МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение  
высшего образования

**«Южно-Уральский государственный университет**

**(национальный исследовательский университет)»**

**Высшая школа электроники и компьютерных наук**

**Кафедра системного программирования**

|  |
| --- |
| ДОПУСТИТЬ К ЗАЩИТЕ  Заведующий кафедрой, д.ф.-м.н., профессор  \_\_\_\_\_\_\_\_\_\_ Л.Б. Соколинский  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

**Разработка приложения для анализа географически-распределенных данных на платформе PySyft**

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ЮУрГУ – 09.03.04.2023.308-278.ВКР

|  |  |
| --- | --- |
|  | Научный руководитель,  доцент кафедры СП, к.ф.-м.н.,  доцент  \_\_\_\_\_\_\_\_\_\_ Г.И. Радченко  Автор работы, студент группы КЭ-403  \_\_\_\_\_\_\_\_\_\_ В.А. Дегтярев  Ученый секретарь  (нормоконтролер)  \_\_\_\_\_\_\_\_\_\_\_\_\_ И.Д. Володченко  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

Челябинск, 2023 г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение  
высшего образования

**«Южно-Уральский государственный университет**

**(национальный исследовательский университет)»**

**Высшая школа электроники и компьютерных наук**

**Кафедра системного программирования**

УТВЕРЖДАЮ

Зав. кафедрой СП

\_\_\_\_\_\_\_\_\_\_ Л.Б. Соколинский

06.02.2023 г.

**ЗАДАНИЕ**

**на выполнение выпускной квалификационной работы бакалавра**

студенту группы КЭ-403

Дегтяреву Владимиру Андреевичу,

обучающемуся по направлению

09.03.04 «Программная инженерия»

1. **Тема работы** (утверждена приказом ректора от \_\_.\_\_.2023 г. № \_\_\_)

Разработка приложения для анализа географически-распределенных данных на платформе PySyft.

1. **Срок сдачи студентом законченной работы:** 05.06.2023 г.
2. **Исходные данные к работе2**
3. Официальный сайт OpenMined. [Электронный ресурс] URL: <https://www.openmined.org/> (дата обращения: 13.02.2023 г.).
4. Официальный сайт PySyft. [Электронный ресурс] URL: <https://github.com/OpenMined/PySyft> (дата обращения 13.02.2023 г.).
5. Официальный сайт TenserFlow Federated. [Электронный ресурс] URL: <https://www.tensorflow.org/federated?hl=ru> (дата обращения 13.02.2023 г.).
6. Ziller A., Trask A., Lopardo A., Szymkow B., Wagner B., Bluemke E., Nounahon J.-M., Passerat-Palmbach J., Plakash K., Rose N., Ryffel T., Reza Z.N., Kaissis G. PySyft. A Library for Easy Federated Learning. // Part of the Studies in Computation Intelligence book series, 2021. – pp. 111–139.
7. **Перечень подлежащих разработке вопросов**
8. Выполнить обзор литературы.
9. Выполнить анализ аналогичных проектов.
10. Определить функциональные и нефункциональные требования к системе.
11. Спроектировать систему для анализа географически-распределенных данных на платформе PySyft.
12. Реализовать систему для анализа географически-распределенных данных на платформе PySyft.
13. Провести тестирование системы для анализа географически-распределенных данных на платформе PySyft.
14. **Дата выдачи задания:** 06.02.2023 г.

**Научный руководитель,**

доцент кафедры СП, к.ф.-м.н., доцент Г.И. Радченко

**Задание принял к исполнению** В.А. Дегтярев

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 5](#_Toc128160195)

[1. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ 7](#_Toc128160196)

[1.1. Описание предметной области 7](#_Toc128160197)

[1.2. Анализ аналогичных проектов 9](#_Toc128160198)

[1.2.1. PySyft 9](#_Toc128160199)

[1.2.2. TensorFlow Federated 10](#_Toc128160200)

[2. ПРОЕКТИРОВАНИЕ 12](#_Toc128160201)

[2.1. Функциональные требования к системе 12](#_Toc128160202)

[2.2. Нефункциональные требования к системе 13](#_Toc128160203)

[2.3. Диаграмма вариантов использования системы 13](#_Toc128160204)

[2.4. Диаграмма компонентов 15](#_Toc128160205)

[ЗАКЛЮЧЕНИЕ 17](#_Toc128160206)

[ЛИТЕРАТУРА 18](#_Toc128160207)

# ВВЕДЕНИЕ

**Актуальность**

В настоящее время в мире существует огромное количество информации. А также большое количество людей, которые хотят использовать эту информацию в своих научных интересах, для нахождения закономерностей, обучения нейросетей, чтобы получать ответы на важные вопросы.

Машинное обучение и анализ данных уже активно применяется в медицине, финансах, промышленности [1]. Однако эти технологии еще не могут уверенно отвечать на некоторые глобальные и сложные вопросы из-за отсутствия доступа у разработчиков и ученых к большому количеству информации. Основные причины этого выражаются в виде защиты персональных данных, сохранения приватности конкретных данных, а также раздробленности этих данных среди огромного количества организаций.

Эти проблемы можно решить с помощью систем географически-распределенного и конфиденциального машинного обучения.

**Постановка задачи**

Целью выпускной квалификационной работы является реализация системы для анализа географически-распределенных данных на платформе PySyft. Для достижения поставленной цели необходимо решить следующие задачи:

1. выполнить обзор литературы;
2. выполнить анализ аналогичных проектов;
3. определить функциональные и нефункциональные требования к системе;
4. спроектировать методы машинного анализа географически‑распределенных данных;
5. реализовать методы машинного анализа географически‑распределенных данных;
6. провести тестирование методов машинного анализа географически‑распределенных данных.

**Структура и содержание работы**

Работа состоит из введения, пяти глав, заключения и списка литературы. Объем работы составляет 29 страниц, объем списка литературы – 11 источников.

В первой главе описываются предметная область и аналогичные проекты.

Вторая глава содержит описание теоретической части по теме работы.

Третья глава посвящена определению функциональных и нефункциональных требований к системе и проектированию ее архитектуры.

Четвертая глава содержит в себе подробности и особенности реализации методов машинного анализа.

В пятой главе описывается процесс тестирования работы методов машинного анализа географически-распределенных данных.

# 1. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1. Описание предметной области

Целью данной работы является разработка приложения для анализа географически-распределенных данных на платформе PySyft. Анализ данных представляет собой область математики и информатики, которая занимается построением и исследованием наиболее общих математических методов и вычислительных алгоритмов извлечения знаний из экспериментальных данных с целью получения полезной информации и принятия решений [2].

Для решения сложных аналитических задач часто используются нейронные сети. Нейронная сеть – это математическая модель, а также её программное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей [3]. Нейронная сеть обучается в процессе обработки входных данных и при постепенном подборе нужных коэффициентов. Моделью обучения называется файл, который обучен распознаванию определенных типов закономерностей. Модель обучается на основе набора данных и алгоритма, который она может использовать для анализа и обучения на основе этих данных [4]. Нейронная сеть не имеет последовательного алгоритма выполнения. Результаты анализа нейронной сетью идентичных данных могут различаться между собой.

Особенностью машинного анализа географически-распределенных данных является то, что информация, которую анализирует система, распределена между различными независимыми устройствами.

Для обеспечения географически-распределенного анализа и конфиденциальности данных современные решения используют такие методы, как федеративное обучение, дифференциальная приватность, гомоморфное шифрование [5].

Федеративное обучение представляет собой метод машинного обучения, который позволяет коллективно обучать алгоритм на нескольких устройствах без централизации всех исходных данных на одном сервере. Системы федеративного обучения совершенствуют единую общую модель. Источники данных никогда не перемещаются и не объединяются, но каждое устройство вносит свой вклад в обучение и повышение качества общей модели [6].

Дифференциальная приватность – это область, изучающая методы, которые обеспечивают максимально точные результаты статистических запросов в базу данных при минимизации возможности идентификации отдельных записей в ней. Для каждого человека, чьи данные входят в анализируемый набор, дифференциальная приватность гарантирует, что результат анализа на дифференциальную приватность будет практически неотличим вне зависимости от того, есть ли данные этого конкретного человека в наборе или нет [7]. Дифференциальная приватность основана на введении случайности в данные. Чем больше случайности добавляется, тем сильнее сохраняется приватность, однако получаются более неточные результаты. Также на точность результатов влияет размер выборки, чем больше выборка, тем точнее результаты [8].

Гомоморфное шифрование – это форма шифрования, позволяющая производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполненных с открытым текстом [9]. Использование гомоморфного шифрования открывает множество перспектив при обработке конфиденциальных данных в среде, участники которой не доверяют друг другу. Оно позволяет осуществлять индексацию, фильтрацию спама, обработку платежей и другие действия без расшифровки самих сообщений и может применятся в облачных вычислениях, децентрализованных системах, электронном голосовании [10].

1.2. Анализ существующих платформ распределенного анализа данных

1.2.1. PySyft

В 2019 году была создана библиотека PySyft сообществом OpenMined. Это люди, объединенные темой конфиденциальности в машинном обучении. PySyft представляет собой обертку над PyTorch, Tensorflow или Keras для приватного машинного обучения [8].

Основная задача, стоящая перед сообществом OpenMined, заключалась в том, чтобы создать программное обеспечение, которое бы позволяла одному человеку получать ответы на свои вопросы, используя данные, принадлежащие другому человеку без необходимости просмотра и создания копии этих данных [11].

Проект предоставляет удаленный вызов процедур, что позволяет разработчику отправлять модель нейронной сети к пользователям, где она локально обучается на их данных, после чего возвращается с обновленными весами обратно разработчику (рисунок 1). Данный процесс может происходить одновременно на разных устройствах, тем самым происходит параллельное обучение модели нейронной сети[8].



Рисунок 1 – Взаимодействие разработчика с пользователями [12]

Также ключевой особенностью PySyft является использование дифференциальной приватности [11]. По измененным весам модели нейронной сети можно догадаться, какие данные были у пользователя. Чтобы это предотвратить, к данным, которые хранятся на вычислительной машине пользователя, добавляется шум. Дифференциальная приватность представляет собой методы, которые описывают добавление шума.

1.2.2. TensorFlow Federated

Компания Google давно занимается сбором некоторой информации с устройств пользователей в единое защищенное хранилище, на котором тренируют свои нейросети. В 2017 году в Google Research был предложен инновационный подход под названием федеративное машинное обучение. Он позволяет всем устройствам, которые участвуют в машинном обучении, делить на всех единую модель для прогнозирования, но при этом не делиться первичными данными для обучения модели. Система федеративного обучения работает по принципу совершенствования единой общей модели нейросети [13].

Для проверки системы федеративного обучения на больших объемах данных компанией Google был реализовал этот алгоритм в мобильном приложении клавиатуры Gboard [13]. Основной задачей являлось прогнозирование слов и выражений, которые пользователь предположительно использовал бы следующими во время печатания текста. Система федеративного обучения не отправляет текст, который печатает пользователь, на сервер компании Google, она отправляет На устройстве каждого пользователя производится анализ текста, который он использовал. Затем результаты анализа отправляются в компанию Google, где они будут объединены с другими результатами анализа для улучшения общей модели набора текста. Тем самым, каждый пользователь улучшает опыт использования Gboard каждому пользователю.

Компанией Google была создана платформа TensorFlow Federated с открытым исходным кодом для машинного обучения на децентрализованных данных. Архитектура данного платформы представлена на рисунке 2. TensorFlow Federated был разработан для облегчения исследований и экспериментов с федеративным обучением [14].



Рисунок 2 – Архитектура TensorFlow Federated [14]

**Выводы по первой главе**

В данной главе был проведен обзор предметной области и анализ существующих решений и проектов в области машинного анализа географически-распределенных данных.

# 2. ПРОЕКТИРОВАНИЕ

Целью данной работы является разработка системы для анализа географически-распределенных данных на платформе PySyft. Система представляет собой децентрализованное приложение, которое будет предоставлять одноранговую сеть для владельцев данных и аналитиков данных.

Владелец данных с помощью приложения сможет создать узел внутри целостной одноранговой сети, загружать и управлять данными, расположенными на этом узле.

Аналитик данных с помощью приложения сможет подключаться к различным узлам внутри сети и проводить аналитические операции на основе данных, расположенным на этих узлах.

В рамках данной работы будет создано 2 узла с данными. Также будет создан 1 узел для анализа данных, которые расположены на других узлах.

2.1. Функциональные требования к системе

Можно выделить следующий набор функциональных требований к системе.

1. Система должна предоставлять владельцу данных возможность запустить узел в одноранговой сети.
2. Система должна предоставлять владельцу данных возможность загрузить данные на созданный им узел в одноранговой сети.
3. Система должна предоставлять владельцу данных возможность удалить данные на созданном им узле в одноранговой сети.
4. Система должна предоставлять владельцу данных возможность отключить созданный им узел в одноранговой сети.
5. Система должна предоставлять владельцу данных возможность указать, к каким данные, среди тех, которые владелец данных разместил на узле, ограничивать доступ для аналитика данных.
6. Система должна предоставлять аналитику данных возможность использовать данные, размещенные на любых других узлах одноранговой сети.

2.2. Нефункциональные требования к системе

Можно выделить следующие нефункциональные требования к системе.

1. Система должна образовывать одну целостную одноранговую сеть.
2. Система должна обеспечивать аналитику данных возможность получать данные из нескольких узлов одновременно.
3. Система должна быть написана на языке программирования Python.
4. Система должна быть разработана с использованием таких инструментов, как: PySyft, PyGrid, PyTorch.

2.3. Диаграмма вариантов использования системы

Для проектирования системы был использован язык графического описания для объектного моделирования UML. На рисунке 3 представлена диаграмма вариантов использования.

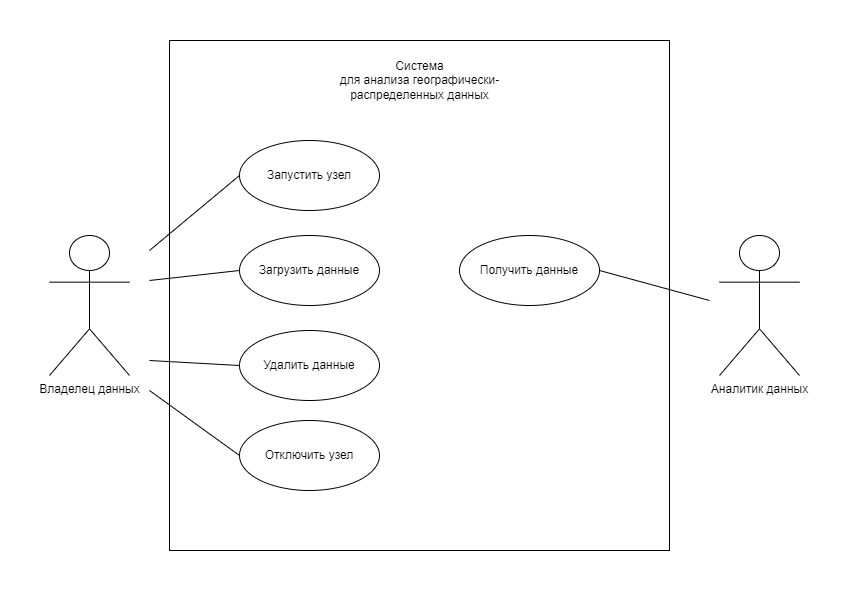


Рисунок 3 – Диаграмма вариантов использования системы для анализа географически-распределенных данных

В системе определены следующие виды акторов.

1. *Владелец данных* – это пользователь приложения, который может запустить и отключить узел в одноранговой сети для размещения на него определенных данных.
2. *Аналитик данных* – пользователь приложения, который может использовать размещенные на узлах данные для аналитических операций.

Актору «Владелец данных» доступны следующие варианты использования системы.

1. Владелец данных может запустить узел в одноранговой сети с помощью приложения для дальнейшего размещения на нем данных.
2. Владелец данных может загрузить данные на созданный им узел, которые в дальнейшем будут доступны аналитикам данных.
3. Владелец данных может удалить данные с созданного им узла.
4. Владелец данных может отключить узел в одноранговой сети с помощью приложения, после этого, все данные, которые были размещены на узле, станут недоступными для использования аналитиками данных.

Актор «Аналитик данных» может использовать систему только для получения данных, которые разместил актор «Владелец данных». Для этого ему необходимо выбрать определенный узел, загрузить данные, которые на нем размещены, и использовать их в своих аналитических операциях.

2.4. Диаграмма компонентов

На рисунке 4 представлена диаграмма компонентов системы.

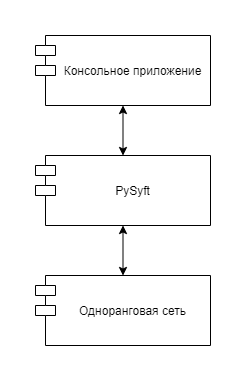


Рисунок 4 – Диаграмма компонентов системы

Система состоит из следующих компонентов.

1. Консольное приложение – приложение, с которым взаимодействуют пользователи.
2. PySyft – платформа, которая предоставляет методы для безопасного и конфиденциального анализа данных.
3. Одноранговая сеть – сетевая технология, которая позволяет нескольким сетевым устройствам совместно использовать ресурсы и взаимодействовать друг с другом.

2.5. Диаграммы деятельности

На рисунке 5 представлена диаграмма деятельности прецедента «Загрузить данные».

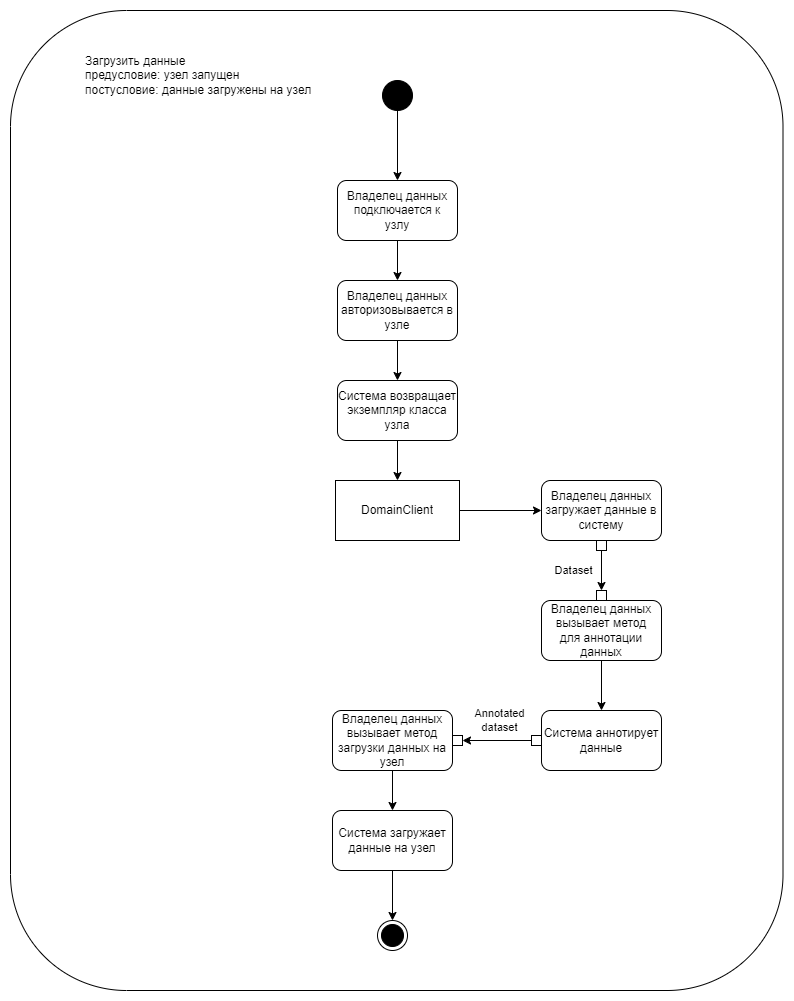


Рисунок 5 – Диаграмма деятельности прецедента

На рисунке 6 представлена диаграмма деятельности прецедента «Получить данные».

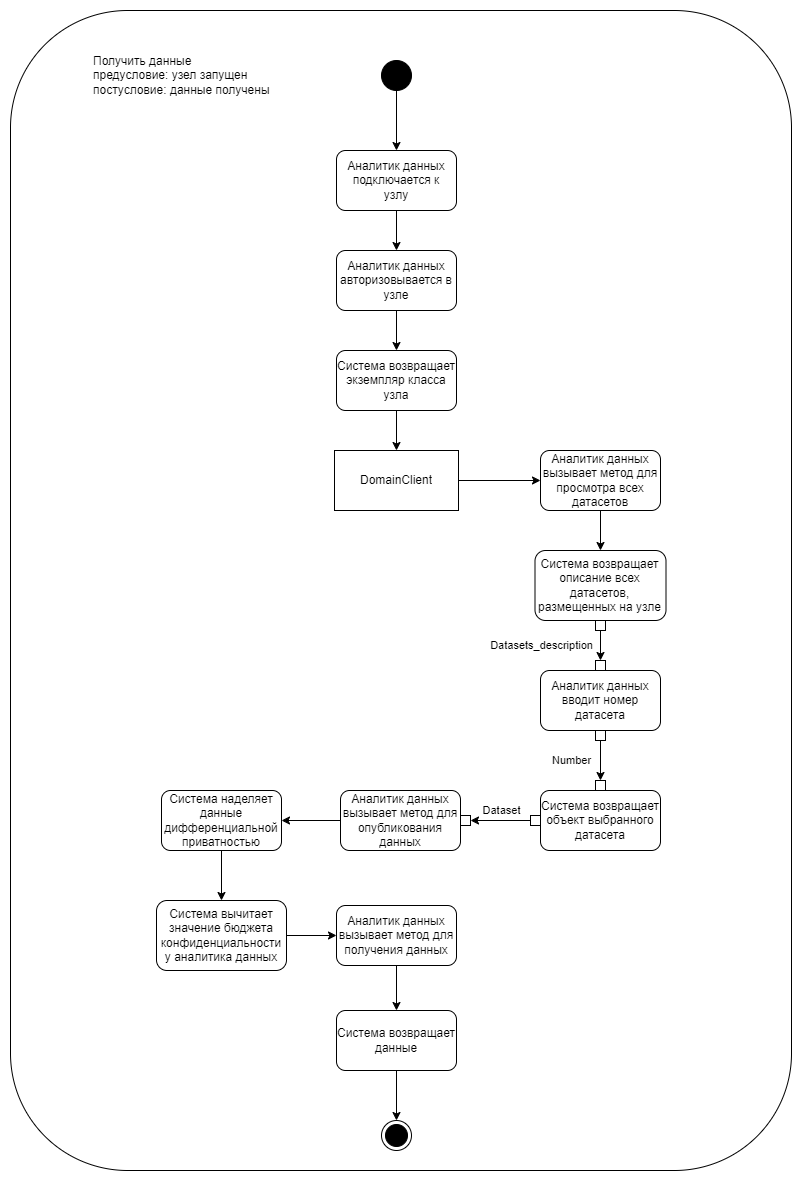


Рисунок 6 – Диаграмма деятельности прецедента

**Выводы по второй главе**

В данной главе были выделены функциональные и нефункциональные требования к системе, составлена диаграмма вариантов использования системы и разработана диаграмма компонентов системы.

# 3. РЕАЛИЗАЦИЯ

Для реализации системы для анализа географически-распределенных данных на платформе PySyft был выбран высокоуровневый язык программирования Python 3 [https://www.python.org], библиотека PySyft [?], инструмент командной строки HaGrid [?].

Для преобразования и анализа данных были использованы библиотеки numpy (?), pandas (?), sklearn (?).

3.1. Настройка окружения

Для создания изолированных сред была выбрана платформа Conda [https://docs.conda.io/]. На рисунке 7 показан процесс запуска изолированной среды для владельца данных «syft\_env».

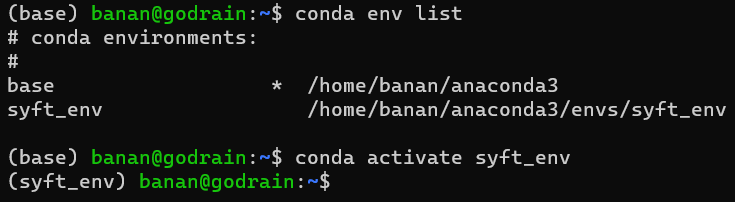


Рисунок 7 – Запуск изолированной среды для владельца данных

Запуск узла домена владельца данных был произведен с помощью инструмента HaGrid. HaGrid – это инструмент командной строки, который ускоряет развертывание PyGrid, программного обеспечения, обеспечивающего одноранговую сеть владельцев данных и аналитиков данных, которые могут совместно анализировать данные и обучать модели с помощью PySyft, [https://openmined.github.io/PySyft/deployment/index.html]. Процесс запуска узла домена показан на рисунке 8.

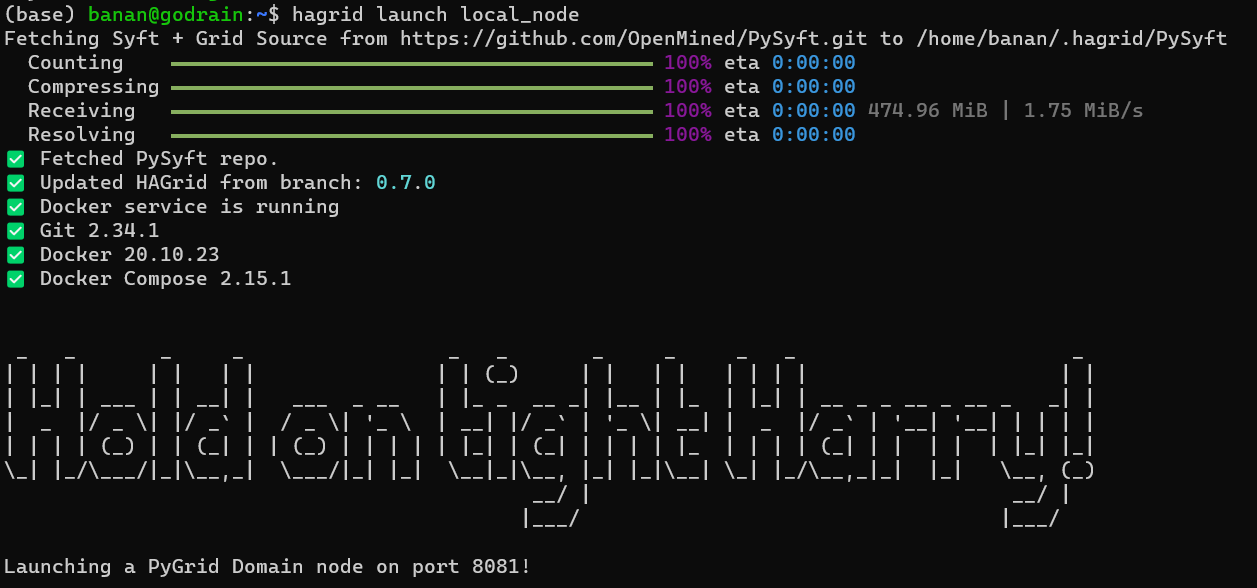


Рисунок 8 – Запуска узла домена владельца данных

Узел домена занимает порт 8081. При развертывании узла домена создаются и запускаются «Docker» контейнеры. Данный процесс показан на рисунке 9.

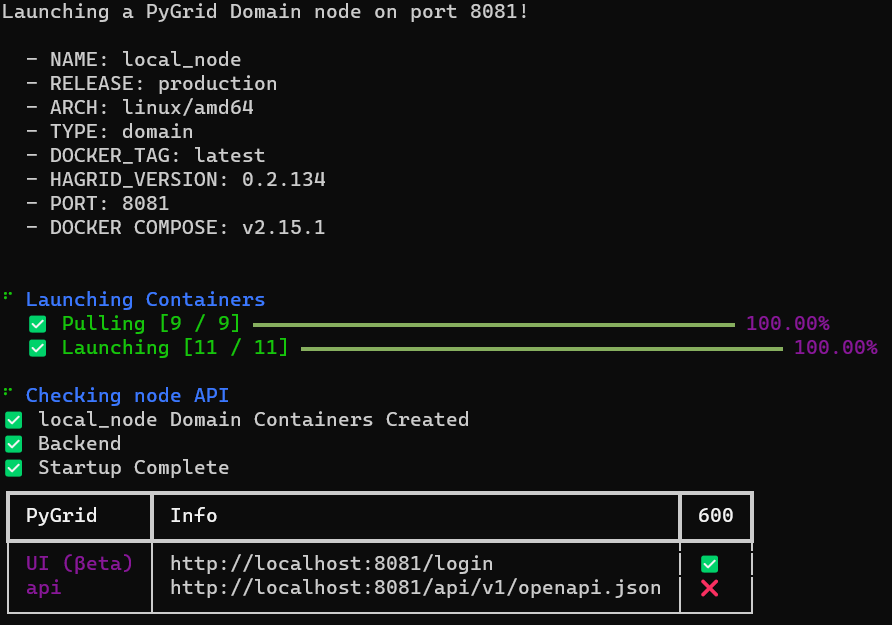


Рисунок 9 – Запуска узла домена владельца данных

3.2. Постановка прикладной задачи

В качестве примера работоспособности системы в рамках данной работы будет решена задачи классификации.

Цель прикладной задачи заключается в том, чтобы на основе данных о ядрах клеток опухоли молочной железы выявить, злокачественной или доброкачественной является клетка опухоли.

Для решения данной задачи будет реализована модель дерева решений.

Данные о клетках молочной железы были взяты с сайта Kaggle [https://www.kaggle.com/datasets/uciml/breast-cancer-wisconsin-data]. Это набор данных, представляющий собой таблицу с 31 столбцом, каждый из этих столбцов обозначает определенную характеристику ядра клетки молочной железы и имеет вещественное значение, а также столбец, который обозначает тип клетки.

3.3. Процесс загрузки данных на узел

Процесс подключения к узлу в качестве владельца данных продемонстрирован в листинге 1.

Листинг 1 – Подключение к узлу

try:

domain\_client = sy.login(

port=8081,

email="info@openmined.org",

password="20052005"

)

except Exception as e:

print("Unable to login. Please check your domain is up with `!hagrid check localhost:8081 --timeout=120`")

Исходные данные были обработаны. Был удален пустой столбец «Unnamed». Исходный набор данных был разделен на два набора данных, так как для решения задачи нужно наделить дифференциальной приватностью все столбцы, кроме столбца, обозначающего тип клетки.

Данные были аннотированы с дифференциальной приватностью с помощью метода annotate\_with\_dp\_metadata класса Tensor. В параметрах данного метода были указаны нижняя и верхняя границы предельно допустимых значений для конкретного набора данных. Для каждого набора данных эти значения будут различаться, например, на основе всего набора данных, для данных о среднем расстоянии от центра до точек на периметре ядра клетки (radius\_mean) нижняя граница равняется 0, а верхняя граница 30. Также были выделены субъекты набора данных, то есть сущности, информация о которых не будет никому предоставляться. Для данного набора данных субъектом является идентификатор (id), то есть у любой строки таблицы будет отсутствовать идентификатор (id).

Процесс аннотации представлен в листинге 2.

Листинг 2 – Аннотирование данных

final\_dataset = dict()

data\_subjects = sy.DataSubjectArray.from\_objs(dataset1["id"])

final\_dataset["radius\_mean"] = sy.Tensor(dataset1["radius\_mean"]).annotate\_with\_dp\_metadata(

lower\_bound=0, upper\_bound=30, data\_subject=data\_subjects

)

Аналогично были аннотированы все столбцы набора данных. Все аннотированные столбцы добавляются в словарь final\_dataset. Исходный код представлен в приложении.

Для загрузки данных на узел был использован метод load\_dataset класса DomainClient (листинг 3). В параметрах метода были указаны данные, которые будут храниться в датасете, его имя и описание.

Листинг 3 – Загрузка данных характеристик

domain\_client.load\_dataset(

name="testDataset\_v3",

assets=final\_dataset,

description="Our dataset contains real-valued features for cell nucleus of a breast mass. There are 31 columns and 250 rows in our dataset."

)

Также на узел был загружен второй набор данных, обозначающий тип клетки (листинг 4).

Листинг 4 – Загрузка данных типа клетки

domain\_client.load\_dataset(

name="testDataset\_v3\_diagnosis",

assets={

"diagnosis": diagnosis,

},

description="Dataset contains diagnosis result. There are 1 column and 250 rows in our dataset."

)

Для того, чтобы проверить загрузку данных на узел, выведем объект datasets класса DomainClient. Вывод объекта представлен на рисунке 10.

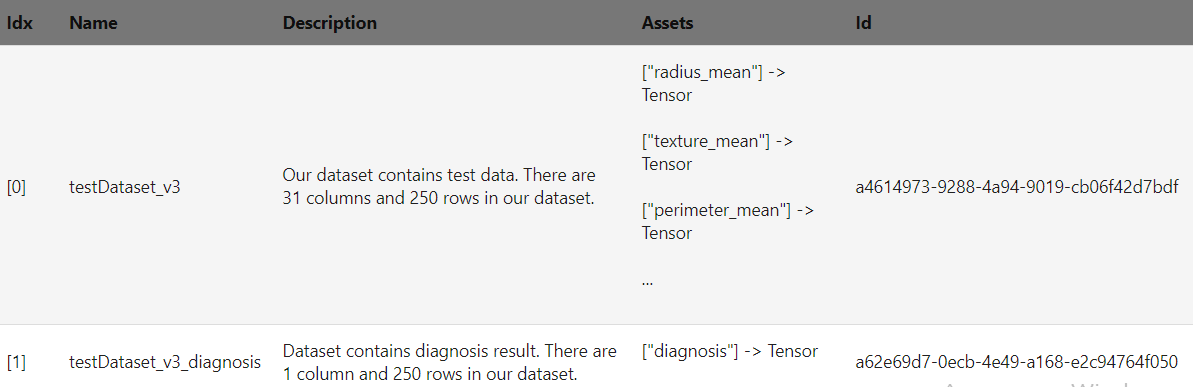


Рисунок 10 – Загруженные на узел данные

Также с профиля владельца данных был создан новый пользователь с ролью аналитика данных при помощи метода create объекта users. В параметрах метода были указаны имя пользователя, почта, пароль и количество бюджета конфиденциальности. Вызов метода представлен в листинге 5.

Листинг 5 – Создание нового пользователя

domain\_client.users.create(

\*\*{

"name": "Vladimir Fake",

"email": "vova.degtyarev.01@mail.ru",

"password": "20012002",

"budget": 5000000

}

)

Для того, чтобы посмотреть всех пользователей узла, выведем объект users (рисунок 11). В рамках данного узла существуют два пользователя. Пользователь Jane Doe является владельцем данных, а пользователь Vladimir Fake является аналитиком данных.

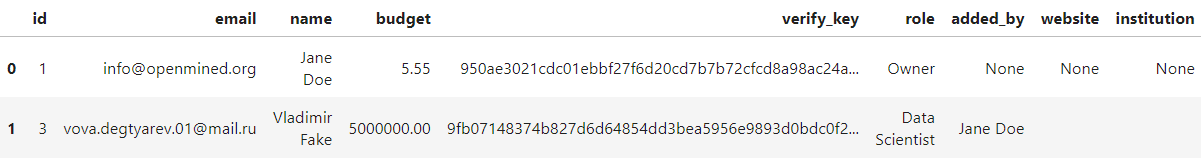


Рисунок 11 – Вывод объекта users

3.4. Процесс получения данных из узла

Процесс подключения к узлу в качестве аналитика данных продемонстрирован в листинге 6.

Листинг 6 – Подключение к узлу

try:

domain = sy.login(

email="vova.degtyarev.01@mail.ru",

password="20012002",

url="localhost",

port=8081

)

except Exception as e:

print("Unable to login. Please check the domain you are connecting to`")

Информация о том, какие данные хранятся на подключенном узле находится в объекте datasets экземпляра domain. Вывод объекта представлен на рисунке 12.

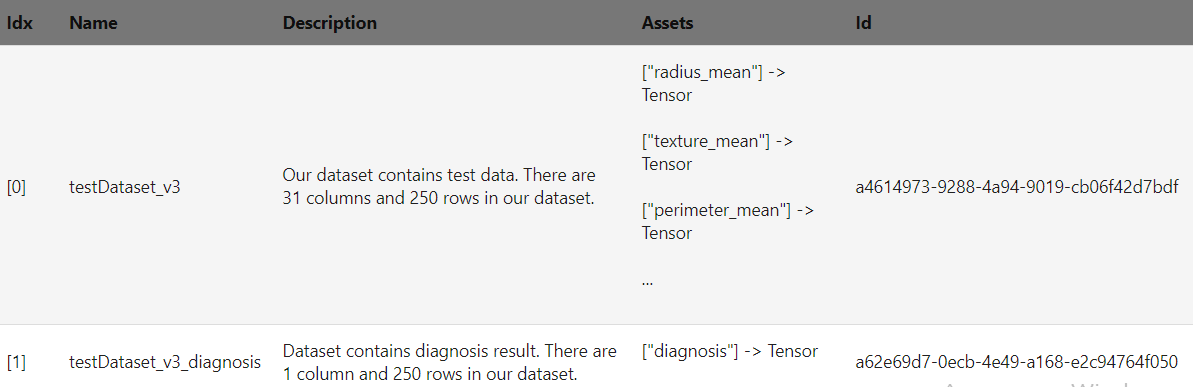


Рисунок 12 – Вывод объекта datasets

Аналитик данных может вывести любой размещенный на узле объект данных для получения демонстрационных данных. Например, вывод объекта, представляющего собой тензор radius\_mean датасета с идентификатором 0 представлен на рисунке 13.

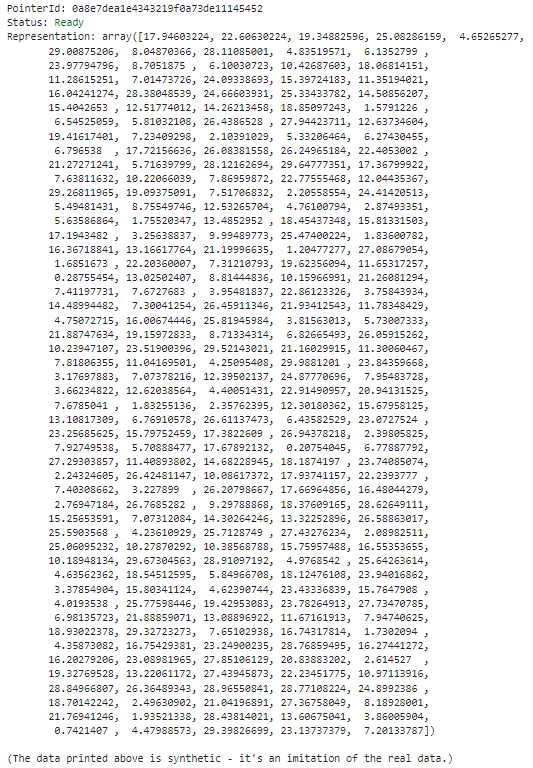


Рисунок 13 – Вывод тензора radius\_mean

Для того, чтобы аналитик данных смог получить данные с узла, ему нужно вызвать метод publish определенного объекта данных, чтобы узел наделил исходные данные этого объекта дифференциальной приватностью. Процесс преобразования данных происходит на узле, к которому подключается аналитик данных. В параметрах этого метода указывается значение сигмы. Значение сигмы определяет насколько точны будут полученные данные. Сигма определяет максимальный разброс между значениями исходных и предоставляемых данных. Преобразование данных происходит так, что к исходным значениям данных добавляется случайная величина в диапазоне от отрицательного до положительного значения сигмы. Чем меньше значение сигмы, тем более точны будут полученные данные, и тем больше бюджета конфиденциальности будет потрачено у аналитика данных. Для каждой из характеристик ядра клетки экспериментальным путем были подобраны оптимальные значения сигм.

После того, как узел преобразовал данные, аналитик данных может получить преобразованные данные вызвав метод get.

Процесс получения данных о характеристиках ядер клеткок аналитиком показан в листинге 7.

Листинг 7 – Получение данных

published\_data = []

sigmas = [3, 4, 20, 100, 0.03, 0.01, 0.05, 0.03, 0.04, 0.01, 0.05, 0.15, 0.4, 5, 0.01, 0.04, 0.08, 0.01, 0.01, 0.01, 4, 5, 15, 80, 0.015, 0.01, 0.1, 0.1, 0.08, 0.02]

for asset\_n, sigma\_n in zip(assets, sigmas):

feature = cancer\_dataset[asset\_n['name']]

feature\_public = feature.publish(sigma=sigma\_n)

feature\_public.block\_with\_timeout(50)

privacy\_feature = feature\_public.get(delete\_obj=False)

published\_data.append(privacy\_feature)

Полученные данные были обработаны и преобразованы в DataFrame (листинг 8).

Листинг 8 – Преобразование данных

published\_data1 = np.asarray(published\_data)

deboxed = np.array([item for item in published\_data1.flatten()]).reshape(published\_data1.shape)

data\_df = pd.DataFrame(deboxed)

data\_df = data\_df.transpose()

Преобразованные данные продемонстрированы на рисунке 14.

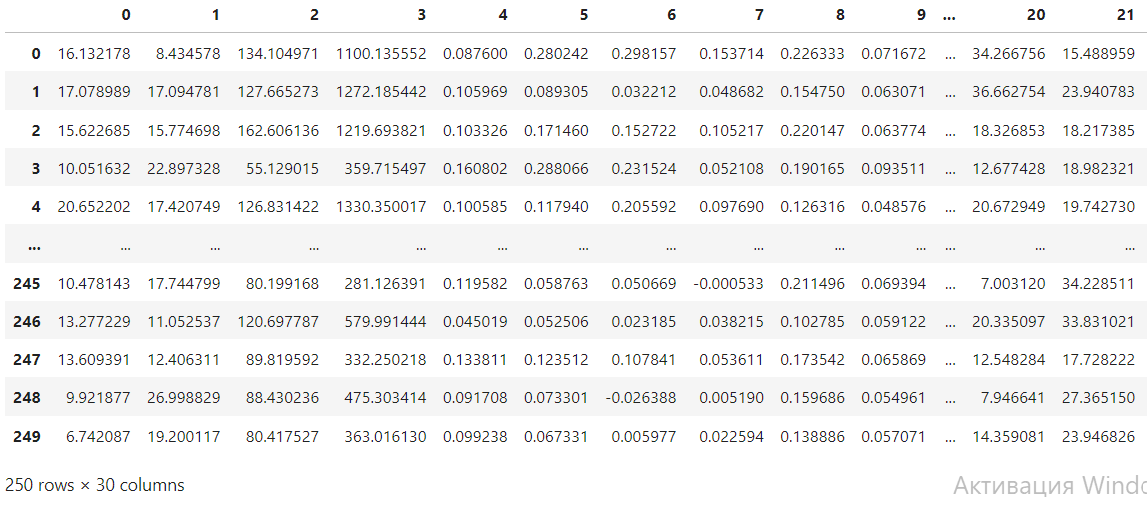


Рисунок 14 – Преобразованные данные

Также аналитиком были получены данные о типах клеток, так как эти данные не были аннотированы дифференциальной приватностью, для их получения достаточно вызвать метод get. Процесс получения и преобразования данных в DataFrame показан в листинге 9.

Листинг 9 – Получение данных

diagnosis\_data = diagnosis\_dataset["diagnosis"].get(delete\_obj=False)

diagnosis\_data = diagnosis\_data.child

deboxed\_diagnosis = np.array([item for item in diagnosis\_data.flatten()]).reshape(diagnosis\_data.shape)

data\_df\_diagnosis = pd.DataFrame(deboxed\_diagnosis)

На операции получения данных аналитик данных потратил 311996 единиц конфиденциальности бюджета.

3.5. Реализация прикладной задачи

Для построение модели дерева решений был использован класс DecisionTreeClassifier библиотеки sklearn [?]. В конструкторе класса был указан критерий энтропии, который вычисляет энтропию Шеннона возможных классов [https://scikit-learn.org/stable/modules/tree.html#tree-mathematical-formulation].

После разделения данных на обучающие и тестовые выборки, модель была обучена на обучающей выборке с помощью метода fit, где обучающими входными образцами являлись данные о характеристиках ядер клеткок, а целевым значением данные о типах клеток. Также на тестовых данных было подсчитана средняя точность модели с помощью метода score.

Перед обучением модели, она с помощью библиотеки pickle [?] загружается из файла «model.pkl», а после обучения модели на данных, она сохраняется в этот же файл. Тем самым, модель совершенствуется после каждого обучения на новом наборе данных.

Процесс загрузки, обучения и сохранения модели продемонстрирован в листинге 10.

Листинг 10 – Загрузка, обучение и сохранение модели

from sklearn import tree

from sklearn.model\_selection import train\_test\_split

import pickle

import os.path

X = data\_df

y = data\_df\_diagnosis

#загрузка или создание модели

if os.path.isfile('model.pkl'):

with open("model.pkl", 'rb') as file:

clf = pickle.load(file)

else:

clf = tree.DecisionTreeClassifier(criterion='entropy')

X\_train, X\_test, y\_train, y\_test = train\_test\_split(X, y, test\_size=0.2, random\_state=42)

clf.fit(X\_train, y\_train)

accuracy = clf.score(X\_test, y\_test)

print("Accuracy:", accuracy)

#сохранение модели

pkl\_filename = "model.pkl"

with open(pkl\_filename, 'wb') as file:

pickle.dump(clf, file)

**Выводы по третьей главе**

В данной главе была реализована система для анализа географически-распределенных данных на платформе PySyft, было запущено два узла, на которые были загружены данные о ядрах клеток опухоли молочной железы, с другого компьютера были получены эти данные, обладающие дифференциальной приватностью, также была реализована прикладная задача по построению модели дерева решений на основе полученных данных.

# 4. ТЕСТИРОВАНИЕ

Для тестирования системы для анализа географически-распределенных данных на платформе PySyft и функции системы наделять данные на узлах дифференциальной приватностью выведем данные, которые были загружены на узел (рисунок 15), а также данные, которые были получены аналитиком данных (рисунок 16).

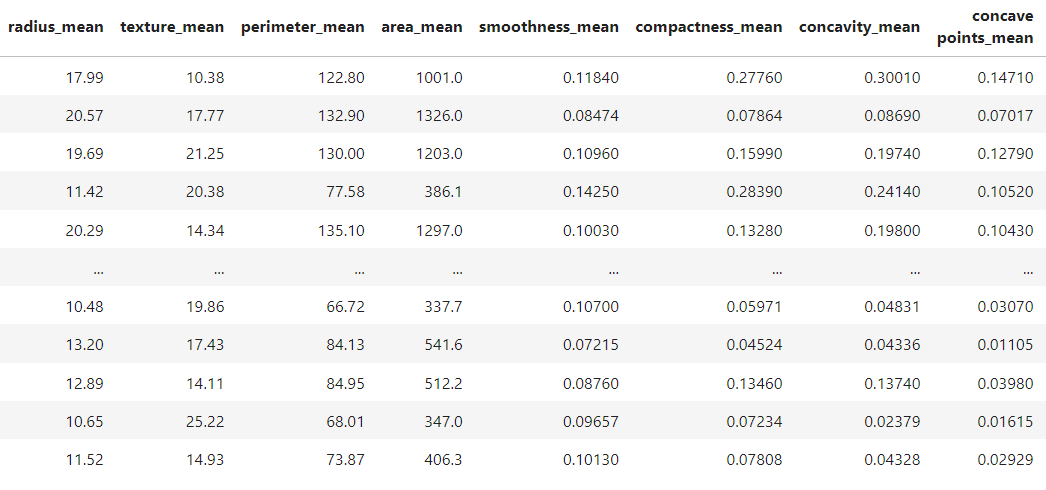


Рисунок 15 – Загруженные на узел данные



Рисунок 16 – Полученные данные

После обучения модели на наборе данных, размещенном на первом узле, среднее значение точности модели было равно 0,88. После последующего обучения этой же модели на наборе данных, размещенном на втором узле, среднее значение точности модели было равно 0,94.

**Выводы по четвертой главе**

В данной главе была протестирована система для анализа географически-распределенных данных на платформе PySyft на возможность загрузки данные на узел, получения этих данных, преобразованных с дифференциальной приватностью. Также были получены результаты точности построенной модели дерева решений после обучения на данных, размещенных на двух узлах.

# ЗАКЛЮЧЕНИЕ

В рамках данной работы была спроектирована и реализована система для анализа географически-распределенных данных на платформе PySyft. При этом были решены следующие задачи.

1. Выполнен обзор литературы.
2. Выполнен анализ аналогичных проектов.
3. Определены функциональные и нефункциональные требования к системе.
4. Составлена диаграмма вариантов использования системы.
5. Разработана диаграмма компонентов системы.

# ЛИТЕРАТУРА

1. 7 примеров применения машинного обучения в 5 отраслях бизнеса. [Электронный ресурс] URL: https://mcs.mail.ru/blog/17-primerov-mashinnogo-obucheniya (дата обращения: 13.02.2023 г.).
2. Анализ данных – основы и терминология. [Электронный ресурс] URL: https://habr.com/ru/post/352812/ (дата обращения: 13.02.2023 г.).
3. Нейронные сети для начинающих. Решение задачи классификации Ирисов Фишера. [Электронный ресурс] URL: https://habr.com/ru/company/ruvds/blog/679988/ (дата обращения: 16.02.2023 г.).
4. Что такое модель машинного обучения? [Электронный ресурс] URL: https://learn.microsoft.com/ru-ru/windows/ai/windows-ml/what-is-a-machine-learning-model (дата обращения: 16.02.2023 г.).
5. Официальный сайт PySyft. [Электронный ресурс] URL: <https://github.com/OpenMined/PySyft>/ (дата обращения: 13.02.2023 г.).
6. Масштабируемый подход к частично локальному федеративному обучению. [Электронный ресурс] URL: https://habr.com/ru/post/645783/ (дата обращения: 16.02.2023 г.).
7. Дифференциальная приватность — анализ данных с сохранением конфиденциальности. [Электронный ресурс] URL: https://habr.com/ru/company/domclick/blog/526724/ (дата обращения: 16.02.2023 г.).
8. Конфиденциальное машинное обучение. Библиотека PySyft. [Электронный ресурс] URL: <https://habr.com/ru/post/500154/> (дата обращения: 16.02.2023 г.).
9. Методы обфускации трафика. Гомоморфное шифрование. [Электронный ресурс] URL: https://habr.com/ru/company/globalsign/blog/717482/ (дата обращения: 16.02.2023 г.).
10. Цифровые фиатные деньги, гомоморфное шифрование и другие перспективные направления криптографии. [Электронный ресурс] URL: https://habr.com/ru/company/kryptonite/blog/658113/ (дата обращения: 16.02.2023 г.).
11. Официальный сайт OpenMined. [Электронный ресурс] URL: <https://www.openmined.org/> (дата обращения: 13.02.2023 г.).
12. Introduction to Remote Data Science. [Электронный ресурс] URL: https://habr.com/ru/post/402987/ (дата обращения: 13.02.2023 г.).
13. Google изобрела распределённый ИИ для миллиарда смартфонов. [Электронный ресурс] URL: https://habr.com/ru/post/402987/ (дата обращения: 13.02.2023 г.).
14. Официальный сайт Tensorflow Federated. [Электронный ресурс] URL: https://www.tensorflow.org/federated/ (дата обращения: 13.02.2023 г.).