1. **Документ концепции о границах**
   Положение о концепции приложения для распознавания сообщений с признаками информации ограниченного доступа

Для специалистов информационной безопасности, которым необходимо классифицировать сообщения в информационных системах. Данное приложение, помимо своей основной цели, способно осуществлять мониторинг файловой системы для поиска конфиденциальных файлов. Приложение оснащено функциями авторизации при выходе, логирования и запуску в фоновом режиме, что делает возможным ее использование простыми пользователями для собственных нужд (например, при временной передаче устройства). Данное приложение не имеет аналогов на рынке.

2. **Варианты использования**

Таблица 1 – Автоанализ

Идентификатор и название варианта использования	UC-1. Автоматический анализ файлов
Автор	Никита Колпаков
Основное действующее лицо	Временный пользователь устройства
Дополнительные действующие лица	Владелец устройства
Описание	При запуске программы активизируется модуль анализа файлов. При совершении каких-нибудь операций с файлами (копирование, переименование, удаление, перемещение), а также с текстом в буфере обмена все содержимое будет отправляться на анализ. Результат будет записываться в логи.
Условие-триггер	Совершение временным пользователем различных действий в файловой системе и буфере обмена
Предварительные условия	PRE-1. Владелец запустил программу на устройстве в фоновом режиме PRE-2. Временный пользователь взял устройство для пользования

Выходные условия	POST-1. Результаты действий временного пользователя записываются в логи POST-2. При попытке совершить различные действия с конфиденциальными файлами будет наложен запрет и высветится диалоговое окно с уведомлением
Нормальное направление	**1.0 «Легальная» работа в устройстве** 1. Временный пользователь совершает различные действия, которые не затрагивают работу с конфиденциальными файлами на устройстве 2. Все действия записываются в логи 3. После окончания работы владелец вводит пароль от приложения, и оно отключается
Альтернативные направления	**1.1 «Нелегальная» работа в устройстве** 1. Временный пользователь совершает различные действия, которые могут затрагивать работу с конфиденциальными файлами на устройстве 2. При наличии таких действий они блокируются и высвечивается диалоговое окно с описанием 3. Шаги 2-3 в нормальном направлении **1.2 Попытка временного пользователя отключить программу** 1. Пользователь пытается закрыть программу в трее 2. Высвечивается диалоговое окно с вводом пароля для отключения, который имеется только у владельца устройства
Исключения	**1.0E1. Ложные срабатывания классификатора** 1. При действиях, совершенных с файлами или текстовыми данными, которые классификатор ошибочно посчитал конфиденциальными, будут записываться события в логи или блокироваться действия (в зависимости от того, над чем были совершены действия)
Приоритет	Высокий

Частота использования	В зависимости от наличия и потребностей временных пользователей
Бизнес-правила	
Другая информация	1. Для большей безопасности пароль для закрытия приложения генерируется заново при совершении негативного действия
Предположения	Предполагается, что пользователь точно попробует закрыть программу (пойдет по направлению 1.2)

Таблица 2 – Ручной анализ

Идентификатор и название варианта использования	UC-2. Ручной анализ выбранных файлов
Автор	Никита Колпаков
Основное действующее лицо	Временный пользователь устройства
Дополнительные действующие лица	Владелец устройства
Описание	При запуске программы есть возможность запустить модуль ручного анализа файлов. При переходе к нему открывается новое окно, в котором пользователю нужно выбрать файл для анализа и нажать на кнопку «Проверить». Через несколько секунд проверка закончится и в новом диалоговом окне высветится результат.
Условие-триггер	Активация временным пользователем модуля ручного анализа файлов
Предварительные условия	PRE-1. Владелец запустил программу на устройстве в фоновом режиме PRE-2. Временный пользователь взял устройство для пользования
Выходные условия	POST-1. Результат проверки показывается временному пользователю
Нормальное направление	**1.0 Проверка файлов поддерживаемых типов**

	1. Временный пользователь загружает файлы из файловой системы в формате .txt, .pdf или .docx 2. После проверки файла в диалоговом окне высвечивается результат
Альтернативные направления	**1.1 Проверка файлов неподдерживаемых типов** 1. Временный пользователь загружает файлы из файловой системы в любом неподдерживаемом формате (все, кроме .txt, .pdf или .docx) 2. В диалоговом окне высвечивается информация, что данные форматы не поддерживаются. Проверка не осуществляется
Исключения	**1.0E1. Неверный ввод** 1. В модуле есть возможность выбрать файл, задав его абсолютный путь в файловой системе. При ошибке в написании высвечивается диалоговое окно с ошибкой, что такого файла не существует
Приоритет	Высокий
Частота использования	В зависимости от наличия и потребностей временных пользователей
Бизнес-правила	
Другая информация	нет
Предположения	Предполагается, что данный вариант использования будет актуальным только для владельца

3. Спецификация требований

1. Введение

1.1 Назначение проекта

Эта спецификация требований к ПО описывает функциональные и нефункциональные требования к приложению для распознавания сообщений с признаками информации ограниченного доступа (Приложение). Этот документ предназначен для команды, которая будет реализовывать и проверять корректность работы системы. Кроме специально обозначенных

случаев, все указанные здесь требования имеют высокий приоритет и приписаны к выпуску 1.0.

1.2 Соглашения, принятые в документах

В этой спецификации нет никаких типографских условных обозначений.

1.3 Границы проекта

Приложение позволит владельцам устройств быть осведомленными о совершенных действиях временными пользователями в удобочитаемом формате.

1.4 Ссылки

1. Beatty, Joy. Process Impact Intranet Development Standard, Version 1.3, *www.processimpact.com/corporate/standards/PI Intranet Development Standard.pdf*

2. Общее описание

2.1 Общий взгляд на продукт

Приложение – это программный комплекс, направленный на защиту данных устройства путем установки разграничения доступа к файлам после их классификации. Use-case диаграмма временного пользователя представлена на рисунке 1.

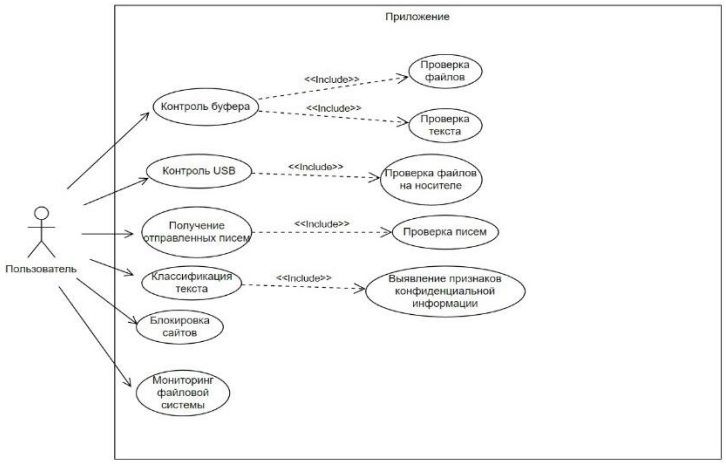

Рисунок 1 – Use-case диаграмма временного пользователя

2.2 Классы и характеристики пользователей

Классы и характеристики пользователей приведены в таблице 3.

Таблица 3 – Пользователи

Класс пользователей	**Описание**
Владелец устройства	Лицо, имеющее в собственности устройство, на котором запущено Приложение. Предполагается, что на устройстве имеются различные конфиденциальные файлы владельца, которые Приложение и должно защищать.
Временный пользователь	Лицо, нуждающееся в использовании устройства владельца на определенное время и под определенные задачи.

2.3 Операционная среда

OE-1. Приложение работает со следующими операционными системами: Windows 8.1, 10, 11.

2.4 Ограничения дизайна и реализации

CO-1. Документация системы по дизайну, коду и сопровождению должна соответствовать *Process Impact Intranet Development Standard, версия 1.3* [1].

2.5 Предположения и зависимости

DE-1. Приложение зависит от сторонних библиотек на Python таких, как tensorflow и пр., а также от состояния и вида обучающих данных для нейросетевой модели.

3. Системные функции

3.1 Автоматический анализ файлов

3.1.1 Описание

Временный пользователь совершает различные действия в устройстве. Допускается, что он может не знать, какие файлы конфиденциальные, а какие нет. При первом запуске Приложение осуществляет автоматический анализ файлов в выбранной директории и помещает результаты проверки в базу данных.

3.1.2 Функциональные требования

Описание функциональных требований с использованием иерархических текстовых тегов приведено в таблице 4.

Таблица 4 – ФТ Автоанализа

Автоанализ. Запись в БД	**Запись результатов в БД**
.Проверка:	Все файлы в выбранной директории проверяются с помощью классификатора
.Запись:	Все результаты проверки помещаются в БД в виде: <имя_файла> - <хэш> - <результат_проверки (bool)>

3.2 Ручной анализ выбранных файлов

3.2.1 Описание

Владелец устройства может до запуска основного функционала Приложения протестировать работу классификатора на конкретных выбранных файлах. Примечание: владелец должен знать сам, какие файлы в тестах являются конфиденциальными, а какие нет.

3.2.2 Функциональные требования

Описание функциональных требований с использованием иерархических текстовых тегов приведено в таблице 5.

Таблица 5 – ФТ Ручного анализа

Ручной анализ. Проверка	**Проверка файов**
.Выбор:	Владелец выбирает нужный файл для проверки. Важно, чтобы он был поддерживаемого типа (.txt, .docx или .pdf)
.Проверка:	Выбранный файл проверяется с помощью классификатора
.Результат:	Результат проверки высвечивается в диалоговом окне, без записи в БД

4. Требования к данным

4.1 Логическая модель данных

Фрагмент модели данных для Приложения приведен на рисунке 2.

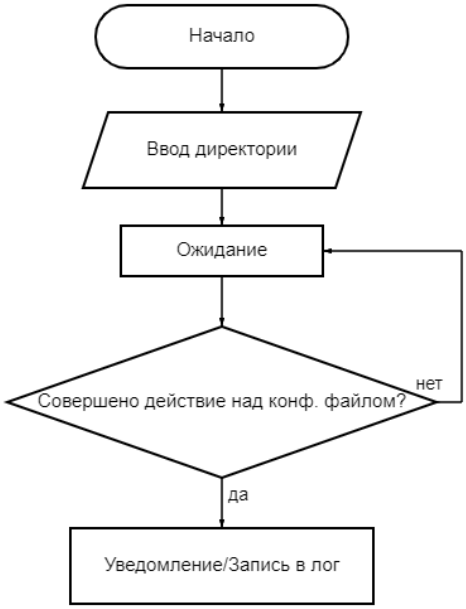

Рисунок 2 – Общий алгоритм Приложения

4.2 Отчеты

4.2.1 Отчет о зарегистрированных действиях

Требования к отчету о зарегистрированных действиях приведен в таблице 6.

Идентификатор отчета	RPT-1
Заголовок отчета	Зарегистрированные действия
Приоритет	Высокий
Пользователи отчета	Владелец устройства
Источники данных	Данные формируется на основе действий временного пользователя
Частота и использование	Данные отчета статичны. Отчет можно распечатать, если устройство поддерживает печать
Время доступа	Доступен сразу после окончания сеанса Приложения
Тело отчета	Отображаемые поля и заголовки столбцов: - Действие (перемещение, удаление и пр.) - Путь к файлу - Время действия
Признак конца отчета	Нет

4.3 Целостность, сохранение и утилизация данных

DI-1. Приложение должно хранить отчеты на протяжении всего времени, до их непосредственного удаления владельцем устройства.

5 Требования к интерфейсам

5.1 Пользовательские интерфейсы

UI-1. Все элементы на экранах должны быть удобочитаемы, а также соответствовать требованиям дизайна создания десктоп-приложений на Python.

5.2 Интерфейсы ПО

Все интерфейсы и модули Приложения указаны на рисунке 3.

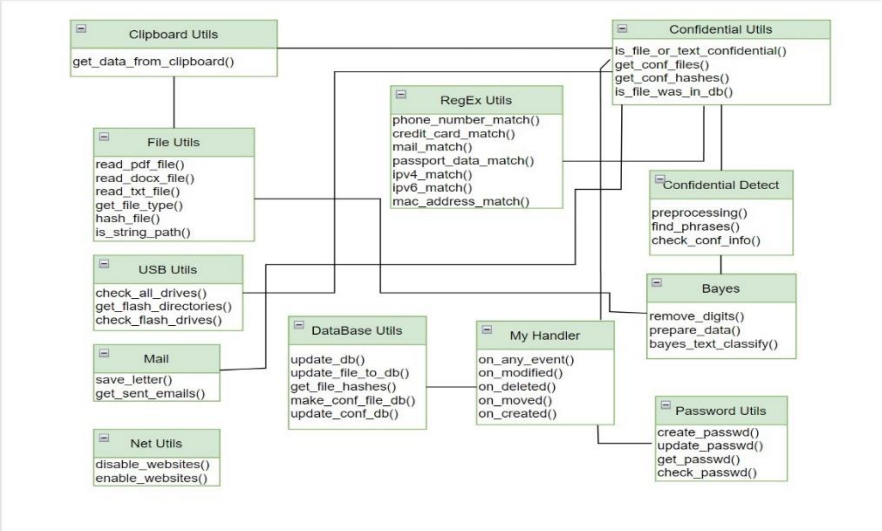

Рисунок 3 – Диаграмма классов Приложения

5.3 Интерфейсы оборудования

Не выявлены

5.4 Коммуникационные интерфейсы

Не выявлены

6 Атрибуты качества

6.1 Требования по удобству использования

USE-1. Приложение не должно оказывать существенное влияние на работу временного пользователя, которая не касается работы с конфиденциальными данными.

6.2 Требования к производительности

PER-1. Ручной анализ файла должен занимать не более 15 секунд в случае, когда файл больше 2 Мб.

6.3 Требования к безопасности

SEC-1. Пароль от выхода из Приложения должен быть не менее 8 символов в длину, а также содержать цифры, буквы в различном регистре.

SEC-2. У временного пользователя не должна быть возможность удалить отчеты в процессе работы Приложения.

6.4 Требования к защите

SAF-1. Временный пользователь должен быть осведомлен о некорректности своих действий путем получения уведомлений от Приложения.

6.5 Требования к доступности

AVL-1. Приложение должно быть активно и доступно на протяжении всего сеанса временного пользователя.

6.6 Требования к надежности

ROB-1. Приложение должно оставаться активным при совершении большого количества операций временным пользователем.