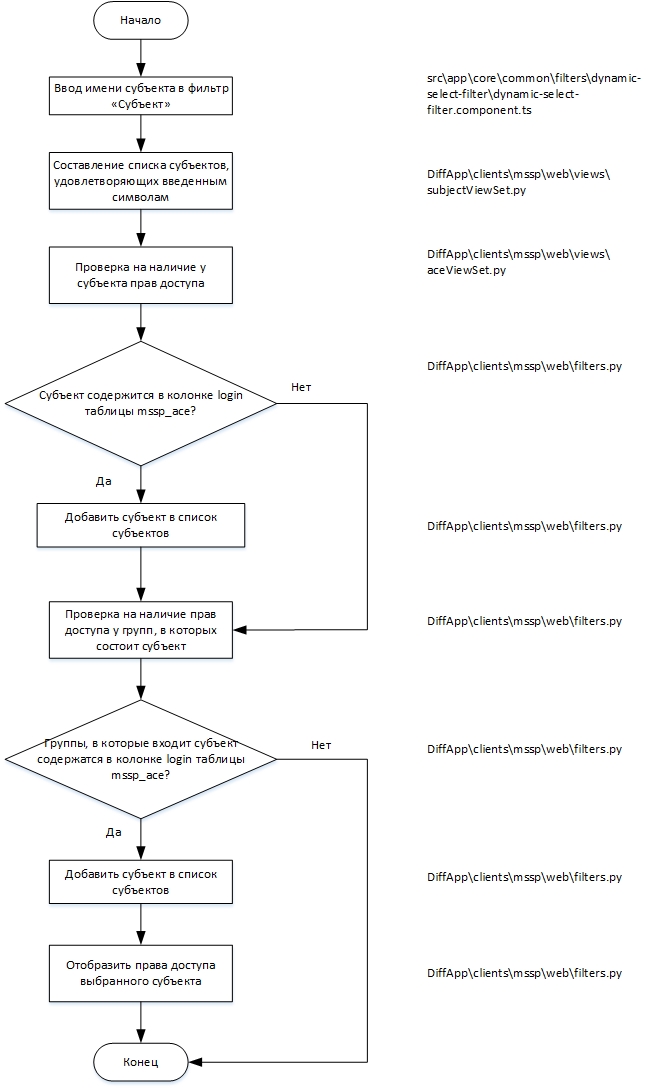


Рисунок 3.24

**Блок схема алгоритма реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом. MS Sharepoint (Ролевая модель управления)**

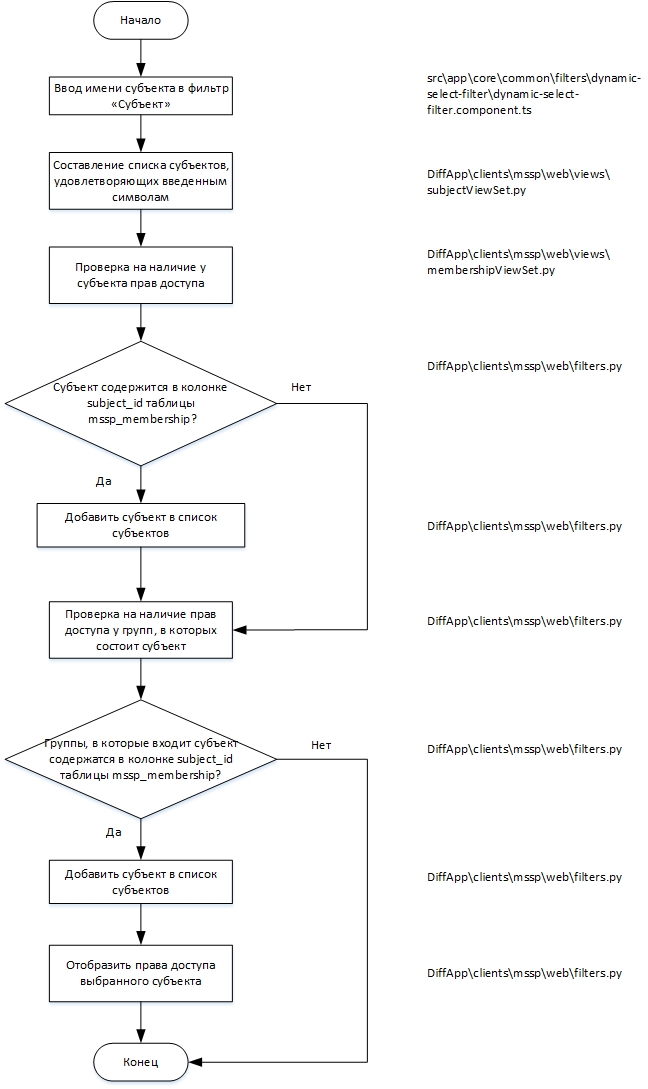


Рисунок 3.25

**Блок схема алгоритма реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом. MS SQL Server (На уровне БД)**

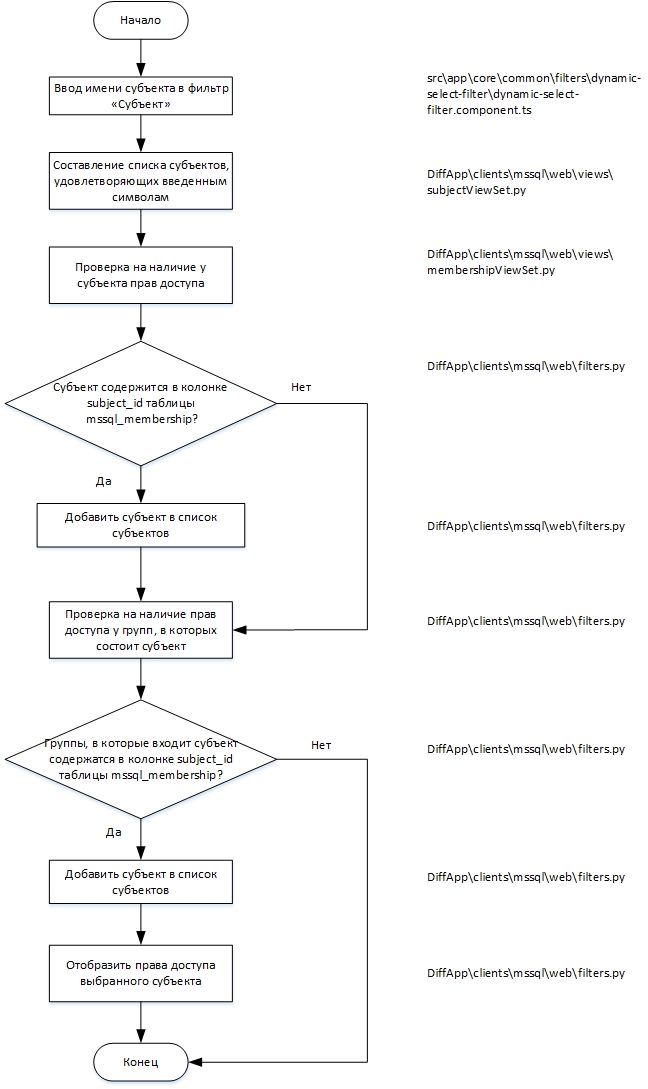


Рисунок 3.26

**Блок схема алгоритма реализации функции отображения текущих прав доступа для заданного пользователя защищаемой системы с дискреционной либо ролевой моделями управления доступом. MS SQL Server (На уровне сервера)**

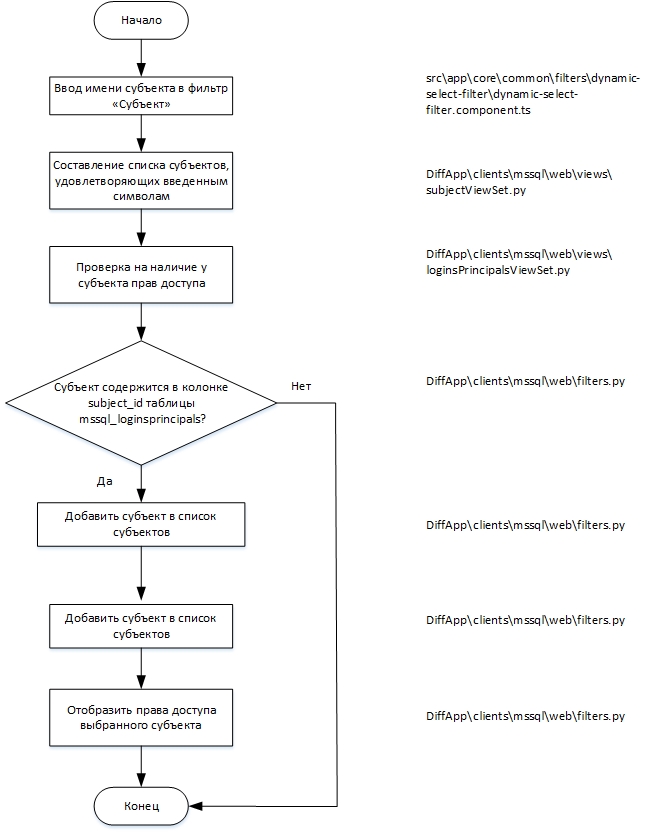


Рисунок 3.27

**Блок схема алгоритма реализации функции сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона. Файловый сервер.**

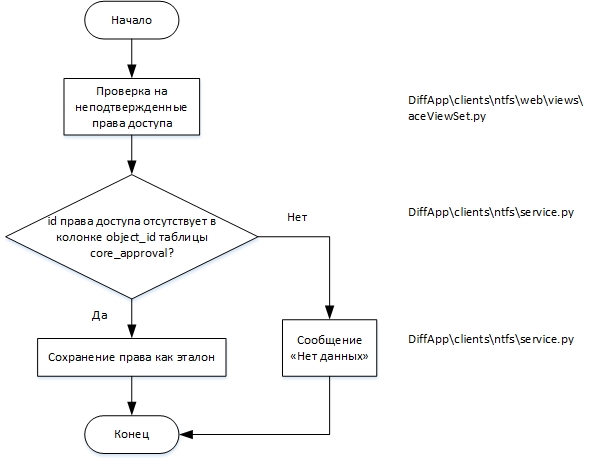
****

Рисунок 3.28

**Блок схема алгоритма реализации функции сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона. 1С Предприятие.**

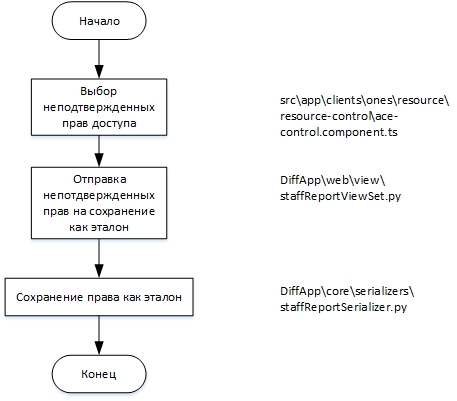
****

Рисунок 3.29

**Блок схема алгоритма реализации функции сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона. СЭД Docsvision.**

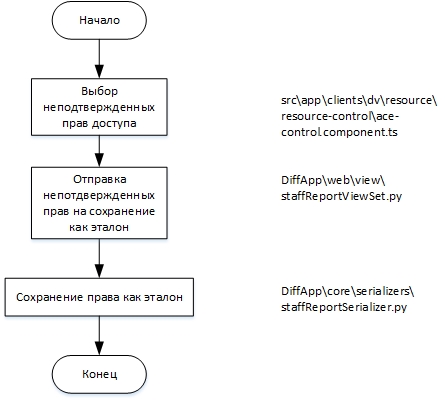


Рисунок 3.30

**Блок схема алгоритма реализации функции сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона. MS Sharepoint.**

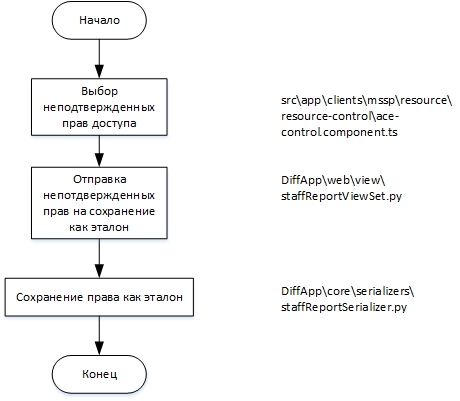


Рисунок 3.31

**Блок схема алгоритма реализации функции сохранения сформированной матрицы текущих прав доступа пользователей в качестве эталона. MS SQL Server.**

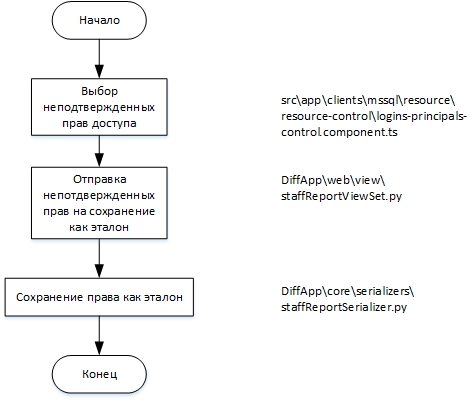


Рисунок 3.32

**Блок схема алгоритма реализации функции сравнения сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений. Файловый сервер.**

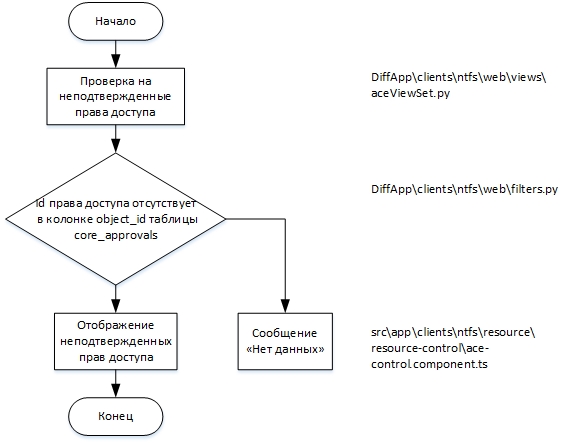
****

Рисунок 3.33

**Блок схема алгоритма реализации функции сравнения сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений. 1С Предприятие.**

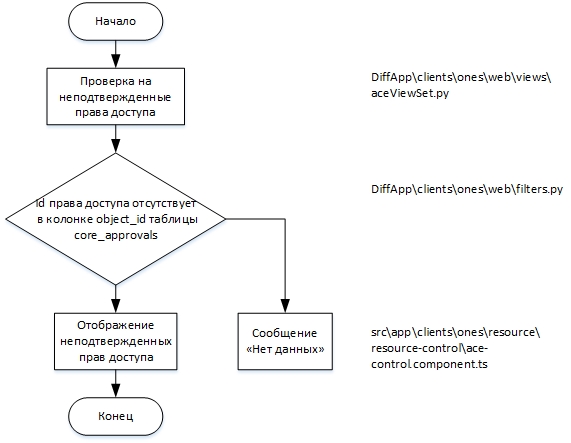


Рисунок 3.34

**Блок схема алгоритма реализации функции сравнения сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений. СЭД Docsvision.**

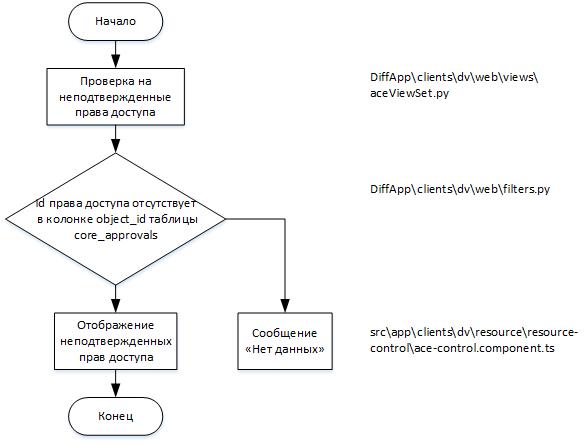


Рисунок 3.35

**Блок схема алгоритма реализации функции сравнения сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений. MS Sharepoint.**

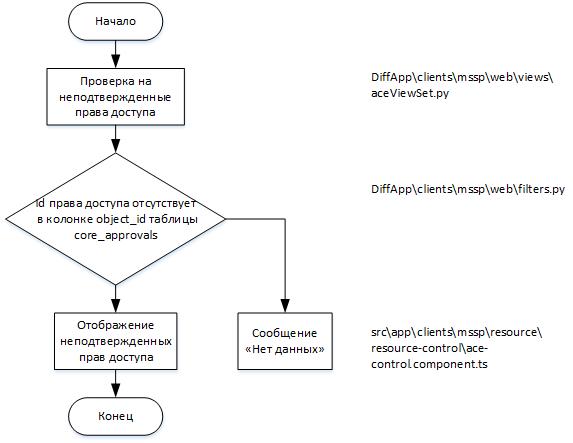


Рисунок 3.36

**Блок схема алгоритма реализации функции сравнения сформированной матрицы текущих прав доступа пользователей защищаемой системы с эталоном и отображение выявленных изменений. MS SQL Server.**

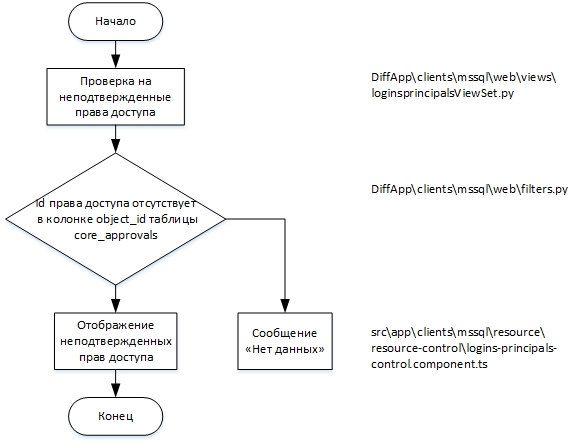


Рисунок 3.37

**Блок схема алгоритма реализации функции ведения истории прав доступа.**

**Файловый сервер.**

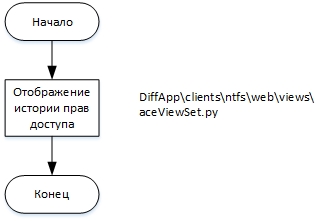
****

Рисунок 3.38

**Блок схема алгоритма реализации функции ведения истории прав доступа.**

**1С Предприятие.**

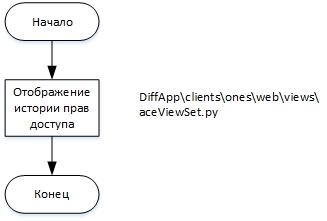
****

Рисунок 3.39

**Блок схема алгоритма реализации функции ведения истории прав доступа.**

**СЭД Docsvision.**

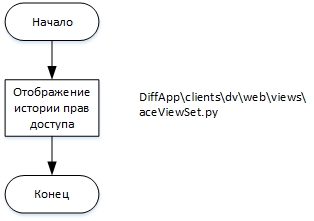
****

Рисунок 3.40

**Блок схема алгоритма реализации функции ведения истории прав доступа.**

**MS Sharepoint.**

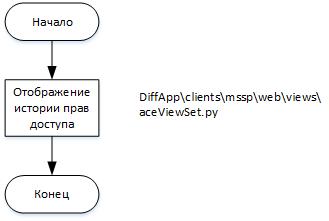
****

Рисунок 3.41

**Блок схема алгоритма реализации функции ведения истории прав доступа.**

**MS SQL Server.**

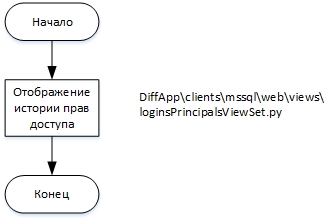
****

Рисунок 3.42

## Связь файлов исходных текстов и функций безопасности, реализуемых Системой

Описание назначения файлов исходных текстов и их связь с функциями безопасности Системы представлен в таблице ниже.

**Назначение файлов исходных текстов**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п/п** | **Наименование файла исходного текста** | **Назначение файла исходного текста** | **Функция безопасности, реализуемая в файле исходного текста** |
|  | DiffApp\clients\ad\web\views\membershipViewSet.py | Класс отображения списка вхождения субъектов в группы MS Active Directory | Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory |
|  | DiffApp\clients\ad\web\filters.py | Класс фильтра по объектам MS Active Directory | Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory |
|  | src\app\clients\ad\resource\resource-report\membership-report.component.ts | Класс отображения отчета по актуальным вхождениям субъектов в группы MS Active Directory | Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory |
|  | src\app\core\common\filters\dynamic-select-filter\dynamic-select-filter.component.ts | Класс динамического фильтра по субъектам MS Active Directoru | 1. Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\ad\web\views\subjectViewSet.py | Класс отображения списка субъектов MS Active Directory | Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory |
|  | src\app\clients\ad\resource\resource-control\membership-control.component.ts | Класс отображения отчета по отличиям вхождений субъектов в группы MS Active Directory относительно эталона. | Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory |
|  | DiffApp\web\view\staffReportViewSet.py | Класс отображения списка подтверждений прав доступа | 1. Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory 2. Контроль реализации полномочий пользователей |
|  | DiffApp\core\serializers\staffReportSerializer.py | Класс-сериализатор объектов подтверждения | 1. Контроль заведения и удаления учетных записей пользователей в защищаемой системе – службе каталогов MS Active Directory 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\ones\web\views\membershipViewSet.py | Класс отображения списка вхождения субъектов в роли 1С Предприятие | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\ones\web\filters.py | Класс фильтра по объектам 1С Предприятие. | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | src\app\clients\ones\resource\resource-report\membership-report.component.ts | Класс отображения отчета по актуальным вхождениям субъектов в роли 1С Предприятие | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\ones\web\views\aceViewSet. | Класс отображения списка прав доступа 1С Предприятие | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | src\app\clients\ones\resource\resource-report\ace-report.component.ts | Класс отображения отчета по актуальным правам доступа 1С Предприятие | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\dv\web\views\aceViewSet.py | Класс отображения списка прав доступа СЭД Docsvision | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\dv\web\filters.py | Класс фильтра по объектам СЭД Docsvision. | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | src\app\clients\dv\resource\resource-report\ace-report.component.ts | Класс отображения отчета по актуальным правам доступа СЭД Docsvision | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\dv\web\views\membershipViewSet.py | Класс отображения списка вхождения субъектов в группы СЭД Docsvision | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | src\app\clients\dv\resource\resource-report\membership-report.component.ts | Класс отображения отчета по актуальным вхождениям субъектов в группы СЭД Docsvision | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\mssp\web\views\aceViewSet.py | Класс отображения списка прав доступа MS Sharepoint | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\mssp\web\filters.py | Класс фильтра по объектам MS Sharepoint. | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | src\app\clients\mssp\resource\resource-report\ace-report.component.ts | Класс отображения отчета по актуальным правам доступа MS Sharepoint | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\mssp\web\views\membershipViewSet.py | Класс отображения списка вхождения субъектов в группы MS Sharepoint | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | src\app\clients\mssp\resource\resource-report\membership-report.component.ts | Класс отображения отчета по актуальным вхождениям субъектов в группы MS Sharepoint | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\mssql\web\views\loginsPrincipalsViewSet.py | Класс отображения списка вхождения субъектов в группы MS SQL Server на уровне сервера | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\mssql\web\filters.py | Класс фильтра по объектам MS SQL Server | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | src\app\clients\mssql\resource\resource-report\logins-principals-report.component.ts | Класс отображения отчета по актуальным вхождениям субъектов в группы MS SQL Server на уровне сервера | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\mssql\web\views\membershipViewSet.py | Класс отображения списка вхождения субъектов в группы MS SQL Server на уровне БД | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | src\app\clients\mssql\resource\resource-report\membership-report.component.ts | Класс отображения отчета по актуальным вхождениям субъектов в группы MS SQL Server на уровне БД | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\ntfs\web\views\aceViewSet.py | Класс отображения списка прав доступа Файлового сервера | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | DiffApp\clients\ntfs\web\filters.py | Класс фильтра по объектам Файлового сервера | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | src\app\clients\ntfs\resource\resource-report\ace-report.component.ts | Класс отображения отчета по актуальным правам доступа Файлового сервера | 1. Контроль реализации правил разграничения доступом 2. Контроль реализации полномочий пользователей |
|  | generalized-text-filter-component.component.ts | Общий класс текстового фильтра | Контроль реализации полномочий пользователей |
|  | DiffApp\clients\ones\web\views\subjectViewSet.py | Класс отображения списка субъектов 1С Предприятие | Контроль реализации полномочий пользователей |
|  | DiffApp\clients\dv\web\views\subjectViewSet.py | Класс отображения списка субъектов СЭД Docsvision | Контроль реализации полномочий пользователей |
|  | DiffApp\clients\mssp\web\views\subjectViewSet.py | Класс отображения списка субъектов MS Sharepoint | Контроль реализации полномочий пользователей |
|  | DiffApp\clients\mssql\web\views\subjectViewSet.py | Класс отображения списка субъектов MS SQL Server | Контроль реализации полномочий пользователей |
|  | src\app\clients\ones\resource\resource-control\ace-control.component.ts | Класс отображения отчета по отличиям прав доступа 1С Предприятие относительно эталона. | Контроль реализации полномочий пользователей |
|  | src\app\clients\dv\resource\resource-control\ace-control.component.ts | Класс отображения отчета по отличиям прав доступа СЭД Docsvision относительно эталона. | Контроль реализации полномочий пользователей |
|  | src\app\clients\mssp\resource\resource-control\ace-control.component.ts | Класс отображения отчета по отличиям прав доступа MS Sharepoint относительно эталона. | Контроль реализации полномочий пользователей |
|  | src\app\clients\mssql\resource\resource-control\logins-principals-control.component.ts | Класс отображения отчета по отличиям вхождений субъектов в группы MS SQL Server на уровне сервера относительно эталона. | Контроль реализации полномочий пользователей |
|  | src\app\clients\ntfs\resource\resource-control\ace-control.component.ts | Класс отображения отчета по отличиям прав доступа Файлового сервера относительно эталона. | Контроль реализации полномочий пользователей |

## Связи Системы с другими программами

Система при функционировании взаимодействует со средствами операционной системы и СУБД. Доступ к Системе осуществляется посредством интернет-браузера.

Система посредством программных коннекторов интегрируется со следующими корпоративными информационными ресурсами:

* файловые сервера на базе MS Windows;
* ИС «1С: Предприятие»;
* служба каталогов MS Active Directory;
* СЭД «Docsvision»;
* корпоративный портал на базе MS Sharepoint;
* СУБД MS SQL Server.

# Используемые технические средства

## Требования технического и техноллогического характера при выполнении разработки и сборки Системы

При разработке Системы для разработки ее ПО используется среда разработки PyCharm (Professional Edition).

Среда разработки PyCharm – это интегрированная среда разработки для языка программирования Python. Предоставляет средства для анализа кода, графический отладчик, инструмент для запуска юнит-тестов и поддерживает веб-разработку на Django. PyCharm разработана компанией JetBrains на основе среды разработки IntelliJ IDEA.

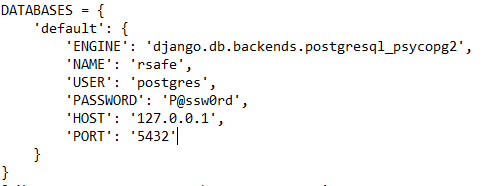
Основными требованиями при выполнении сборки дистрибутива программного обеспечения (далее – ПО) Системы являются следующие:

* наименование и версия операционной системы – операционная система Windows 8 и выше;
* ПО Inno Setup 5;
* ПО NodeJS версии 10.16.3;
* ПО Python версии 3.8.2.

Иные требования при выполнении компиляции файлов исходных текстов ПО Системы не предъявляются.

## Алгоритм подготовки испытательного стенда

1. Поместить все папки с исходными текстами в локальное хранилище;
2. Установить ПО NodeJS версии 10.16.3;
3. Установить Python версии 3.8.2;
4. Установить зависимости Python
   1. Перейти в папку diff-2.2.2.1302.release
   2. Установить зависимости путем выполнения команды: *python -m pip install -r requirements.txt --find-links thirdparty\python\wheels*
5. Установить зависимости rsafe-front
   1. Установить webdriver-manager, выполнив команду: *npm install webdriver-manager*;
   2. Установить зависимости nz-common, выполнив команду *npm install nz-common-1.2.85.tgz*;
   3. Установить зависимости rsafe-material-icons, выполнив команду *npm install rsafe-material-icons-0.0.5.tgz*;
   4. Установить зависимость material-bootstrap, выполнив *команду npm install bootstrap-material-design-4.0.2.tgz*;
   5. Установить остальные зависимости, выполнив команду *npm install*.
6. Запустить Redis
   1. Перейти в папку *diff-2.2.2.1302.release\thirdparty\redis*  и распаковать архив *Redis-x64-2.8.2104*;
   2. Запустить исполняемый файл *Redis-x64-2.8.2104\redis-server*.
7. Установить СУБД PostgreSQL 10 версии и создать базу данных, используя команду CREATE DATABASE rsafe, где rsafe – имя базы данных;
8. Создать переменные окружения со следующими значениями:
   1. DJANGO\_SETTINGS\_MODULE=Diff.settings.dev;
   2. RSAFE\_BACKEND=<Путь до исходных текстов>\diff-2.2.2.1302.release;
   3. SUPPORT\_MAIL= info@innostage-group.ru;
   4. SUPPORT\_PHONE=+7 (843) 567-42-90;
   5. PATH+=C:\Program Files (x86)\Inno Setup 5;
   6. RIGEL\_PATH= <Путь до исходных текстов>\rigel-2.2.2.1302.release;
   7. NPM\_HOME=%PROGRAMFILES%\nodejs\
   8. REMOTE\_USER=administrator
9. Скорректировать файл настроек <Путь до исходных текстов>\diff-2.2.2.1302.release\Diff\settings\dev.py
   1. Внести параметры подключения к БД DATABASES, пример:



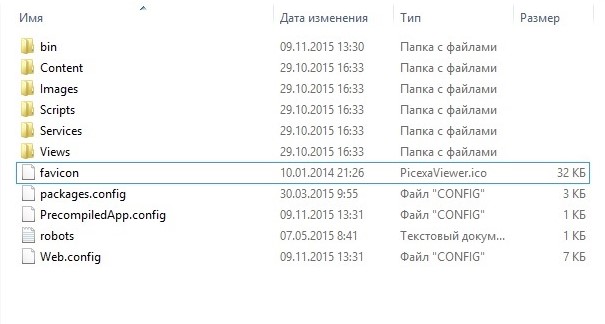
Где NAME – имя базы данных, USER – имя пользователя БД, PASSWORD – пароль пользователя БД, HOST – адрес сервера, на котором развернута СУБД, PORT – порт подключения.

1. Установить миграции
   1. Перейти в папку <Путь до исходных текстов>\diff-2.2.2.1302.release;\
   2. Используя командную строку выполнить команду *python manage.py migrate*;
2. Запустить backend сервер командой *python manage.py runserver --noreload <Имя сервера>:8000*
3. Запустить frontend сервер
   1. Перейти в папку <Путь до исходных текстов>\rsafe-front-2.2.2.1302.release
   2. Выполнить команду npm start
4. Система будет доступна по адресу http://<Имя сервера>:8001

## Последовательность действий при выполнении сборки дистрибутива

1. Открыть файл < Путь до исходных текстов >\diff-2.2.2.1302.release\setup.py
   1. Заменить значение переменной REMOTE\_FOLDER на актуальный путь до директории BuildNumberFile (пример: REMOTE\_FOLDER = r'C:\tmp\BuildNumberFile');
   2. Земенить значение переменной BUILD\_LOG\_PLACE на актуальный путь до папки Log (пример: BUILD\_LOG\_PLACE = r'C:\tmp\Log')
2. Перейти в директорию < Путь до исходных текстов >\diff-2.2.2.1302.release
3. Выполнить команду *python setup.py dist\_kit -p -i -d <Директория, в которую будет сохранен дистрибутив>*

**Файлы дистрибутива ПО Системы**



**Рис.1.**

## Требования к программному и аппаратному обеспечению, необходимому для работы Системы

Перечень аппаратных и программных средств, необходимых для корректной работы компонентов Системы, представлен в таблице ниже (Таблица 4.1).

Таблица 4.1 - Требования к аппаратным и программным средствам

| **Компонент** | **Требования к аппаратной части** | **Требования к программной части** |
| --- | --- | --- |
| **1** | **2** | **3** |
| ПО «Система контроля прав доступа «Матрица доступа»» и СУБД | * процессор: 2 или более ядер с частотой 2.4 ГГц; * оперативная память: 8 ГБ;   свободное дисковое пространство: не менее 150 ГБ | 1. Операционная система:  * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2012 Standard * Windows Server 2012 R2 Standard * Windows Server 2016 Standard * Windows Server 2019 Standard  1. Python версии 3.8.1; 2. Веб сервер Apache HTTP Server версии 2.4 3. СУБД PostgreSQL версии 10.3-2 4. Распространяемый пакет Visual C++ для Visual Studio 2013 5. Распространяемый пакет Visual C++ для Visual Studio 2017 |

# Вызов и загрузка

Способ вызова компонентов Системы представлен ниже.

## База данных

В процессе загрузки ОС выполняется автоматический запуск служб экземпляра БД, балансировщика нагрузки PgBouncer и брокера сообщений Redis.

## Веб-модуль

В процессе загрузки ОС выполняется автоматический запуск службы экземпляра веб-сервера Apache.

## АРМ пользователей

Запуск можно осуществить после полной загрузки используемой ОС, после запуска драйверов сетевой платы и стандартных сетевых служб ОС. Для работы в Системе выполняется запуск веб–браузера, в адресную строку вводится путь страницы.

# Входные данные

Входными данными Системы являются:

1. данные о субъектах информационных систем;
2. данные о структуре объектов доступа;
3. данные о правах доступа пользователей информационных систем;
4. данные для настроек подключения к информационным ресурсам.

Данные о субъектах информационных систем принимаются в следующем виде:

* идентификатор субъекта (SID, UID);
* связи субъектов доступа друг с другом (вхождения в группы);
* дополнительная информация о субъекте (номер телефона, электронная почта и т.д.).

Данные о структуре объектов доступа принимаются в следующем виде перечня объектов доступа с иерархией.

Данные о правах доступа пользователей информационных систем принимаются в следующем виде:

* идентификаторы субъектов;
* структура объектов доступа;
* права доступа субъектов на объекты доступа.

Данные настроек подключения к информационным ресурсам принимаются в следующем виде:

* адрес информационного ресурса;
* название информационного ресурса;
* логин пользователя для подключения к информационному ресурсу;
* пароль доступа.

# Выходные данные

Выходными данными Системы являются матрицы прав доступа информационных систем, а так же матрицы вхождения пользователей в группы, хранящиеся в БД и представляющиеся в веб-интерфейсе.

Перечень терминов

В данном документе используются следующие термины и их определения:

1. **Администратор –** лицо, ответственное за функционирование Системы контроля прав доступа «Матрица доступа» в установленном штатном режиме работы.
2. **Аутентификация** – процедура проверки подлинности вводимых учетных данных.
3. **База данных** – представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины.
4. **Контролер** – лицо, ответственное за контроль над выполнением функций безопасности Системы контроля прав доступа «Матрица доступа».
5. **Оператор –** лицо, имеющее ограниченные привилегии по контролю выполнения функций безопасности Системы контроля прав доступа «Матрица доступа».
6. **Система доступа** – таблица, отображающая правила разграничения доступа.

Перечень сокращений

|  |  |
| --- | --- |
| Сокращение | Полное наименование |
| **АНЗ** | Контроль (анализ) защищенности информации |
| АРМ | Автоматизированное рабочее место |
| **БД** | База данных |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| **Система** | Система контроля прав доступа «Матрица доступа» |
| **СУБД** | Система управления базами данных |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Лист регистрации изменений** | | | | | | | | | |
| Изм. | Номера листов (страниц) | | | | Всего  листов  (страниц)  в докум. | № док. | Входящий № сопроводитель ного докум. и дата | Под. | Дата |
| изменен- ных | заменен-ных | новых | аннулиро-ванных |
|  |  |  |  |  |  |  |  |  |  |