Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Институт прикладной математики и компьютерных наук
Кафедра компьютерной безопасности

ДОПУСТИТЬ К ЗАЩИТЕ В ГЭК
Руководитель ООП
канд. техн. наук, доцент
_____ В.Н. Тренькаев

26 января 2024 г.

# ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА СПЕЦИАЛИСТА (ДИПЛОМНАЯ РАБОТА)

Разработка защищённого программного обеспечения АСУТП установки анализа металлургической пульпы с пробоотбором

по специальности 10.05.01 Компьютерная безопасность
специализация «Анализ безопасности компьютерных систем»

Фесковича Андрея Олеговича

Научный руководитель ВКР
канд. техн. наук, доцент
_____С. А. Останин
*подпись*
15 января 2024 г.

Автор работы
студент группы № 931824
_____ А. О. Фесковича
*подпись*
15 января 2024 г.

Томск – 2024

Министерство науки и высшего образования Российской Федерации.
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Институт прикладной математики и компьютерных наук
Кафедра компьютерной безопасности

УТВЕРЖДАЮ
Руководитель ООП
канд. техн. наук, доцент

_____ В.Н. Тренькаев

«_04_» _декабря_ 2023 г.

ЗАДАНИЕ

по выполнению выпускной квалификационной работы специалиста обучающемуся Фесковичу Андрею Олеговичу

по направлению подготовки 10.05.01 Компьютерная безопасность, специализация (профиль) «Анализ безопасности компьютерных систем»

1 Тема выпускной квалификационной работы

РАЗРАБОТКА ЗАЩИЩЁННОГО ПО АСУТП УСТАНОВКИ АНАЛИЗА МЕТАЛЛУРГИЧЕСКОЙ ПУЛЬПЫ С ПРОБООТБОРОМ

2 Срок сдачи обучающимся выполненной выпускной квалификационной работы:

а) в учебный офис / деканат – 15.01.2024 б) в ГЭК – 26.01.2024

3 Исходные данные к работе:

Объект исследования – установка отбора и анализа металлургической пульпы с использованием пробоотбора

Предмет исследования – программное обеспечение АСУТП установки анализа металлургической пульпы с использованием пробоотбора

Цель исследования – разработка защищённого программного обеспечения АСУТП установки продвинутого анализа металлургической пульпы с использованием пробоотбора.

Задачи:

1. Разработать модель угроз для АСУТП установки
2. Спроектировать систему управления установки отбора и анализа
3. Реализовать систему управления установки отбора и анализа
4. Верифицировать систему управления установки отбора и анализа на соответствие требованиям алгоритма управления техническим процессом и требованиям безопасности
5. Обеспечить защищенность операционной системы ЭВМ АСУТП

Методы исследования: теоретический, экспериментальный на базе ЭВМ.

Организация или отрасль, по тематике которой выполняется работа, – ООО “Корпорация Западная Сибирь”

4 Краткое содержание работы

Алгоритмы, программы и описания, решающие поставленные задачи

Научный руководитель
выпускной квалификационной работы
канд. техн. наук, доцент _____ / Останин С.А.

Задание принял к исполнению
студент гр. 931824 _____ / Фескович А.О.

# АННОТАЦИЯ

Дипломная работа содержит 28 страниц, 7 рисунков, 7 литературных источников.

АСУТП, ВЕРИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

**Актуальность:** разработанное программное обеспечение необходимо для вновь созданной установки, применяющей принципиально новый подход к решению задачи анализа металлургической пульпы, автоматизируя процесс отбора проб пульпы и механических операций над пробами пульпы. Данная установка удовлетворяет возросший спрос на анализ металлургической пульпы, и сделана по заказу ведущего производителя металлов России ПАО «ГМК „Нори́льский ни́кель“». Программное обеспечение верифицировано на предмет соответствия требованиям безопасности, что является необходимым условием, поскольку принципиально новый подход к анализу пульпы, включающий механические операции над пробами ценных металлов порождает новые, по отношению к традиционным методам анализа металлургической пульпы, угрозы.

**Объект исследования**: АСУТП установки анализа металлургической пульпы с пробоотбором

**Цель работы**: разработка защищённого ПО АСУТП установки анализа металлургической пульпы с пробоотбором

**Метод исследования**: теоретический и экспериментальный на базе ЭВМ.

**Результат**: Спроектировано и реализовано ПО АСУТП установки анализа металлургической пульпы с использованием пробоотбора.

В соответствии с требованием тех. задания реализован ряд функциональностей ПО, обеспечен ряд требований безопасности.

Проведена верификация программы на соответствие требованиями безопасности при помощи теста на соответствие формальной модели

Обеспечена безопасность операционной системы АСУТП для внедрения системы в технологическую сеть предприятия

# ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

В данной работе рассматривается ПО, разработанное для АСУТП установки анализа металлургической пульпы с пробоотбором.

Пульпа - это смесь твердых частиц руды и жидкости. Форма пульпы используется в металлургии для различных нужд, таких как обогащение руд, транспортировка руд и т.д. Анализ металлургической пульпы является неотъемлемой частью производственного процесса и играет важную роль в планировании и оптимизации производства.

Распространённым решением для автоматизированного анализа металлургической пульпы является анализ с помощью радиоизотопных, оптических, электромагнитных плотномеров [1] без отбора проб. В таком подходе спектральный плотномер закрепляется на пульпопроводе и непрерывно снимает показания с потока пульпы. Этот подход требует значительно меньших трудозатрат и имеет большую скорость анализа пульпы в сравнении с ручным анализом. Однако такой подход не позволяет применить многие инвазивные техники анализа, включающие в себя механические воздействия на пробы, выдерживание проб в определённых температурных, атмосферных и др. условиях, и т.д. Поэтому по сей день в индустрии сохраняется практика ручного анализа пульпы, задействующего ручной труд квалифицированных специалистов.

Для удовлетворения возросшей потребности в автоматизации анализа руд была создана установка, которая позволяет в автоматическом режиме выполнять анализ металлургической пульпы с пробоотбором, который традиционно выполняется вручную. Установка автоматически выполняет анализ, в алгоритм которого входят: отбор пробы; механические, термические и др. воздействия на пульпу, снятие показаний; возврат пробы.

Разработанное ПО, в соответствии с технологическим процессом анализа пульпы, реализует функциональность управления операциями над пульпой, в том числе отбором и возвратом проб пульпы. Также реализована функциональность снятия показаний с датчиков установки. Эксплуатация установки возможна в ручном режиме для выполнения анализа выходящего за рамки возможностей автоматического режима эксплуатации. В программе управления также предусмотрены функции: калибровки (градуировки) датчиков, настройки переменных технологического процесса анализа и удалённого доступа.

Такие факторы как: комплексность технического процесса анализа, включающего механические манипуляции над пробами; ценность металлов; наличие разных режимов управления установкой; высокая чувствительность данных; наличие удалённого доступа к

программе управления установкой порождают целый ряд угроз безопасности, в том числе специфических для данной задачи.

Разработанное ПО верифицировано на соответствие требованиям безопасности при помощи проверяющего теста на соответствие формальной модели требований безопасности

Для обеспечения конфиденциальности некоторые названия, используемые в работе, были заменены на псевдонимы.

# 1 Обзор установки

Разработанное ПО является частью всей установки анализа. Оно установлено и работает на компьютере управления установкой.

## 1.1 Состав установки

Установка состоит из следующих элементов:

1. Блоки операций:
    a. Блок отбора пробы
    b. Блоки манипуляций над пробой
    c. Блок возвращения пробы
2. Шкафы управления блоками
3. Датчики
4. Компьютер управления установкой

Всего в установке 4 блока манипуляций над пробой. Каждому блоку манипуляции и блоку отбора соответствует один шкаф управления.

Шкафы управления работают на основе микроконтроллеров. Компьютер управления установкой является персональным компьютером, настроенным для нужд эксплуатации установки.

## 1.2 Структура установки

Блоки операций установки, соединённые последовательно, образуют "конвейер", через который, в соответствующем порядке, проходят пробы.

Также, в определённых местах установки располагаются датчики, снимающие необходимые показания с проб. Конструктивно датчики являются частью блоков операций, но управление датчиками и блоками операций осуществляется отдельно от блоков операций.

Компьютер управления связан с датчиками напрямую, а с блоками манипуляций над пробами опосредованно - через шкафы управления блоками. Компьютер управления подключен к технологической сети предприятия.

На рисунке 1 представлена структурная схема установки.

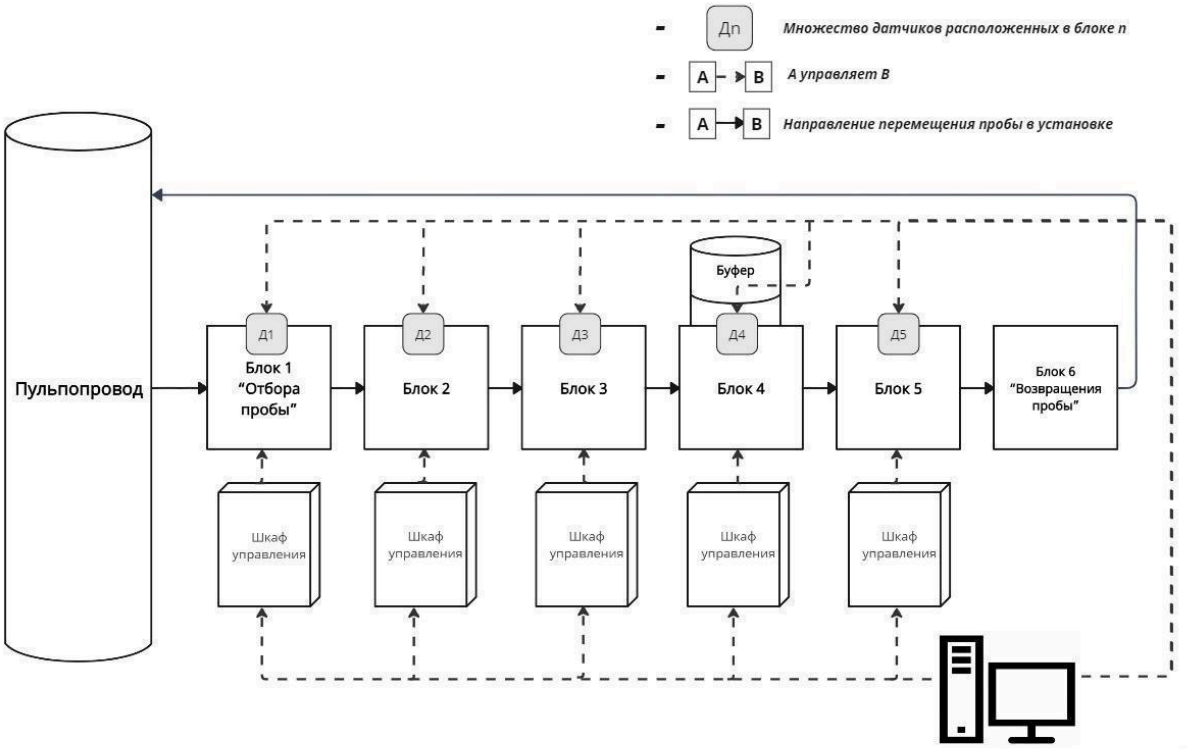


Рисунок 1 – Структурная схема установки

Для связи элементов между собой в разных частях установки используются стандарты интерфейсов RS485, USB, Ethernet. Более подробная схема, обозначающая состав и структуру аппаратного обеспечения управления установки находится в приложении А “Схема аппаратного обеспечения управления установки”

## 1.3 Работа установки

Установка располагается вблизи пульпопровода и способна осуществлять циклический отбор проб, манипуляции над пробой и возвращение проб в пульпопровод.

Каждый блок из цепочки блоков операций осуществляет очередное, необходимое для анализа, воздействие на пробу. Каждая проба сначала проходит 1-й блок (блок отбора пробы), затем 2-й и т.д. до 6-го блока (блок возвращения пробы) в строгой последовательности. Датчики установки, градуированные в составе установки, снимают необходимые показания такие как вес, температура и т.д.

Управление установкой с компьютера осуществляется через дискретные входные и выходные сигналы шкафов управления блоками (полный список сигналов и их функции см. в приложении Б). Управление датчиками осуществляется напрямую.

При помощи управляющих сигналов с компьютера управления возможен запуск блока 1 и блока 4.

Блоки операций работают по следующему алгоритму

1. Получение сигнала “Пуск” (с компьютера управления или с предыдущего блока). Переход к состоянию “в работе”
2. Выполнение операции
3. Действия по передаче пробы в следующий блок
4. Подача сигнала “Пуск” на следующий блок. Переход к состоянию готовности к работе.

На рисунке 2 представлена диаграмма работы блоков в цикле работы установки. Диаграмма создана на языке последовательностных диаграмм языка UML [2].

Работа 4-го блока не прекращается после подачи сигнала “Пуск” на следующий блок. В блоке 4 присутствует буферная область для обеспечения необходимости длительной обработки проб. Таким образом, проба из 4-го блока попадает в 5-й блок с задержкой в несколько часов.

Для синхронизации работы датчиков (снятия показаний) в установке предусмотрены выходные сигналы “Измерение 1”, “Измерение 2”.

Для контроля готовности блоков к работе предусмотрены выходные сигналы “Готовность 1”, … , “Готовность 5”, сигнализирующие о готовности блока с соответствующим номером к работе.

Для контроля аварийной ситуации предусмотрены выходные сигналы “Авария 1”, … , “Авария 5”, сигнализирующие об аварии на соответствующем блоке.

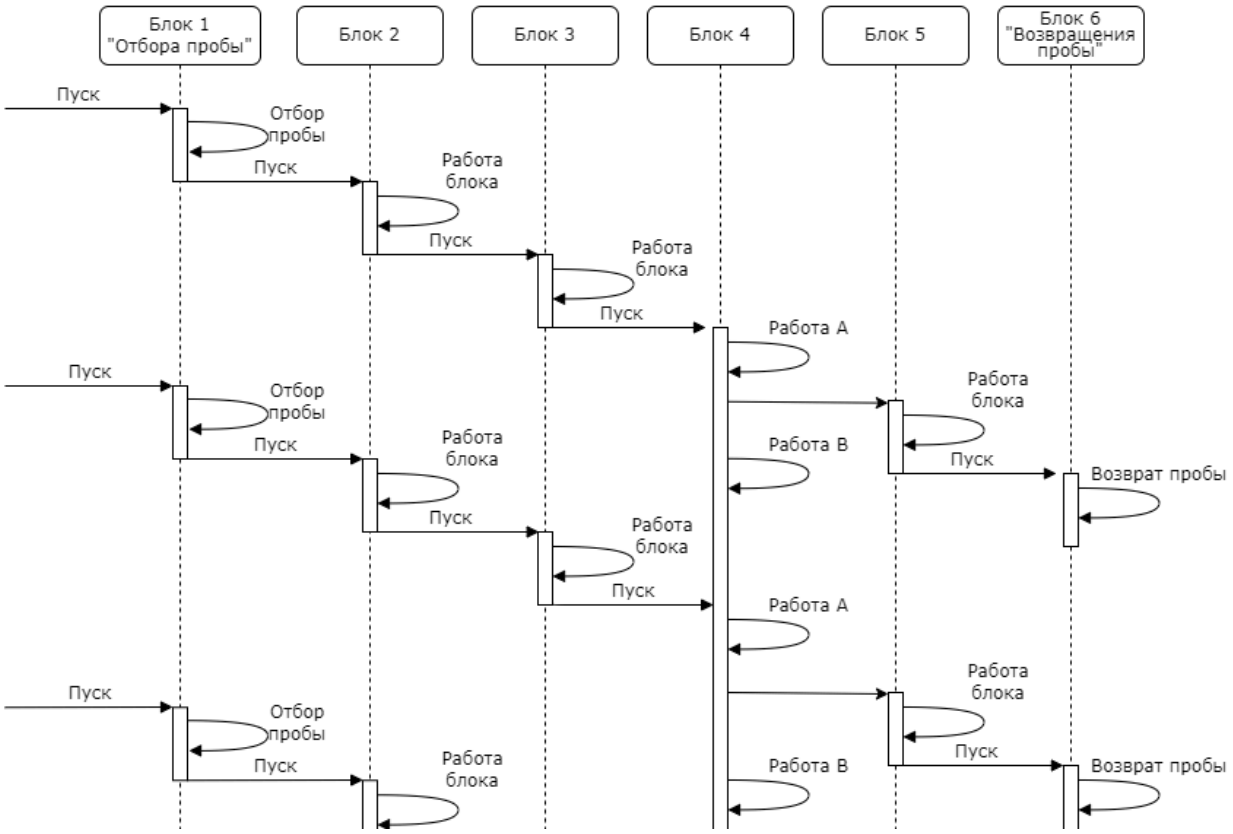


Рисунок 2 – Последовательностная диаграмма UML работы блоков операций установки

В установке предусмотрены входные сигналы “Стоп”, “Сброс”.

По входному сигналу “Стоп” работа во всех блоках операций немедленно останавливается. Блок операции, получивший такой сигнал, останавливается в том состоянии в котором он был на момент получения сигнала. Это состояние может не соответствовать состоянию готовности к работе.

По входному сигналу “Сброс” блок операции, вне зависимости от его текущего состояния, переходит в состояние готовности к работе.

# 2 Постановка задачи

Программное обеспечение, разработанное для управления установкой анализа металлургической пульпы, должно соответствовать ряду функциональных требований и требований безопасности.

## 2.1 Функциональные требования

### 2.1.1 Режим автоматического анализа

Работа установки в автоматическом режиме представляет из себя цикл. Итерации цикла начинаются через равные промежутки времени (около 4 минут, в зависимости от настроек системы).

Итерации подразделяются на полные и завершающие. Полные итерации включают в себя отбор пробы, все необходимые операции над пробой, и возвращение пробы в пульпопровод. Завершающие итерации предусмотрены для завершения работы с уже отобранной пробой (находящейся в буфере блока 4) без отбора новых проб.

По ходу движения проб через блоки операций в режиме автоматического анализа с датчиков установки снимаются показания в соответствии с технологическим процессом анализа.

В режиме автоматического анализа установка управляется оператором опосредованно - через элементы управления автоматическим анализом. Программный модуль автоматического анализа получает на вход команды с элементов управления, и, в соответствии с алгоритмом автоматического анализа, посылает нужные управляющие сигналы на вход установки. Прямого доступа к подаче сигналов управления установкой в режиме автоматического анализа у оператора нет.

Список элементов управления автоматическим анализом (кнопок пользовательского интерфейса):

- “Старт”. Запуск цикла. Начало первой полной итерации.
- “Завершить (штатно)”. Завершение цикла. Последующие операции цикла будут завершающими.
- “Приостановить”/”Возобновить”. Приостановка работы.
- “СТОП! (аварийно)”. Аварийная остановка работы.

Алгоритм работы автоматического анализа представлен на рисунке 3.

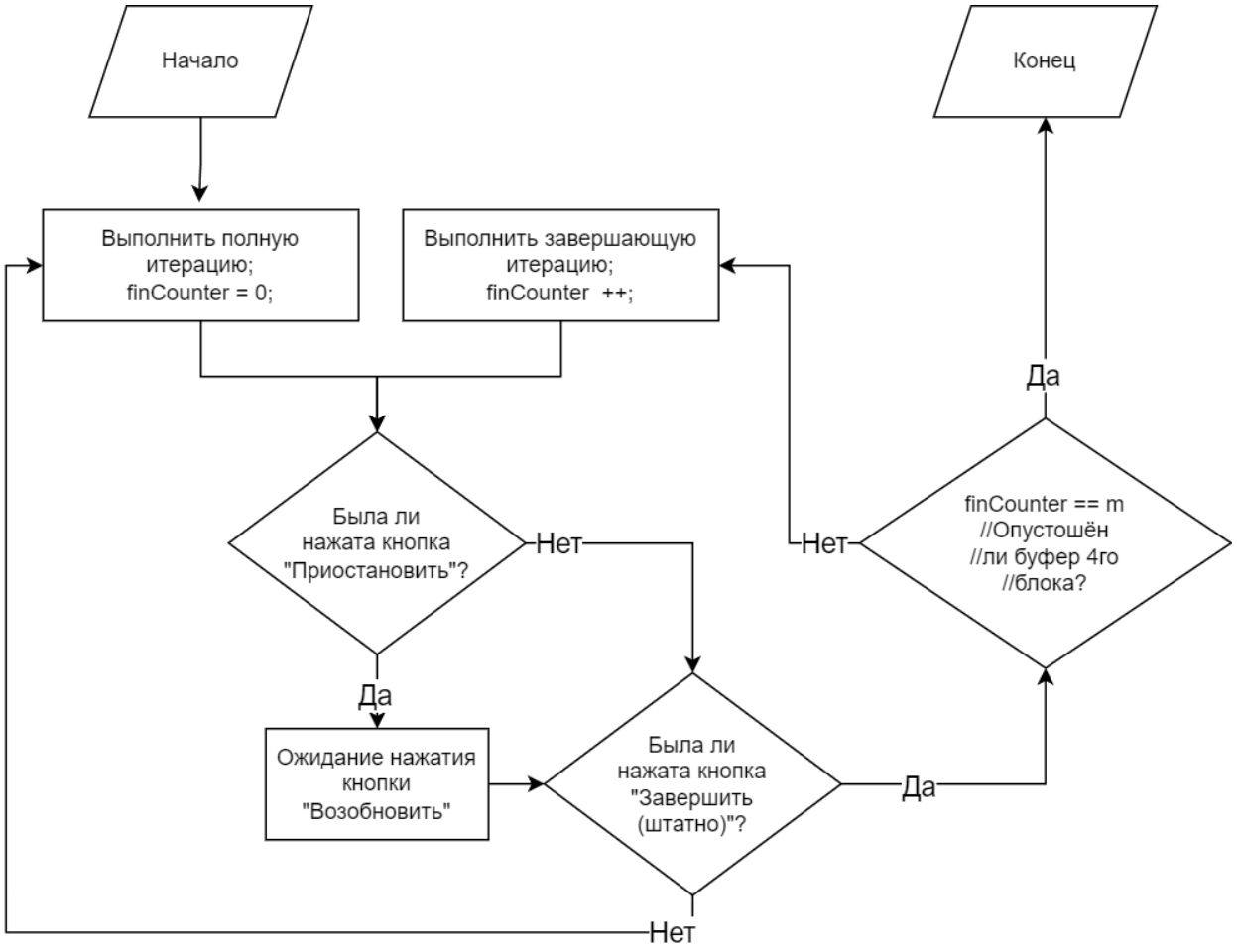


Рисунок 3 – Алгоритм работы автоматического анализа

На данной схеме переменная *m* - это объем буфера 4-го блока, а finCounter - переменная - счётчик завершающих итераций.

Таким образом, цикл работы автоматического анализа, выполненный без аварийных остановок, состоит из *n* полных итераций и, следующих за ними, *m* завершающих итераций, где *n* - произвольное число, зависящее от длительности работы установки, а *m* - фиксированное число равное объёму буфера 4-го блока.

#### 2.1.2.1 Полная итерация

Полная итерация начинается с работы 1-го блока - с отбора пробы. Отобранная проба попадает в следующий - 2-й блок. Далее над пробой выполняются операции 2-го, 3-го, 4-го блока без временных задержек между ними. А операция над пробой на 5-м блоке выполняется по мере выхода пробы из 4-го блока - с задержкой.

Запуск первой полной итерации цикла автоматического анализа осуществляется при помощи сигнала "Пуск 1", который запускает работу блока 1. Сигнал “Пуск 1” в

начале первой итерации цикла подаётся при условии готовности к работе всех блоков. Все последующие полные итерации (все кроме первой) имеют условием запуска только готовность блоков 1, 2, 3, 4.

#### 2.1.2.2 Завершающая итерация

Завершающая итерация отличается от полной тем, что в ней отсутствует отбор пробы за счёт того, что сигнал запуска подаётся на 4-й блок ("Пуск 4"). В ходе завершающей итерации происходит обработка пробы в блоках 4, 5, 6. Таким образом, завершающая итерация, включающая в себя только последние три операции надо пробой (с соответствующими им снятиями показаний) является “усечённой версией - окончанием” полной итерации.

#### 2.1.2.3 Анализ

Алгоритм анализа данных состоит из двух подалгоритмов, которые состоят из последовательных шагов с фиксированными показаниями длительности шагов и задержек между ними. Первый (аналогично - второй) подалгоритм должен запускаться при помощи сигнала “Измерение 1” (Соответственно, при помощи сигнала“Измерение 2”)

Данные автоматического анализа записываются в формате таблицы CSV с названием, соответствующим дате анализа, и располагаются в каталоге выходных данных. Таблицы данных имеют вид (см. приложение В). Таблицы данных содержат в себе также средние значения показаний за календарный день работы установки. Все данные анализа доступны к чтению в любой момент работы установки. Чтение данных анализа не препятствует работе установки

### 2.1.2 Ручное управление

Работа установки в режиме ручного управления предоставляет оператору возможность непосредственно посылать сигналы управления на вход установки в произвольном порядке (см. приложение Б)

Снятие показаний в данном режиме также требует ручной команды.

## 2.2 Требования безопасности

Требования безопасности, предъявляемые к программному обеспечению, разработанному для управления установкой, представлены в виде формальной модели конечного частично определённого детерминированного инициального автомата (далее - модель безопасности) и обеспечивают выполнения следующих свойств программы:

- Аварийная безопасность. Корректное управление аварийными остановками.
- Ограничения элементов управления в соответствии с технологическим процессом установки. Запрет доступа к командам нарушающим корректность работы установки.
- Управление доступом. Авторизация в соответствии с принятой политикой управления доступом.

Состав модели безопасности:

- Состояния (множество $S_E$). Состояния модели безопасности соответствуют состоянию программы. Состояние модели безопасности – это тройка значений:
    - Режим работы
        - Шаг в режиме работы
    - Набор доступных элементов управления (в пользовательском интерфейсе)
    - Уровень доступа
- Входной алфавит (множество $X_E$). Входной алфавит есть сумма множеств:
    - Команд пользователя
    - Внешних сигналов с датчиков управления установкой
- Выходной алфавит (множество $X_E$). Выходной алфавит является множеством команд которые программа может послать установке
- Функции переходов и выходов (функции $\delta_E$ и $\lambda_E$). Функции переходов и выходов представляют из себя набор правил модели безопасности. Таким образом:
    - Недостижимость некоторого состояния в модели безопасности соответствует недопустимости этого состояния в программе
    - Наличие/отсутствие определённых переходов по определённым входным символам с определенными выходными реакциями определяет правила по которым должна работать программа
- Начальное состояние (состояние $s_{E,0}$). Состояние в котором программа должна находится в момент запуска при каждом запуске

На рисунке 4 представлен фрагмент модели безопасности. Состояния и алфавиты автомата заменены на псевдонимы.

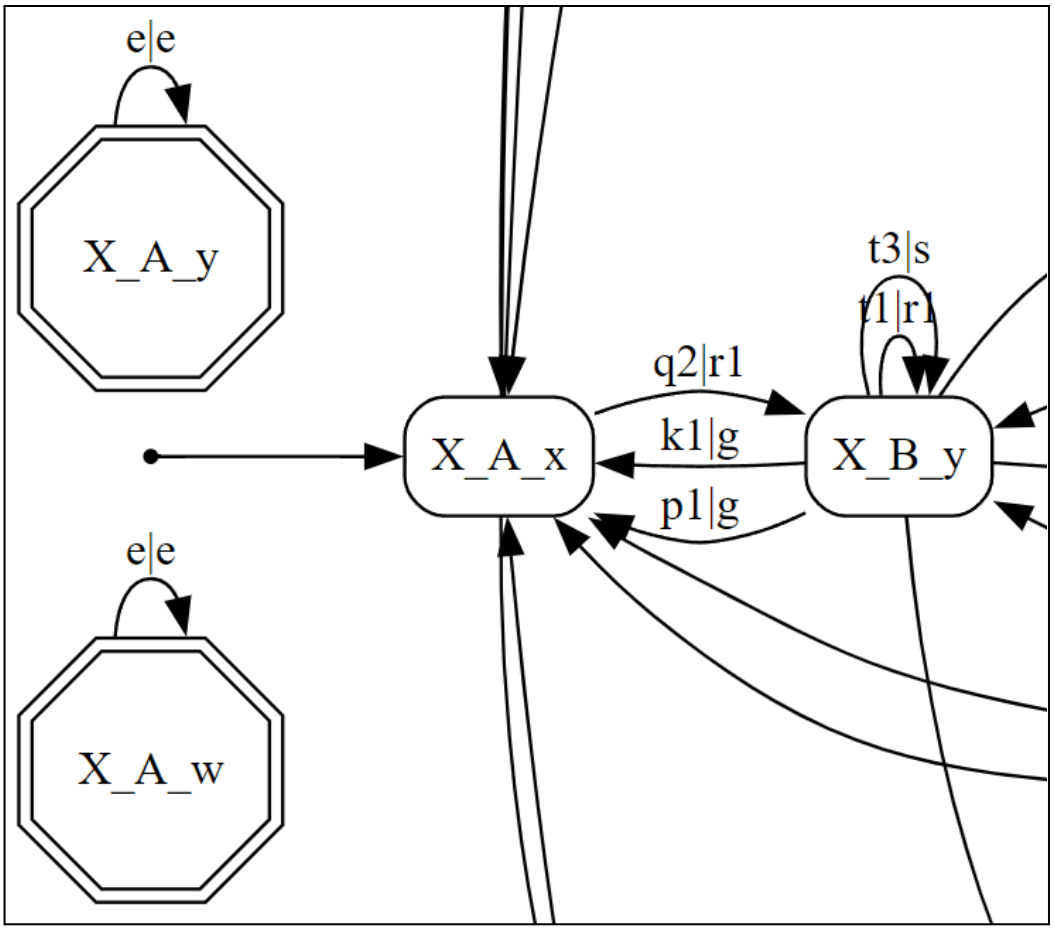


Рисунок 4 – Фрагмент модели безопасности

По схеме видно, что:

- Состояние программы, соответствующее состоянию X_A_w является недопустимым состоянием
- Начальным состоянием программы является состояние X_A_x
- Из состояния X_A_x по команде q2 программа должна выдать реакцию r1 и перейти в состояние X_B_y

# 3 Модель угроз

В соответствии с рекомендуемой структурой модели угроз безопасности информации методического документа ФСТЭК [4] была создана модель угроз для разработанного программного обеспечения

## 3.1 Описание систем и сетей и их характеристика как объектов защиты

Функциональные характеристики:

- Назначение и задачи систем и сетей:
    - Управление операциями анализа металлургической пульпы, включая отбор пробы, механические и термические воздействия, снятие показаний и возврат пробы
- Состав обрабатываемой информации и ее правовой режим:
    - Данные анализа металлургической пульпы, подпадающие под законы о промышленной тайне и конфиденциальности
- Основные процессы (бизнес-процессы) обладателя информации и оператора:
    - Процессы автоматизированного анализа металлургической пульпы с пробоотбором
- Состав и архитектура систем и сетей:
    - Операционная система
    - Программа управления установкой анализа металлургической пульпы
- Интерфейсы и взаимосвязи компонентов систем и сетей:
    - Удалённый доступ через технологическую сеть предприятия
    - Взаимодействие со спутниками GPS (локальная синхронизация времени)
    - Связь с датчиками установки через промышленные интерфейсы

Инфраструктурные аспекты:

- Информация о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры:
    - Развертывание в промышленной среде с выделенной информационной инфраструктурой
- Модель предоставления вычислительных услуг:
    - Локальное развертывание с возможностью удаленного управления

## 3.2 Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

- Нарушение целостности данных:
    - Возможные сценарии: манипуляции с данными анализа пульпы могут привести к искажению результатов.
    - Негативные последствия: неверные выводы, принятие ошибочных решений на основе анализа. Потеря конкурентоспособности в результате потери возможности планирования работы предприятия
- Утечка конфиденциальных данных:
    - Возможные сценарии: Несанкционированный доступ к результатам анализа.
    - Негативные последствия: Раскрытие коммерчески важной информации, угроза конкурентоспособности.
- Несанкционированный доступ к программе управления:
    - Возможные сценарии: Несанкционированный доступ для внесения вредоносных изменений в протоколе анализа пульпы.
    - Негативные последствия: Некорректное управление установкой, потеря данных, поломка оборудования. Возможные материальные потери из-за неработоспособности установки и потери ценных металлов, а также временные простои в производственном процессе.
- Отказ в обслуживании (DoS) или атаки на доступность:
    - Возможные сценарии: Попытки блокировки работы программы.
    - Негативные последствия: Прерывание анализа, задержки в производственных процессах.
- Нарушение работы установки:
    - Возможные сценарии: Сбои в процессе анализа пробы.
    - Негативные последствия: Некорректные пробы, искажение результатов анализа. Потеря цветных/драгоценных металлов; поломка установки
- Нарушение свойств других элементов технологической сети:
    - Возможные сценарии: Эксплуатация уязвимости в протоколе взаимодействия системы с другими элементами технологической сети:
    - Негативные последствия: Эксплуатация уязвимости может привести к несанкционированному доступу к системе, манипуляциям данными и возможным атакам на другие элементы технологической сети.

## 3.3 Возможные объекты воздействия угроз безопасности информации

Объекты воздействия:

- Компоненты систем и сетей:
    - Операционная система
    - Программа управления установкой анализа
        - Элементы управления
        - Код программы
        - База данных
    - Модуль удалённого доступа
- Интерфейсы взаимодействия:
    - Сетевой интерфейс для удалённого взаимодействия с программой
    - Окно программы управления установки с элементами управления
    - Интерфейсы для взаимодействия с датчиками

## 3.4 Источники угроз безопасности информации

Характеристика нарушителей и их целей:

- Внутренние сотрудники:
    - Цели: Несанкционированный доступ к конфиденциальной информации с целью ее использования в личных интересах.
- Конкуренты:
    - Цели: Получение конкурентного преимущества за счет доступа к конфиденциальным данным и технологическим процессам.
- Хакеры и киберпреступники:
    - Цели: Вымогательство через блокировку или угрозу уничтожения данных.
- Специальные службы иностранных государств:
    - Цели: Нанесение урона государству в области обороны, экономической безопасности и др. сферах посредством нанесения урона металлургической отрасли

# 4 Реализация

Программа включает в себя следующие основные модули:

- Система коммуникации.
    - Реализует связь с датчиками установки
- Пользовательский интерфейс
- Главный модуль программы
    - Управляет логикой работы программы, моделируя конечный автомат
- Модуль автоматического анализа
    - Реализует автоматическое непрерывное управление установкой и снятие показаний с датчиков в соответствии с алгоритмом анализа пульпы
- Модуль базы данных
    - Обеспечивает работу с данными анализа и переменными программы (см. 4.5)
- Модуль калибровки
    - Реализует функционал калибровки (градуировки) датчиков установки

## 4.1 Система коммуникации

Для коммуникации с устройствами реализовано несколько модулей коммуникации. Часть устройств поддерживает стандартный для индустрии протокол ModbusTCP [5] - для таких устройств используется отдельный единый модуль. Для остальных устройств, которые используют малораспространенные протоколы коммуникации, созданы отдельные модули по одному на протокол.

## 4.2 Пользовательский интерфейс

При включении программы управления появляются два окна: основное окно, представленное на рисунке 5, и окно-журнал, представленное на рисунке 7.

Интерфейс основного окна состоит из следующих частей:

A. Блок индикации входов
B. Индикация режима программы
C. Кнопки управления автоматическим отбором и анализом:
    a. “Старт”. По нажатию запускается автоматический анализ
    b. “Приостановить”/”Возобновить”. Приостанавливает/возобновляет цикл автоматического анализа.

c. “Завершить (штатно)”. После нажатия программа переходит в режим штатного завершения.

d. ”СТОП! (аварийно)”. Немедленно прекращает работу установки.

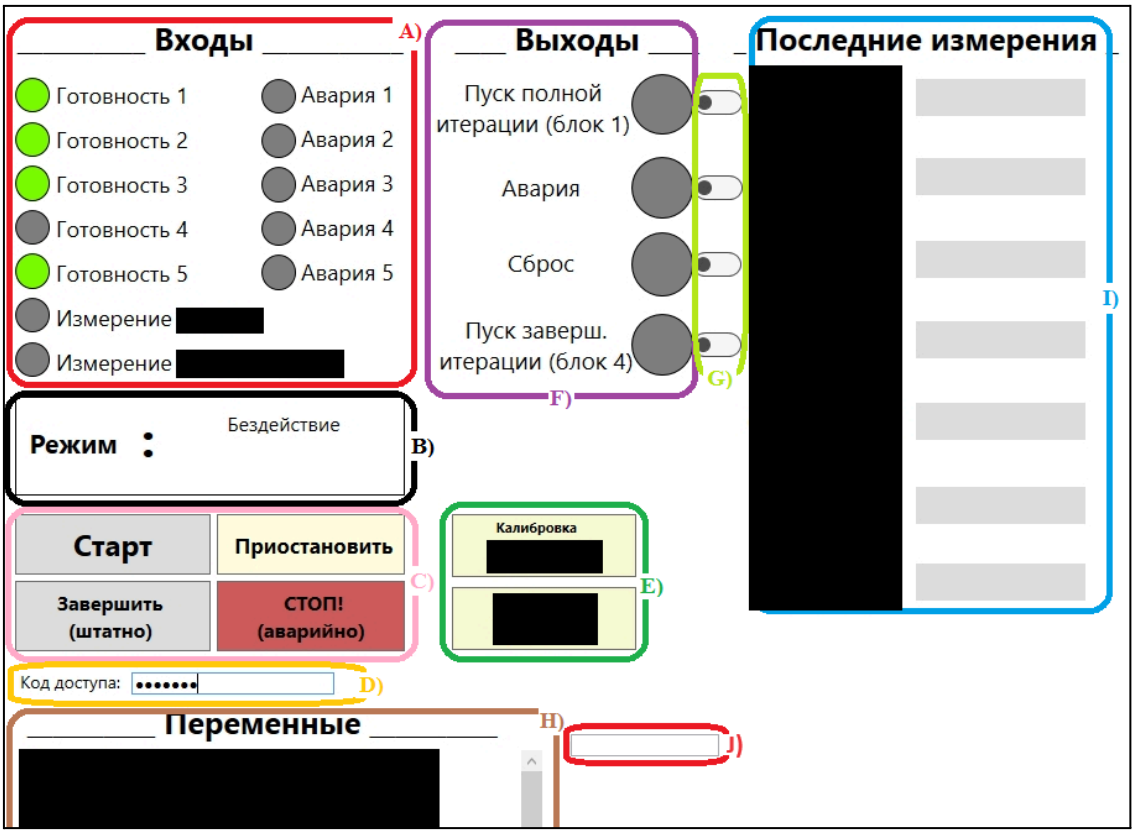


Рисунок 5 – Основное окно пользовательского интерфейса программы

D. Поле ввода кода доступа.

   a. Ручное управление и/или настройка переменных заблокирована без специального кода доступа

E. Калибровка датчиков. Кнопки управления градуировкой датчиков.

F. Блок индикации выходов программы

G. Блок ручного управления выходами программы

   a. Данный блок не отображается в основном окне программы. Для активации данного блока необходимо ввести соответствующий код доступа.

H. Блок настройки переменных

   a. Данный блок не отображается в основном меню программы. Для работы с блоком необходимо ввести код доступа.

I. Блок вывода последних измерений

J. Консоль расширенного управления

В любой момент времени элементы управления любого действия, которое недоступно по какой-либо причине, (в соответствии с логикой работы приложения и с моделью безопасности) закрываются серыми прямоугольниками и являются неинтерактивными. Пример отображения блокировки элементов управления в пользовательском интерфейсе представлен на рисунке 6.

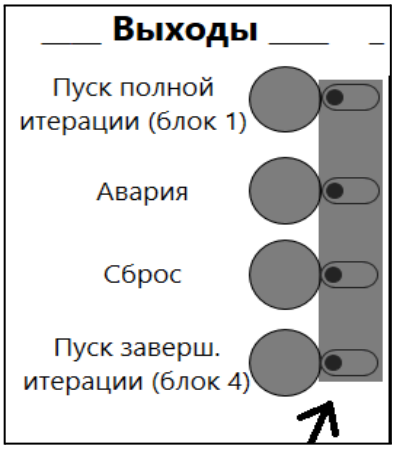


Рисунок 6 – Заблокированные элементы ручного управления

В окне-журнале выводится подробная информация о событиях в работе установки

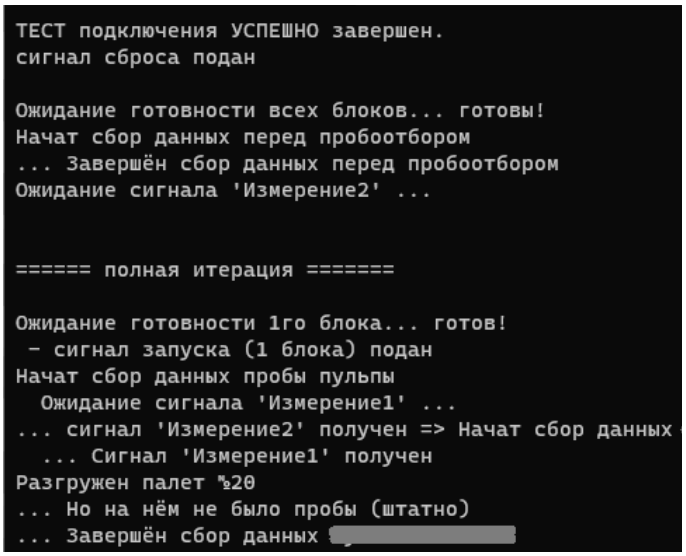


Рисунок 7 – Окно-журнал пользовательского интерфейса программы

## 4.4 Главный модуль программы

Главный модуль программы реализует функции:

- Управления подпрограммами
- Ручного управления установкой
- Связь функций программы с элементами пользовательского интерфейса через:
    - Индикацию
    - Элементы управления
    - Поля настройки переменных программы

### 4.4.1 Управления подпрограммами

В основе управления программой лежит поле S и функция δ(x). Любые команды в программе выполняются вызовом функции δ(x), где x - одна из команд списка команд программы. В функции δ(x) заложены правила, которые, в зависимости от значения поля S, ограничивают список доступных команд. Вызов функции δ(x) от недоступной команды ни к чему не приведёт. А в случае если вызов функции был от доступной команды, происходит вызов соответствующих команде подпрограмм

## 4.5 Модуль базы данных

Данный модуль работает с файлами в энергонезависимой памяти и имеет несколько подмодулей:

- Модуль переменных программы. Для настройки алгоритма анализа в программе предусмотрено множество переменных. Данный модуль позволяет обновлять и сохранять значения этих переменных.
- Модуль работы с таблицами данных анализа.

# 5 Верификация

Для формальной проверки программы на соответствие требованиям безопасности использована модель неисправности “модель белого ящика” [3] тестирования конечных автоматов.

Автомат $A$ является набором объектов $(S_a, X_a, Y_a, \delta_a, \lambda_a, s_{a,0})$, *где*:

- $S_a$ - множество состояний автомата $A$
- $X_a$ - входной алфавит автомата $A$
- $Y_a$ - выходной алфавит автомата $A$
- $\delta_a: S_a \times X_a \rightarrow S_a$ - функция переходов автомата $A$
- $\lambda_a: S_a \times X_a \rightarrow Y_a$ - функция выходов автомата $A$
- $s_{a,0}$ - начальное состояние автомата $A$
- $S_a'$ - множество “достижимых” состояний автомата $A$
    - $S_a' \subseteq S_a, \forall\ s' \in S_a'\ \exists\ x_1, \ldots, x_n : \delta_a(\ldots\delta_a(\delta_a(s_{a,0}, x_1), x_2)\ldots, x_n) = s'$

## 5.1 Модель неисправности

Модель неисправности верификации программы состоит из следующих элементов:

- **Эталонный автомат**
    - Эталонный автомат $E$ (далее Эталон) - конечный, детерминированный, частично определённый, инициальный автомат
    - В качестве эталона используется конечный автомат, являющийся представлением требований безопасности, предъявляемых к программе, в виде формальной модели
    - Программное представление
        - Эталонный автомат представлен программно с помощью готового решения (библиотеки) для программного моделирования автоматов
- **Проверяемый автомат (область неисправности)**
    - Проверяемый автомат $P$ - конечный, детерминированный, частично определённый, инициальный автомат
    - Проверяемым автоматом является модель поведения верифицируемой программы
    - Программное представление
        - Программа спроектирована в виде конечного автомата
- **Отношение соответствия**
    - В качестве отношения соответствия автоматов выбрано отношение равенства*.

- Определение отношения равенства*: Автомат $A$ находится в отношении равенства* с автоматом $B \Leftrightarrow s_{a,0} = s_{b,0}$; $S_a' = S_b'$; $X_a = X_b$; $Y_a = Y_b$; $\forall\ s \in S_a'$, $\forall\ x \in X_a$: $\delta_a(s, x) = \delta_b(s, x)$, $\lambda_a(s, x) = \lambda_b(s, x)$

## 5.2 Проверяющий тест

Программа спроектирована в виде конечного автомата $P$. Множество состояний, начальное состояние, входной и выходной алфавиты программы и эталонного автомата попарно равны по построению программы.

$S_p = S_e$, $X_p = X_e$, $Y_p = Y_e$, $s_{p,0} = s_{e,0}$

Таким образом, для доказательства равенства* автоматов достаточно доказать равенство функций переходов и выходов для каждого достижимого состояния. То есть достаточно показать, что:

$\forall\ s' \in S_E'$, $\forall\ x \in X_E$: $\delta_E(s, x) = \delta_P(s, x)$, $\lambda_E(s, x) = \lambda_P(s, x)$

Алгоритм построения входных последовательностей полного проверяющего теста [5] относительно введённой модели неисправности иметь следующий вид:

1. Построить множество достижимости $D$ для эталонного автомата $E$
   a. Множество достижимости $D$ - это множество входных последовательностей, по которым автомат $E$ можно перевести из начального состояния в каждое из достижимых состояний. $D = \{x \in X^* \mid \forall\ s' \in S_E'\ \exists\ x : \delta_E(...\delta_E(\delta_E(s_{E,0}, x_1), x_2)..., x_n) = s'\}$ и $|D| = |S_E'|$
2. Построить все возможные последовательности вида $d, x$ , где $d$ - элемент (последовательность) из множества $D$, а $x$ - буква $X_E$

В результате имеем множество $D$ x $X_E$ входных последовательностей проверяющего теста. Пусть это множество обозначается $K$. $D$ x $X_E = K$

Тогда алгоритм выполнения полного проверяющего теста имеет следующий вид:

1. i = 0
2. Пока i < $|K|$; i ++;
   2.1. Перевести автоматы в $P$ и $E$ в начальное состояние
   2.2. Подать на вход автоматам $P$ и $E$ входную последовательность $k_i$ (i-ый элемент множества $K$). Запомнить последовательности выходных реакций автоматов $O_{P,i}$ и $O_{E,i}$ . Запомнить последовательности состояний автоматов (как реакций на входную последовательность $k_i$) $\overline{S}_{P,i}$ и $\overline{S}_{E,i}$ (модель неисправности белого ящика подразумевает возможность узнать текущее состояние проверяемого автомата)

2.3. Если $O_{P,i} \neq O_{E,i}$ или $\overline{S}_{P,i} \neq \overline{S}_{E,i}$ → перейти на шаг 4

3. Завершить тест и вернуть значение ИСТИНА. (Проверяемый автомат равен эталонному. P = E)
4. Завершить тест и вернуть значение ЛОЖЬ (Проверяемый автомат не равен эталонному. P ≠ E)

По построению теста на шаге 2.2 при подаче на вход автоматам *P* и *E* последних значений входных последовательностей $k_i$ множества *K* происходит вычисление функций $\delta_E, \lambda_E$ *и* $\delta_P, \lambda_P$ на всевозможных значениях $S_E' \times X_E$. То есть, $\forall\ s' \in S_E', \forall\ x \in X_E\ \exists\ k_i : s' = \delta_E(...\delta_E(\delta_E(s_{E,0}\ ,\ k_{i,1}),\ k_{i,2})\ldots,\ k_{i,n-1})$ и $k_{i,n} = x$. Благодаря тому, что в каждый момент времени известно состояние проверяемого автомата мы можем сравнить значения функции $\delta_P = \delta_E$. Таким образом, тест позволяет сравнить значения функции $\delta_E$ со значением функции $\delta_P$ и значения функции $\lambda_E$ со значением функции $\lambda_P$ от каждого элемента $S_E' \times X_E$

Таким образом устанавливается наличие отношения равенства* автоматов *P* и *E*.

# ЗАКЛЮЧЕНИЕ

В рамках работы были достигнуты следующие результаты:

1. Разработана архитектура программы управления установкой анализа металлургической пульпы
2. Реализованы функциональные требования программы управления
3. При помощи проверяющего теста программа верифицирована на предмет соответствия требованиям безопасности
4. Обеспечена безопасности среды исполнения программы управления установкой

Разработка установки анализа продолжается и следующим этапом работы станет внедрение установки в технологическую сеть предприятия. Для этого потребуется перенести программу на специализированное аппаратное обеспечение для АСУТП. Что в свою очередь потребует дальнейшего развития программы для соответствия стандартам специализированного аппаратного обеспечения и используемого в нём программного обеспечения

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ


1. Slurry Flow Measurement: Application Challenges and Project Considerations Fluid Handling Pro — URL: https://fluidhandlingpro.com/ (Дата обращения: 25.10.2021)
2. Unified Modeling Language, v2.5.1. С. 595 - 599 — URL: https://www.omg.org/spec/UML/2.5.1/PDF/ (Дата обращения: 02.11.2023)
3. Математика в тестировании дискретных систем — URL: https://stepik.org/course/73866/ (Дата обращения: 07.11.2023)
4. ФСТЭК РФ: Методический документ "Методика оценки угроз безопасности информации — URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g/ (Дата обращения: 25.12.2023)
5. Modbus - открытый коммуникационный протокол — URL: https://ru.wikipedia.org/wiki/Modbus/ (Дата обращения: 16.08.2023)

# Приложение А

**Схема аппаратного обеспечения управления установки**


Рисунок А.1 – Схема аппаратного обеспечения управления установки

# Приложение Б

**Список сигналов управления блоками операций**

Таблица Б.1 – Входные дискретные сигналы (компьютера управления)

| *Название сигнала* | *Значение сигнала (логическая 1)* |
|---|---|
| Готовность блок 1 | Готовность блока 1 к началу работы |
| Готовность блок 2 | -//- |
| Готовность блок 3 | -//-. |
| Готовность блок 4 | -//- |
| Готовность блок 5 | -//- |
| Авария блок 1 | Авария на блоке 1 |
| Авария блок 2 | -//- |
| Авария блок 3 | -//- |
| Авария блок 4 | -//- |
| Авария блок 5 | -//- |
| Измерение 1 | Выполняется алгоритм измерения 1 |
| Измерение 2 | Выполняется алгоритм измерения 2 |

Таблица Б.2 – Выходные дискретные сигналы (компьютера управления)

| *Название сигнала* | *Значение перехода с 0 на 1* |
|---|---|
| Пуск 1 | Запуск полной итерации |
| Стоп | Аварийная остановка всех блоков |
| Сброс | Сброс блоков к состоянию “По умолчанию” (к готовности) |
| Пуск 2 | Запуск завершающей итерации |

Для корректной работы установки каждый сигнал должен принимать значение 1 не менее чем на одну секунду.

# Приложение В

**Формат таблицы данных анализа**

Таблица В.1 – Таблица данных анализа

| Номер пробы | Дата начала забора пробы | Показатель 1 | Показатель 2 | Показатель 3 | Показатель 4 | Показатель 5 | Показатель 6 | Показатель 7 | Показатель 8 | Код аварии | Показатель 9 | Показатель 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 23/10/2023 12:38:44 pm | -1 | -1 | -0.1 | 0 | 0 | 0 | 0 | -2 | - | -1 | -2 |
| 1 | 23/10/2023 12:42:45 pm | -1 | -1 | -2 | -2 | -2 | -2 | -2 | -2 | Руч н. | -1 | -2 |
| 2 | 23/10/2023 12:48:57 pm | -1 | -1 | -2 | -2 | -2 | -2 | -2 | -2 | Руч н. | -1 | -2 |
| 3 | 01/01/0001 12:00:00 am | -1 | -1 | -2 | -2 | -2 | -2 | -2 | -2 | Руч н. | -2 | -2 |
| 4 | 01/01/0001 12:00:00 am | -1 | -1 | -2 | -2 | -2 | -2 | -2 | -2 | Руч н. | -2 | -2 |
| 5 | 23/10/2023 12:59:30 pm | -1 | -1 | -2 | -2 | -2 | -2 | -2 | -2 | Руч н. | -1 | -2 |
| 6 | 23/10/2023 8:42:44 pm | -1 | -1 | -2 | -2 | -2 | -2 | -2 | -2 | - | -1 | -2 |
| 7 | 23/10/2023 8:43:23 pm | -1 | -1 | -0.1 | 0 | 0 | 0 | 0 | -2 | - | -1 | -2 |
| 8 | 23/10/2023 8:47:23 pm | -1 | -1 | -0.1 | 0 | 0 | 0 | 0 | -2 | - | -1 | -2 |

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

# СПРАВКА

Томский Государственный Университет

о результатах проверки текстового документа
на наличие заимствований

**ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ**

**Автор работы:** Фескович Андрей Олегович
**Самоцитирование рассчитано для:** Фескович Андрей Олегович
**Название работы:** Фескович А.О. Дипломная работа
**Тип работы:** Дипломная работа
**Подразделение:** НИ ТГУ, Институт прикладной математики и компьютерных наук

## РЕЗУЛЬТАТЫ

■ **ОТЧЕТ О ПРОВЕРКЕ КОРРЕКТИРОВАЛСЯ:** НИЖЕ ПРЕДСТАВЛЕНЫ РЕЗУЛЬТАТЫ ПРОВЕРКИ ДО КОРРЕКТИРОВКИ

| | | | | | |
|---|---|---|---|---|---|
| **СОВПАДЕНИЯ** | | **2.7%** | **СОВПАДЕНИЯ** | | **0%** |
| **ОРИГИНАЛЬНОСТЬ** | | **88.81%** | **ОРИГИНАЛЬНОСТЬ** | | **91.51%** |
| **ЦИТИРОВАНИЯ** | | **8.49%** | **ЦИТИРОВАНИЯ** | | **8.49%** |
| **САМОЦИТИРОВАНИЯ** | | **0%** | **САМОЦИТИРОВАНИЯ** | | **0%** |

**ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 23.01.2024**

**ДАТА И ВРЕМЯ КОРРЕКТИРОВКИ: 23.01.2024 19:28**

**Структура документа:** Проверенные разделы: приложение с.26-28, основная часть с.3-24

**Модули поиска:** СМИ России и СНГ; Библиография; Переводные заимствования по eLIBRARY.RU (EnRu); Переводные заимствования по Интернету (EnRu); СПС ГАРАНТ: аналитика; Патенты СССР, РФ, СНГ; Шаблонные фразы; eLIBRARY.RU; Диссертации НББ; Цитирование; Перефразированные заимствования по коллекции Интернет в русском сегменте; ИПС Адилет; Переводные заимствования*; Перефразирования по коллекции IEEE; Коллекция НБУ; Сводная коллекция ЭБС; Сводная коллекция РГБ; Издательство Wiley; Перефразированные заимствования по коллекции Интернет в английском сегменте; Кольцо вузов; Медицина; Переводные заимствования (RuEn); Перефразирования по коллекции издательства Wiley; Модуль поиска "tsu"; Перефразирования по СПС ГАРАНТ: аналитика; Перефразирования по Интернету; Перефразирования по Интернету (EN);

**Работу проверил:** Пахомова Елена Григорьевна

ФИО проверяющего

**Дата подписи:** 23.01.2024

Подпись проверяющего

Чтобы убедиться
в подлинности справки, используйте QR-код,
который содержит ссылку на отчет.

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.